

Annual report 2019/2020

Disclaimer: no rights may be derived from this translation and under all circumstances the official Dutch text of the *Jaarverslag 2019/2020* of the TIB prevails.

1 Summary

The Investigatory Powers Commission (TIB) published its full annual report on 20 June 2020, after having presented an abbreviated version on 16 April 2020. When the intelligence and security services AIVD and MIVD wish to use certain special investigatory powers, they submit a request to the Minister of the Interior and Kingdom Relations or the Minister of Defence. If the Minister grants authorization, the TIB then assesses whether that authorization was given lawfully, before the investigatory power may be used. In this annual report the TIB accounts for the way it assesses the authorization of the requests.

In the period from 1 April 2019 to 1 April 2020, the TIB assessed a total of 2,355 requests from both services. For 1.7% of those requests from the AIVD, the TIB ruled that the authorization had been granted unlawfully. For 3.1% of the requests from the MIVD, the TIB ruled that the authorization had been granted unlawfully. This percentage has dropped for both services compared with the preceding year. However, that does not mean everything went well. For example, the AIVD did not always inform the TIB fully, and on a number of occasions also informed the TIB incorrectly. This only came to light after the TIB asked questions about the requests. The MIVD submitted selection lists, which contained names of journalists and lawyers in requests on behalf of foreign partner services, on a number of occasions.

The TIB also assessed requests related to investigation-specific interception on the cable. These requests were ruled to be unlawful. In addition to the requested extension in time, the requests also concerned an expansion in scope. That expansion was unlawful in this particular case. It would have meant that pledges about negative filtering, that were made by the Minister leading up to the ISS Act 2017, would no longer apply. A negative filter indicates which data must not be allowed through to be stored. New requests were subsequently submitted without the expansion and these were assessed to be lawful.

When it assessed hacking requests, the TIB established that bulk hacks are at odds with the requirements of proportionality and exercising the power as targeted as possible, because data regarding millions of individuals could be obtained to gain a better view of relatively few targets. This is particularly an issue if the requirement of exercising the power as targeted as possible is not restored directly after acquisition and if the bulk data remain accessible to the service for a longer period of time. If untargeted acquisition is a goal in its own right, for example to discover unknown threats, it means that the hacks are actually investigation-specific. The ISS Act 2017 does offer safeguards for bulk data acquired by investigation-specific interception using cable or satellite, but not where it concerns bulk data obtained through a hacking operation.

2 Table of contents

1	Summary	2
2	Table of contents.....	3
3	Preface.....	4
4	Introduction.....	5
5	Assessment framework.....	7
5.1	General assessment framework.....	7
5.2	Investigation-specific interception on the cable	8
5.3	Digital intrusion: bulk hacks and innocent people's data	9
5.4	Automated data analysis.....	10
5.5	Requests by foreign services to the AIVD or the MIVD.....	12
5.6	Legal uniformity.....	13
6	Information and knowledge.....	15
6.1	General	15
6.2	Information from the services.....	15
6.3	Information from third parties.....	17
7	Results and findings.....	18
7.1	The quality of the requests.....	18
7.2	Results of the lawfulness assessment	19
7.3	Assessment of the use of the urgency procedure.....	20
7.4	Ground for unlawful conduct	21
8	Conclusions and looking ahead	23
9	Composition of the TIB.....	25

3 Preface

With a minor delay I present to you the TIB's full annual report.

As all of us, the TIB has had to contend with the consequences of Covid-19. The TIB has had to adjust its work method to ensure the continued independent assessment of the exercise of special investigatory powers. It has done so successfully. However, it was inevitable that a number of activities, including adopting this full annual report, would be postponed. An abbreviated annual report was drawn up, which provided insight into the core of the work conducted. That abbreviated annual report was published on 16 April 2020.

The TIB has been in existence for only two years. Where in its first year the TIB focused primarily on the first basic improvement of the quality of the requests by both services, its second year was characterized by a more in-depth look at that quality.

In their 2019 annual reports, the AIVD and MIVD state that they have both made greater efforts to comply with the ISS Act 2017, including improving the quality of their requests. Assessment by the TIB has played a significant role.

The TIB observed that the quality of requests has markedly and clearly improved in the second reporting year. The amount of unlawful requests from both services has also decreased considerably. Despite that declining trend, the TIB cannot afford to sit back because. The TIB found that it was not always correctly informed about the submitted requests. That means that the TIB must remain alert, should not hesitate to ask questions and should probe further if necessary.

With two years of experience, the TIB has gained more expertise and so it can better understand the consequences of the investigatory powers to be used, in particular where it concerns the more complex investigatory powers. However the challenge remains to strike the right balance in the assessment between operational necessity and the legal protection of the general public. In its assessments, the TIB uses the rulings by the European Court of Human Rights.

The ISS Act 2017 will be the subject of an evaluation in the coming year. It is the TIB's experience that the ISS Act 2017 does not always fit in the daily practices, partly because of the complexity of the cyber domain. The TIB will therefore communicate its findings to the evaluation committee.

Mariëtte Moussault
Chair of the Investigatory Powers Commission (TIB)

4 Introduction

The Investigatory Powers Commission (referred to in Dutch as Toetsingscommissie Inzet Bevoegdheden or TIB) is charged with assessing the lawfulness of the authorizations granted by the relevant Minister for the use of certain special investigatory powers by the Military Intelligence and Security Service (hereinafter: MIVD) and the General Intelligence and Security Service (hereinafter: AIVD). Examples of special investigatory powers are intercepting telephone communications or hacking a computer. The TIB is independent and its 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. The TIB's composition and investigatory powers are incorporated in the Intelligence and Security Services Act 2017 (hereinafter: ISS Act 2017).

The Minister's authorization is based on a written request. In practical terms, the TIB assesses the contents of that written request. For readability purposes this annual report will therefore refer to assessing 'requests'.

The TIB consists of three members. Two of those have extensive experience in the judiciary while the third member is appointed based on technical expertise. The TIB's secretarial office also has thorough legal and technical expertise. The procedure at the TIB is that all members read the requests and then assess them together. Sometimes this is not possible if one of the members is on leave or absent due to illness. Assessments by all three members together was also not possible during the spring of 2020 as a result of the measures to contain the coronavirus SARS-CoV-2. The TIB decided to have two members assess requests in that period.¹

The TIB's first year mainly consisted, in addition to its assessment activities, of building the organization and developing an assessment framework. In its first annual report, the TIB reflected on its composition, which of the special investigatory powers that have been provided to the AIVD and MIVD it must assess and how it conducts its activities. The TIB also described how it applies the legal requirements and how it implements the terms necessity, proportionality, subsidiarity and as targeted as possible in its assessments.

¹ The ISS Act 2017 does not provide for the appointment of deputy members. The risk that in a collective assessment the three members would infect one another, rendering further assessments impossible, was just too great. An exception was made for a limited number of fundamental matters.

This is the 2019/2020 Annual Report, covering the period from 1 April 2019 to 1 April 2020. After almost two years of assessments, the TIB's assessment framework has taken a more definite shape where it concerns most investigatory powers, but has not changed in essence compared with the description in the previous annual report. The general assessment framework was explained in the 2018/2019 TIB annual report and will therefore not be repeated here. Chapter 5 of this annual report does describe how the assessment framework applies to a number of specific investigatory powers: investigation-specific cable interception, bulk hacks, automated data analysis and the use of investigatory powers based at the request of a foreign service to the AIVD or MIVD. The chapter where these investigatory powers are discussed also looks in detail at how the assessment was conducted and how the criterion 'as targeted as possible' was applied.

Chapter 6 looks in more detail at the findings relating to the information provided to the TIB. The TIB derives its information primarily through the written requests for the use of special investigatory powers. During the past year, the information provided in requests has repeatedly been shown to be incomplete or incorrect, which is why requests that initially appeared to be lawful were ultimately assessed to be unlawful.

Additionally, it is important to avoid that the TIB obtains information from only one source. For this reason, the TIB conducts interviews with parties other than the services themselves, such as experts from the scientific field, socially committed organizations, service providers and other national and international bodies that assess the lawfulness of government activities.

Chapter 7 contains the results of the reviews conducted during the past year. The TIB established that the quality of the AIVD's requests has increased. Partly because of that improvement of quality, there has been a drop in the number of authorizations which were first granted but later assessed to be unlawful due to avoidable errors. The quality of the MIVD's requests was relatively high at the time of the TIB's start in 2018. Over the course of time, however, several areas of concern have emerged.

Chapter 8 draws conclusions and offers an outlook for the coming year.

5 Assessment framework

Before certain special investigatory powers may be used by the AIVD or MIVD, authorization from the relevant minister is required. If the Minister authorizes a request by the AIVD or MIVD, this request is subsequently submitted to the TIB for assessment. The TIB then reviews whether that authorization was given lawfully. In this chapter the TIB discusses requests for some specific investigatory powers and the areas for concern that the TIB involves in its assessment.

5.1 General assessment framework

The majority of all requests can be assessed as either 'lawful' or 'unlawful' based purely on the written request. However it regularly proves necessary to ask questions and only conduct the definitive assessment once these have been answered. More than once requests exhibit deficiencies for which a binary assessment (lawful/unlawful) is simply not enough. A request may contain sentences that are open to interpretation, in which one interpretation leads to a the assessment of the request as lawful, while another interpretation can be unlawful. Provided that all other legal requirements have been met, the TIB rules these cases as lawful 'subject to', followed by a specific explanation drawn up by the TIB that falls within the framework of the law or followed by a reference to the written response to the question.

The alternative, that is assessing each request containing such deficiencies as unlawful, would result in a greater amount of otherwise lawful requests unnecessarily being assessed as unlawful. After a minor amendment, those requests would then have to be resubmitted and be assessed as lawful with some delay. Therefore the TIB regards it as its implied authority in those cases to assess requests as lawful in the manner described above, also given the importance underlying those requests and to reduce unnecessary administrative burdens. As far as the TIB is aware, the services have followed its recorded explanation in their use of the investigatory power to date.

5.2 Investigation-specific interception on the cable

During the drafting stage of the ISS Act 2017, a major consideration was the investigatory power to conduct investigation-specific interception on the cable. The TIB was asked by the ministers to report on this matter explicitly in its annual report. The 2018/2019 annual report states that the first series of request by both services were assessed as unlawful and the requests subsequently received as lawful with a proviso.

At the start of 2020 both services submitted extension requests for investigation-specific interception on the cable. The TIB ruled these extension requests as unlawful. The requests were not only to extend the existing investigatory power in time, but also to expand it in scope. That expansion was contrary to the pledges made by the Minister leading up to the adoption of the ISS Act 2017 and in letters from the government regarding negative filtering when using cable interception. A negative filter indicates which data must not be allowed through to be stored. That was the reason why the TIB assessed the authorization granted for those specific requests as unlawful.

Following its assessments, the TIB received new requests in this reporting year. These requests no longer contained the unlawful expansion of the investigatory power, but were only asking for an extension of the requests that had already been assessed as lawful in 2019. The TIB ruled these new requests as lawful.

5.3 Digital intrusion: bulk hacks and innocent people's data

Various organizations or companies have data that can provide more information about one or more of the services' targets. If the information about the targets cannot be requested, for example because the company is located abroad, an intelligence service can ask the Minister for permission to conduct a hack to obtain that data. When using the hacking power, the principle here also is to use it in as targeted a way as possible.

However, targeted hacking is not always possible, for example because it may be too conspicuous. Therefore it could be necessary, for operational purposes, to conduct untargeted acquisition of all data. However this means that data from millions of individuals who are not the focus of the services' attention is obtained as collateral intrusion. The ISS Act 2017 offers no additional safeguards for this. The TIB has previously referred in similar cases to *bulk hacks*.²

Where bulk hacks are concerned, the TIB expects the lack of being 'as targeted as possible' during the acquisition to be restored at the first possible instance. Data of individuals that are not the focus of the services must, in the TIB's opinion, be destroyed as soon as possible after acquisition. During the entire retention period, that data should not be used by the services for all other purposes. Restoring the criterion 'as targeted as possible' by destroying data directly after acquisition also improves the proportionality of the requested use, as the extent of the infringement is limited.

In some cases the untargeted acquisition of bulk data is a goal in itself, for example to investigate as yet unknown threats. Those cases could be referred to as investigation-specific bulk hacks, following on from the investigation-specific interception using cable or satellite. However, the TIB points out that the legal system and safeguards which apply to bulk data obtained through investigation-specific interception do not apply to bulk data obtained through hacks. The necessity and proportionality of that use and the extent to which such use is targeted are all items which TIB structurally addresses in its assessments. The TIB will also point this out in the context of the legislative evaluation.

² See the TIB's response to the ISS Act 2017 amendment bill on <https://www.tib-ivd.nl/documenten/brieven/2018/08/23/reactie-wijzigingsvoorstel-wiv-2017>

For some years the services have conducted additional investigations into the cyber threat from state actors. State actors attempt to intrude in ministries, political parties, cultural-social organizations, leading Dutch sectors and vital infrastructure.³ These state actors could pose a threat to national security and are therefore the subject of investigation. When using special investigatory powers, the services may come across the data of victims obtained by a state actor. Data from such victims could be significant and help identify how and for what purpose a state actor operates. The TIB regards it as important that *victim data* is dealt with in the most targeted and proportional way possible. Victim data should in principle, in the TIB's view, only be used in the investigation into the relevant actors and not for all other purposes of the services. This applies in particular to data of victims who themselves cannot not be designated as a target for the services.

5.4 Automated data analysis

Automated data analysis means conducting computerized comparisons of data or making profile-based searches in order to recognize certain patterns. If data that was obtained by investigation-specific interception (through satellite or cable) is used in automated data analysis and the aim of this analysis is to identify individuals or organizations, ministerial authorization is first required. The TIB then reviews that authorization. Automated data analysis of data obtained by multiple (investigation-specific) bulk hacks does not require ministerial authorization and is therefore not assessed by the TIB.

The data obtained through investigation-specific interception consist for the greatest part of information from individuals who are not the focus of the services' attention. Automated data analysis therefore implies a great infringement of the privacy of a great number of individuals. This investigatory power must also be used in as targeted a way as possible. In order to weigh the infringement by automated data analysis against the necessity of the use, it is important to know what type analysis will be conducted and which datasets will be involved. For example, that could mean looking up data in certain datasets but also forms of geographical investigation using location data obtained through a variety of sources.

The use of automated data analysis had been the topic of debate between the TIB, the CTIVD, the services and the ministries for some time. The TIB and CTIVD issued a legal uniformity letter in November 2018 about the application of automated data analysis. Over time, various meetings took place about how the operational wish to use automated data analysis could be brought into line with the current legal framework. It is important to the TIB that it conducts a meaningful assessment of this infringing investigatory power.

³ See the 2019 AIVD annual report.

Mid-2019, the TIB received a request for the use of automated data analysis. Prior to that request, the TIB received a presentation about how automated data analysis is handled in practice. The TIB reviewed the request against its regular assessment framework and the assessment framework for the automated data analysis, as included in the legal uniformity letter by the CTIVD and the TIB. The request was assessed as unlawful, in short because the requested use was not as targeted as possible. This was mainly because an attempt had been made to cluster all conceivable marginal cases under the scope of a single request. In fact, the presentation had shown that in practice the vast majority of the work could be conducted with a more targeted request.

In its decision, the TIB specified elements that could – either individually or collectively – ensure the use was more targeted. By detailing these elements but leaving the choice of the elements to the service, the TIB feels there is ample opportunity for the services to operate flexibly while at the same time ensuring the investigatory power is used in as targeted a way as possible. These elements included but were not limited to:

- the *datasets* included in the automated data analysis (are all available datasets included or specific datasets?)
- the *type of data* included in the automated data analysis (all data types or specifically location data, traffic data or other user data?)
- the *subject of investigation* of the automated data analysis and the level of separation (is the use of the analysis aimed at targets only, or also at non-targets, or locations as a starting point for the automated data analysis and how many degrees of separation with respect to them?)
- the introduction of a *quantitative limit* when showing the results (that would ensure that the system forces a more targeted search request, for example by not showing the results if there are too many)
- the introduction of a *geographical limit* (for example limited to the focus areas)

The TIB subsequently received and reviewed a new request for automated data analysis. To assess this request, the TIB inspected a list of the datasets in respect of which the automated data analysis was intended to be used. This inspection was necessary to establish the possible extent of infringement of privacy of the general public and thus to conduct the proportionality assessment. In addition, listing the datasets included in the automated data analysis is an independent legal requirement.⁴

The TIB assessed the request as lawful with a proviso, adding that it assumes that only those files may be used in the analysis that are lawfully on possession of the services, with a view to the CTIVD's third progress report (report no. 66). In its third progress report, the CTIVD established that the statement of relevance and therefore the unlimited retention of bulk data sets or parts thereof had been unlawful.

⁴ Section 50(4)(b) of the ISS Act 2017.

5.5 Requests by foreign services to the AIVD or the MIVD

It is customary for services to cooperate internationally on a 'quid pro quo' basis (that is: on a give and take basis). That cooperation takes a variety of forms. In that context, information may be shared between the services deemed suitable. Another form is joint cooperation on an investigation. A further option is that a foreign service requests its Dutch colleagues to use investigatory powers to assist the foreign service in carrying out its task.

The assessments that the Dutch services make to determine whether to provide support differ from those that the services make when they want to use investigatory powers to carry out their own tasks.⁵ When it concerns support to a foreign service, the only assessments to be made are whether the interests of the foreign service are not incompatible with those of the AIVD and MIVD and whether the proper task performance by the AIVD and MIVD does not oppose providing the relevant form of support.⁶

If the use of a special investigatory power is requested on behalf of a foreign service, that request must, after ministerial authorization, be submitted to the TIB for assessment. The lawfulness assessment by the TIB applicable to these requests is more limited in nature than the assessment which the TIB conducts if the request is made for a Dutch service.⁷ Naturally a foreign service must substantiate the form of support required, but foreign services are not legally required to substantiate their requests in accordance with the regular requirements of necessity, proportionality, subsidiarity and a use that is as targeted as possible.

⁵ Vice versa, when the Dutch services request a foreign service to use a special investigatory power and that use takes place outside of Dutch jurisdiction, the TIB is not asked for a lawfulness assessment as this type of request is governed by the foreign service's legal framework.

⁶ Section 89 of the ISS Act 2017.

⁷ In its report 38, the CTIVD established that the MIVD uses special investigatory powers for foreign services. In that case it concerned the selection of untargeted data acquired from non-cablebound communication. At the time, the recommendation was to have the responsible minister grant authorization for these requests. This is now provided for by the ISS Act 2017. As it concerns the use of a special investigatory power by the MIVD, the TIB must conduct a lawfulness assessment before the investigatory power can be used.

This marginal assessment also proved significant. During the reporting year the TIB received requests for the use of investigatory powers applied for by foreign services. Those cases included the selection of investigation-specific data acquired from non-cablebound communication. Appended to these requests are lists with selectors⁸ on which selection is requested, known as *selection lists*. Due to the applicable framework, the TIB can only assess these requests marginally. That is to say, it assesses whether the use of the investigatory powers regarding individuals or organizations requested on the basis of certain grounds is incompatible with the interests or proper performance of tasks that the AIVD and MIVD have to represent.

The TIB also checks whether the selection is requested in respect of selectors attributed to lawyers or journalists, because only the Court of The Hague has jurisdiction to rule on that. When assessing this type of request of the MIVD, the TIB has repeatedly established that the selection lists contained lawyers, law firms, press agencies and journalists (without substantiation). The TIB asked questions about this and brought this point to the attention of the director of the MIVD and the Ministry of Defence. New requests were subsequently submitted with amended selection lists. The MIVD informed the TIB that its internal authorization procedure has been tightened for this specific form of support to foreign services. Since then, the TIB has not found any lawyers or journalists on selection lists.

5.6 Legal uniformity

The TIB and the CTIVD consult to formulate a joint legislative interpretation promoting a uniform and consistent application of law.⁹ Consultations take place regularly, both at official and administrative level. As a result, legal uniformity letters were drafted in the previous reporting year and sent to the Dutch House of Representatives. The contents of those letters were generally embraced by the ministers involved.

There was a difference of view on a small number of points, particularly where it concerned the scope of the lawfulness assessment by the TIB.¹⁰ A meeting on this issue was held in June 2019 with the ministers involved and the chairs of the CTIVD and the TIB. The differences of view proved reconcilable, as both Ministers informed the House of Representatives.¹¹

⁸ A *selector* could be a target's name or telephone number, for example.

⁹ House of Representatives, session year 2016-2017, 34 588, no. 18, p. 40.

¹⁰ House of Representatives, session year 2018-2019, 29924, no. 173.

¹¹ House of Representatives, session year 2018-2019, 29924, no. 186.

The following has now been laid down where the scope of the lawfulness assessment by the TIB is concerned:

- When the services already intend to *share data with foreign services* at the time of submitting their request, that intention must be specified in the request. In the context of the proportionality assessment it is particularly important to mention this if it concerns sharing unevaluated data or bulk data.
- The *intended manner of data processing* is included more generally in the authorization requests if this is relevant to assess the requested use in terms of being proportional and targeted.
- The *threat* must be sufficiently substantiated in the authorization requests, with a view to assessing the necessity and proportionality of the requested use.

The CTIVD and the TIB did not draft any new legal uniformity letters in the past reporting year.

The Court of The Hague was consulted in this reporting year. The TIB is not authorized to assess requests if the investigatory power is intended against a journalist and where that use could lead to acquiring data relating to the journalist's source.¹² As regards the question who should be considered a journalist, the TIB follows the case law by the European Court of Human Rights (hereinafter: ECHR). However there are cases of doubt particularly given the fluid definition of journalist. On one occasion a target who was not a professional journalist, conducted activities that could potentially be designated as journalism. Case-related consultations were held, to prevent a situation in which the TIB would declare itself unauthorized and that the Court would subsequently rule that it did not consider the target a journalist and that it therefore lacked jurisdiction.

¹² See Section 30(2) of the ISS Act 2017.

6 Information and knowledge

6.1 General

This chapter looks at how the TIB is informed. In order to properly assess the requested authorization to use an investigatory power, it is imperative that the TIB is fully informed. The requests made by both services are its main source of information. In addition, the TIB receives presentations by the services' staff about specific requests or about certain topics in general. However the TIB feels it is important to be informed by or exchange ideas with other parties.

6.2 Information from the services

It is essential that the information that the TIB receives is complete and correct to conduct a lawfulness assessment. The services provide this information in the written requests they draw up for authorization to use a special investigatory power. These requests are first submitted to the Minister and, if the Minister grants authorization, subsequently to the TIB.

At the start of the assessment, the TIB has the same written information as the Minister. If the information is incomplete or unclear in the TIB's opinion, the TIB can ask questions.¹³ In practice the services are asked these questions directly. The TIB regularly uses its power to ask questions.

The TIB is aware that answering questions requires the services' capacity, but it has proved necessary to ask questions. There have been instances in which requests that would have been assessed as unlawful without any further explanation of the original information were ultimately assessed as lawful with the observance of the written answers to the questions posed. In a number of cases the TIB found that the answers to the questions made such a difference to the original request that it actually constituted a new request based on different grounds, for which the Minister needed to grant authorization anew. In those cases the original authorizations were assessed as unlawful.

¹³ See Section 36(1) of the ISS Act 2017: "On being asked, our Ministers provide the assessment committee with all intelligence and grant all other cooperation it considers necessary to properly exercise its duty."

The answers to the questions repeatedly revealed that the originally provided information in the request was incomplete or even incorrect. In a few cases a request was assessed as unlawful in light of new and complete information. In one individual case dating from mid-2018, it was established that the then Director-General had decided it was not necessary to provide certain information to the TIB. That was information of which the TIB had previously indicated it was relevant to its assessment. That situation in that case lasted until August 2019, at which time the necessary information was provided by the AIVD. In other cases, there were no indications that incomplete or incorrect information was deliberately included in requests. However, regardless of whether or not incomplete or incorrect information was included deliberately in the requests, the fact is that this has undermined the confidence that the TIB should have in the information being accurate. The Minister was informed through written decisions and meetings were held between the TIB and the higher management of the AIVD.

The TIB received presentations on a range of subjects, mainly from AIVD staff, but also from the MIVD. On some occasions these presentations were offered, on others they were requested by the TIB. The purpose of these presentations was to provide the TIB with more background information about a certain operation or to serve as an additional explanation to a specific request. The TIB noticed each time that a great deal of effort had been taken to inform the TIB in detail. There was ample room to ask critical questions and these were answered generously.

6.3 Information from third parties

To preserve some form of balance in the provision of information, the TIB feels it is important to be informed by third parties. Requesting information from parties other than the services, helps the TIB to avoid tunnel vision and to prevent bias by assessing from the services' perspective only. For this reason, the TIB conducts interviews with parties other than the services themselves, such as experts from the scientific field, socially committed organizations, service providers and other national and international bodies that assess the lawfulness of government activities.

In the past year, the TIB liaised with similar review bodies from other European countries. Although state secrets are not discussed, general themes or topics are, such as applying ECHR case law. These discussions contribute to a better assessment of the services' requests. In that context, the CTIVD organized the European Intelligence Oversight Conference, which was held in The Hague at the end of 2019. This is a conference for European oversight bodies of the intelligence and security services and at which the TIB was also present. Exchanging general findings and experiences proved useful to identify best practices in assessment and oversight.

The intelligence and security services cooperate internationally in all areas of investigation and can conduct substantive meetings at case level about the use of investigatory powers and data sharing. Case-related meetings for oversight bodies have not yet been made possible. As a result it cannot be established whether a comprehensive system exists of independent assessment and prior or retrospective oversight in the use of special investigatory powers in the context of specific international cooperations.

7 Results and findings

7.1 The quality of the requests

In the first six months after the TIB became operational, the quality of the AIVD's requests was a point for concern. The TIB stated in its first annual report that from December 2018 onwards measures were taken to improve quality and that quality in fact had improved at the beginning of 2019. The quality of the requests has improved further. For example, the requests now better weigh whether the exercise of a requested investigatory power is disproportionately detrimental compared to the aim of the investigatory power (the proportionality assessment). The requests provide a better substantiation for using the means that cause the least detriment to the parties involved (the subsidiarity assessment). Furthermore, there is a steady decrease of deficiencies relating to the formal requirements of a request, such as failing to report the identity or selectors of targets.

The quality of the MIVD's requests was relatively high at the time of the TIB's start in 2018. Over the course of time, however, several areas of concern have emerged. For example it emerged that at the MIVD the intended use of the special investigatory power sometimes differed from the description in the request. The TIB brought this to the attention of the MIVD and the ministry of Defence.

Furthermore the TIB asked both services to ensure that they substantiate the need to acquire bulk data from non-targets and the possibility, or lack thereof, of reducing the acquired data at the first possible instance to only the data necessary for the investigation. A continuing area of concern is the description of the result in the extension requests in these operations, which means that the proportionality of the requested use is under pressure. If the use of an investigatory power yields little or nothing at all, it could affect the proportionality of an extension of that use. The other area of concern relating to the services' requests that exist to date is the description of the technical means and technical risks involved in digital intrusion (hacking), in particular where that intrusion affects non-targets or third parties.

7.2 Results of the lawfulness assessment

In the period from 1 April 2019 to 1 April 2020, the TIB reviewed a total of 2,355 requests. For 1.7% of those requests from the AIVD in that period, the TIB ruled that the authorization had been granted unlawfully. For 3.1% of the requests by the MIVD, the TIB ruled that the authorization had been granted unlawfully. The amount of unlawful conduct at both services has dropped compared with the period 1 May 2018 to 1 April 2019,¹⁴ when authorization was ruled to be unlawful in 4.5% of the requests by the AIVD and in 5.8% of the requests by the MIVD.

When a request to use a special investigatory power is assessed as unlawful, the service can opt to submit a new and amended request. That new request may then be ruled lawful, for instance because the investigatory power is used in a more targeted way or the infringement of fundamental rights is otherwise limited. In the reporting year, 86% of the unlawful requests were later assessed in a revised form to be lawful. The amendments could, for instance, relate to a better substantiation of a request or to the more targeted use of a means.

In the other 14% of cases, requests ruled as unlawful by the TIB were not resubmitted by the services or were again ruled unlawful. These mainly concerned investigation-specific bulk hacks and other hacks on non-targets or third parties. In those cases, the TIB ruled on substantive grounds that the authorization for the requested use of special investigatory powers was not as targeted as possible, not subsidiary or not proportionate.

In three cases the TIB declared itself to be incompetent to assess the request by the AIVD, because the use was aimed at an individual who, in the TIB's view, should be designated as a journalist or lawyer. The use of an investigatory power aimed at a journalist or lawyer must be submitted to the Court of The Hague if this could otherwise lead to the acquisition of information about journalists' sources or of confidential information between lawyers and their clients.¹⁵

¹⁴ The previous annual report covered an 11-month period because the TIB started its reviews from 1 May 2018. A total of 2,159 requests were reviewed in that period.

¹⁵ Section 30 of the ISS Act 2017.

7.3 Assessment of the use of the urgency procedure

The ISS Act 2017 contains a procedure for urgent cases where the investigatory power may be used before the lawfulness assessment by the TIB has taken place. The Minister must first grant authorization, even in urgent cases. The granted authorization must then be submitted to the TIB for a lawfulness assessment as soon as possible.

In the past year, the AIVD applied the urgency procedure in 3.3% of its requests while the MIVD applied the urgency procedure in 1.6% of its requests. The use of the urgency procedure by the MIVD was ruled lawful in all cases for both the use of the investigatory power and the applied urgency procedure. For 97.1% of those urgent requests by the AIVD, the granted authorization in an urgency procedure was ruled lawful for both the use of the investigatory power and the applied urgency procedure. In 2.9% of the urgent requests by the AIVD, the granted authorization of the use was ruled lawful but the use of the urgency procedure was not, because there was no immediate *operational* urgency. This is an improvement on the previous reporting year, when in 11.6% of cases the urgency procedure was ruled to have been applied unlawfully by the AIVD.

7.4 Ground for unlawful conduct

Figure 1 shows an overview of the reasons why requests may be assessed as unlawful. Figure 2 compares these numbers with the previous annual report. The figures relate to requests by both the AIVD and the MIVD. One request may be assessed as unlawful on more than one ground. For example, the necessity of a request may be insufficiently substantiated and often that request would then not be proportional either. That means that a single request can be included in the tally multiple times.

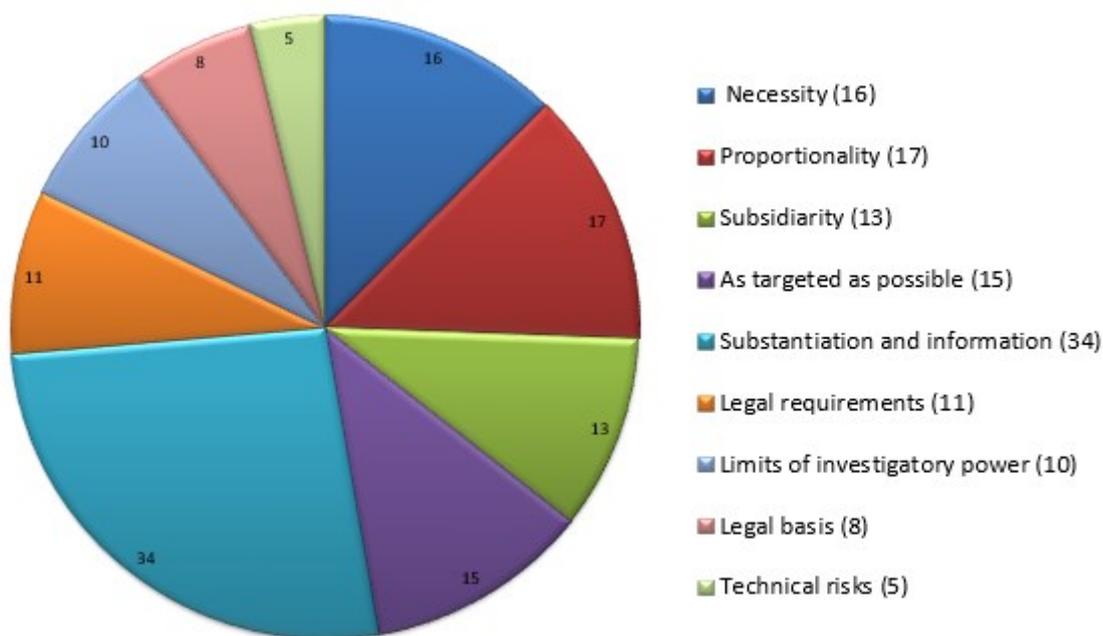


Figure 1 – Overview of the grounds for unlawful conduct (absolute numbers)

Explanation to the assessment elements

The TIB assesses if the use of a special investigatory power is *necessary*, if its use is not disproportionately detrimental compared to the necessity (*proportionality*), if the goal can also be achieved through less invasive investigatory powers (*subsidiarity*) and if the investigatory power is *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, that is does the requested use tie in 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.

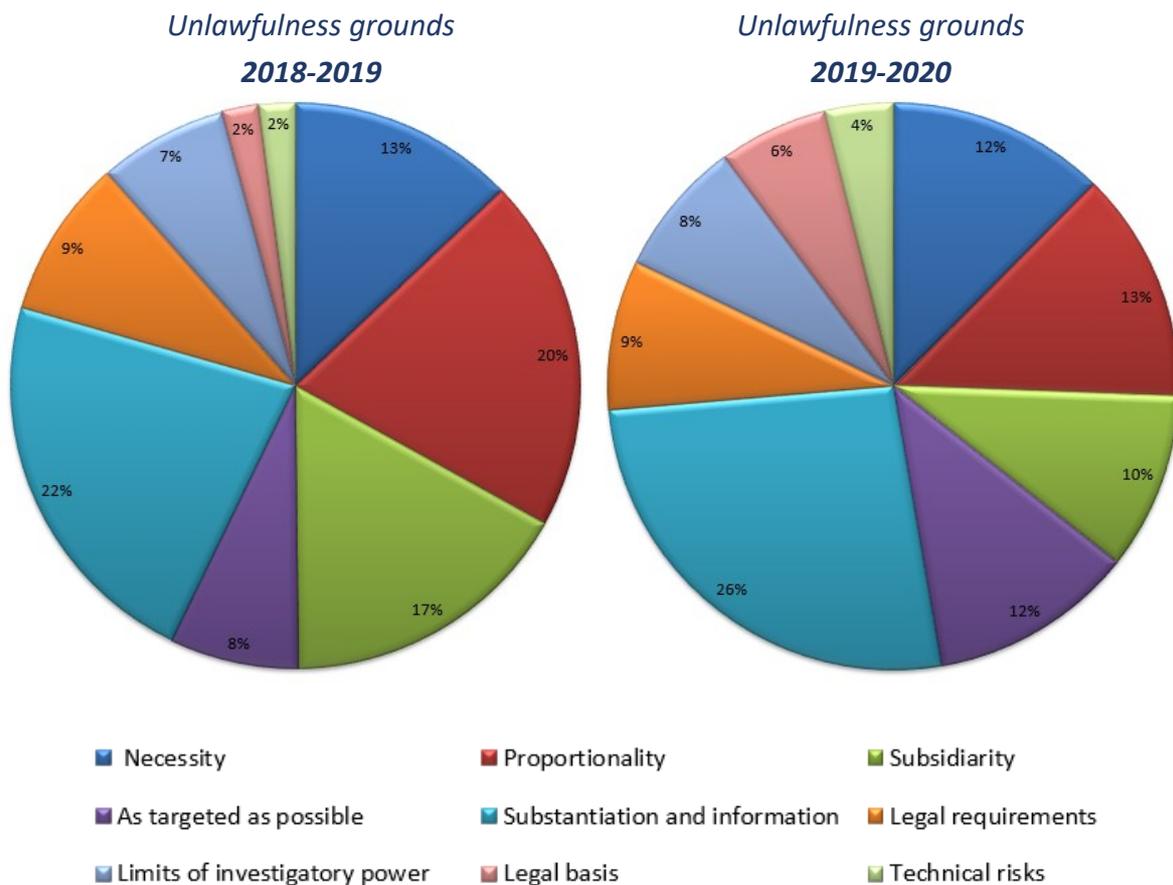


Figure 2 – Comparison of the grounds for unlawful assessments (percentages)

Compared with the 2018-2019 annual report, this 2019-2020 annual report comprises relatively more requests assessed as unlawful based on deficiencies in the information and substantiation submitted, the lack of a legal ground for the requested use and deficiencies in the description of technical risks. The number of requests assessed as unlawful based on the substantiation of necessity, proportionality and subsidiarity of the requested use has decreased in relative terms. In the 2019-2020 period, the grounds of the unlawful conduct on these points were more frequently substantive in nature (that is unlawful in terms of content because the infringement which the requested use entailed was not proportional compared to the interest it served), whereas in 2018-2019 that unlawful conduct was more frequently procedural in nature (for example, no proportionality assessment regarding the household members of a target who was the subject of a request to intercept the landline).

8 Conclusions and looking ahead

In this second annual report, the TIB concludes that the quality of the requests by the AIVD in particular has improved. The percentage of requests assessed as unlawful as a result of avoidable errors has dropped significantly. The percentage of MIVD requests that were assessed as unlawful has also decreased.

Over the past year the TIB established that it had been informed incompletely and incorrectly in the requests. The TIB brought this to the attention of both the AIVD and the Minister. The AIVD management pledged to pay particular attention to providing correct and comprehensive information to the TIB.

Extension requests relating to investigation-specific interception on the cable were initially assessed as unlawful, as they were incompatible with legislative history. New requests were subsequently submitted in which this deficiency had been removed. Those new requests were ruled to be lawful. A request to apply automated data analysis on data partly derived from investigation-specific interception was initially assessed as unlawful because the requested use was not as targeted as possible. The TIB specified a number of elements that are important to achieve as targeted a use as possible. More targeted requests were subsequently assessed as lawful with a proviso.

It emerged over the reporting year that the selection lists provided by foreign services contained selectors of lawyers and journalists. New requests were subsequently submitted with amended selection lists. The MIVD said that the internal checks had been tightened.

In its assessment of requests for digital intrusion in particular, the TIB came across issues that were not explicitly considered when the ISS Act 2017 was drafted. The TIB established that requests to conduct bulk hacks on companies and organizations with the aim of getting a better picture of a relatively small amount of targets is at odds with the requirements of proportionality and being as targeted as possible. This is particularly an issue if the requirement of being as targeted as possible is not restored directly after acquisition and if the bulk data remains accessible long-term for search requests for that specific investigation or even for all the services' other investigations. Another point of concern is how victim data is handled in investigations into cyber threats originating from state actors, where the question is for what purposes the use of such data remains proportional.

The ISS Act 2017 is continuously evolving. On 10 June 2020 a bill amending the ISS Act 2017 was adopted by the House of Representatives,¹⁶ which contains amendments relevant to the TIB, including the option to appoint deputy members. Furthermore, the bill determines that the TIB must also assess the ministerial authorization on the criterion ‘as targeted as possible’ in addition to the criteria of necessity, proportionality and subsidiarity.¹⁷ This criterion was already part of the assessment but has now been given formal legal ground. Furthermore, the current bill further specifies how this criterion should be interpreted. That provides a legal basis to the explanation that has been given by the TIB to date.

Furthermore, the evaluation of the ISS Act 2017 has begun, which will review the effectiveness and the impact of the legislation in practice. The letter to the House of Representatives shows that the evaluation will, as a minimum, address the integral review regime and more specifically the set-up, function and place of the TIB in the system. The TIB will also communicate to the evaluation committee topics such as automated data analysis, the abstraction level to determine relevance and international cooperation between the services. Naturally the TIB will contribute to a balanced evaluation of the law by specifying the points of concern that it established over time to the evaluation committee.

Traditionally national security is one of the pillars of the constitutional state whose regulation is primarily reserved for national government. However where European legislation is concerned, rulings from the highest legislative bodies are expected, which potentially could affect the interpretation of the ISS Act 2017. These European rulings may lead to amendments of the TIB’s assessment framework in the coming reporting year. For example, the Advocate General of the Court of Justice in Strasbourg advised the Court of Appeal to rule that European law also applies to the area of national security when private parties are required to cooperate with the use of investigatory powers or special investigatory powers.

In the coming year the TIB will, when assessing requests, pay particular attention to the question if the additional value of long-term use of certain special investigatory powers as evidenced by their results, continues to outweigh the corresponding infringements. We will again inform you of the TIB’s findings, results and developments next year.

¹⁶ Legislative bill (35242-2), Amendment of the Intelligence and Security Services Act 2017, session year 2018-2019, introduced on 1 July 2019.

¹⁷ A new subsection 5 is added to Section 26 of the ISS Act 2017: The investigatory power must be exercised in as targeted a way as possible.

9 Composition of the TIB

The TIB consists of three members, of which two have a background as judge. The third member can be appointed based on technical expertise. The members are appointed after a selection procedure which involves the judiciary, legislative and executive branches. The commission is supported by a secretary and deputy secretary.



M. (Mariëtte) Moussault
Chair



A.R.O. (Lex) Mooy
Member



J.R. (Ronald) Prins
Technical member until 1 June 2020.



L.W. (Lennart) Schroijen
Secretary



A.P.M. (Paul) Pols
Deputy secretary

