Toetsingscommissie
Inzet Bevoegdheden

# Annual report 2020

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

**Disclaimer**: the English version of the TIB's annual report is a third party translation of the official Dutch text. No rights may be derived from this translation and under all circumstances the official text of the *Jaarverslag 2020* of the TIB prevails.

# 1 Summary

When the intelligence and security services (hereafter: the services) wish to use certain special investigatory powers, they submit a request to the relevant ministers. This is the Minister of the Interior and Kingdom Relations where it concerns the General Intelligence and Security Service (AIVD) and the Minister of Defence where it concerns the Military Intelligence and Security Service (MIVD). If the minister grants authorization, the Investigatory Powers Commission (TIB) then assesses whether that authorization was given lawfully. In practice the TIB assesses the substance of the request because the minister grants authorization by signing the request. This annual report therefore refers to the assessment of requests. The TIB's ruling is binding, which means that if the TIB deems the authorization to be unlawful, the investigatory power may not be exercised.

In this annual report the TIB renders account for the way it assessed the authorization of the requests. The report covers the period from 1 April 2020 to 31 December 2020. In that period a total of 2,165 requests from both services were assessed. For 8.1% of the requests from the MIVD, the TIB ruled that the authorization had been granted unlawfully. In the case of the AIVD this was 1.9% of requests.

Compared with the previous reporting period, a higher percentage of MIVD requests were assessed as unlawful. This is due to both the requested investigatory powers and the quality of those requests. The TIB raised this issue with the management of the MIVD. The percentage of AIVD requests assessed as unlawful has only increased slightly.

The TIB has a greater concern, however. As in the previous reporting period, the TIB was misinformed on several occasions. The TIB established that this happened with both services. In a number of cases the incorrect information provided only came to light after the TIB had repeatedly questioned the services, whereby not only the requests but also the initial answers proved to contain incorrect information.

The number of requests for which authorization was granted increased significantly in the reporting period. The content of the requests has also increased, putting pressure on the TIB’s capacity to continue conducting thorough assessments. The capacity of the TIB will have to grow in line with this increase if it is to continue to carry out its tasks.

In the reporting period, the TIB did not receive new requests relating to investigation-specific interception on the cable. However, the TIB did receive a number of presentations about this by the services, in which the AIVD and MIVD explained the change in how they intend to obtain and filter information.

In November 2020, the TIB sent both ministers a letter about requests to use special investigatory powers to target organizations. These requests pertain to formal organizations but also to informal or fluid organizations. Within the boundaries defined for an organization, individual people can be added in the records during the authorization term, so that the special investigatory power may be used to target them as well, without a new assessment being required beforehand. The TIB established that the organization requests of both services have increased in size and scope. The TIB has announced that it would focus in the coming period on the question whether the organization requests comply with the set criteria.

Lastly, in assessing the hack requests during the reporting period, the TIB again established that bulk hacks are inconsistent with the requirements of proportionality and being as targeted as possible, particularly if the bulk data sets are to remain accessible to the service for longer periods of time. Moreover, the TIB sees authorization requests for hacks that contain a strategic substantiation only. As the legislator has not yet issued an opinion on the permissibility of these types of requests, a specific assessment framework for this is lacking. The TIB feels it is advisable that the legislator issues its opinion on permissibility of hacks conducted purely on strategic grounds and on what the legal framework for that use is.

# 2 Table of contents

# 3 Preface

This is the third annual report by the Investigatory Powers Commission (referred to in Dutch as Toetsingscommissie Inzet Bevoegdheden or TIB). In many respects, 2020 was a very different year than many people had expected at its start. The TIB also had to contend with the consequences of measures taken by the government to prevent the further spread of Covid-19. In the absence of substitutes to replace TIB members in case of illness, the TIB was forced to adapt its work procedure to guarantee continuation of the assessment process. It has done so successfully.

The TIB has been in existence for less than three years. After getting off to a flying start in 2018, the TIB initially focused on improving the quality of the services' requests, so that assessment of those requests could be conducted on all prescribed requirements. The second year was characterized by an in-depth examination of that quality. This annual report concentrates in particular on the organization requests and the hacking power. Due to growth in size and scope of the organization requests made by both services, the TIB sees cause to scrutinize these requests for compliance with all requirements. Where the hacking power is concerned, the TIB focuses in particular on how bulk data is handled.

One point for concern are the proposed plans by the outgoing government to restrict the TIB's assessment in a number of respects. Since the time of its foundation, the TIB is committed to conducting comprehensive assessments that weigh all interests and circumstances. The proposed plans could mean that the TIB will in fact be unable to conduct a proper proportionality assessment. Furthermore, it is also being proposed to cease subjecting two investigatory powers to assessment by the TIB – the power of selection and the automated data analysis. Important safeguards for the privacy of the public will be lost as a result.

However, that is not yet reality. In the coming year, the TIB will continue to conduct its lawfulness assessment to the best of its ability and as effectively as possible. It is and will remain a challenge when assessing requests to strike the right balance between the legal protection of the public and the operational necessity of the use of investigatory powers for national security.

Mariëtte Moussault
Chair of the Investigatory Powers Commission, TIB

# 4 Introduction

The TIB is an independent review committee charged with reviewing the lawfulness of the authorizations granted by the relevant minister for the use of certain special investigatory powers by the AIVD and the MIVD. The TIB's assessments include the authorization for a request to intercept a phone or to hack a computer, but also for the large-scale interception of telecommunication via satellite or cable.

The minister's authorization is based on a written request. The relevant minister grants authorization for the use of an investigatory power by signing the request. In practical terms, the TIB assesses the contents of that written request. For readability purposes this annual report will refer to 'assessing requests'.

The different aspects that the TIB assesses can be found mainly in the Intelligence and Security Services Act 2017 (ISS Act 2017). In its lawfulness assessment, the TIB assesses whether it is *necessary* to use the investigatory power. The importance of the investigatory power to be used is weighed against the detriment the use will cause (*proportionality*). The next aspect assessed is to see whether the lightest remedy was used to obtain the required information (*subsidiarity*). Lastly, the use of the investigatory power is assessed to see whether it is *as targeted as possible.* The assessment framework is explained in greater detail in the 2018/2019 annual report. 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.

The TIB's composition and investigatory powers are incorporated in the ISS Act 2017. The TIB commenced its assessment activities with the introduction of the ISS Act 2017 on 1 May 2018. 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.

There were some changes to staffing at the TIB in the reporting period. On 1 June 2020, member J.R. (Ronald) Prins left the TIB. As a result, the TIB had to conduct assessments with two members for a while. On 1 December 2020 A.W.R. (Bert) Hubert came aboard as a third member and the TIB consequently has a member with technical expertise again. The secretariat was expanded with an adviser from 15 September 2020. A more detailed description of the TIB's composition can be found in section 8.

Not only did the staff changes affect the assessment by the TIB, the measures taken to prevent the spread of Covid-19 also led to additional measures having to be taken in order to safeguard the continuity of the assessment activities. As a result, in the beginning of the reporting period assessments were temporarily conducted by only two members. The ISS Act 2017 still does not

offer scope to appoint deputy members and the risk that in a collective assessment the three members would infect one another, rendering further assessment impossible, was just too great. An exception was made in a limited number of fundamental matters. The number of face-to-face contacts between the members but also between other individuals within their professional field was limited to the strictly necessary.

Since its foundation in 2018, the TIB annually issues a report on its assessment activities. Under the ISS Act 2017, the reports must be issued by 1 May each year. The first annual report covered the period from 1 May 2018, the date on which the ISS Act 2017 entered into force, to 1 April 2019. The following report covered the period from 1 April 2019 to 1 April 2020. The TIB opted to issue a report on a shorter period for one time only – from 1 April 2020 to 31 December 2020. As a result, the TIB's annual reports will from now on cover a calendar year and be in line with the annual reports by the Review Committee on the Intelligence and Security Services (CTIVD) and those by the AIVD and the MIVD.

This annual report is structured as follows: section 5 discusses a number of topics on which the TIB focused specifically. The investigation-specific interception on the cable is addressed because the TIB reports on this every year. In addition, the TIB looks at the detected increase of the services' organization requests in size and scope. Lastly, the report discusses various issues that arise when requests for the use of the hacking power are assessed.

Section 6 contains an overview of the results of the assessments by the TIB in the reporting period. The MIVD requests in particular saw an increase in the number of requests assessed as unlawful. In the previous annual report, the TIB noted that the quality of the requests by the AIVD in particular had improved and the AIVD has kept up this improved quality over the past period. However, there are points for concern. It appeared that in the past period also, both services have informed the TIB incorrectly on multiple occasions.

Lastly, section 7 provides some conclusions about the reporting period and looks ahead at 2021.

# 5 Observations

This section looks at some topics that stood out in particular for the TIB in the reporting period of its lawfulness assessment, starting with an outline of the developments relating to investigation-specific interception on the cable. The TIB reports on the use of this investigatory power every year.

## 5.1 Investigation-specific interception on the cable

During the drafting stage of the ISS Act 2017, the investigatory power to conduct investigation-specific interception on the cable attracted a lot of public and political interest. An advisory referendum was held, partly in response to the proposed introduction of this new investigatory power in the ISS Act 2017. The new investigatory power was referred to by critics as a 'trawl net'. A majority of the voters voted against the legislation in the advisory referendum. However, the proposed new investigatory power was included in the ISS Act 2017, albeit after amendments and restrictions pledged by the minister. Using this investigatory power, the services can intercept telecommunication via the cable without the interception having to be aimed at a specific person or organization. Instead, the point of interception is chosen based on the service's specific investigation assignments.

The TIB was asked by the ministers to report on this investigatory power explicitly. The TIB again does so in this annual report. However, in this reporting period there have been no major developments in this area.

The authorization period for the use of investigation-specific interception on the cable is one year. The investigatory power based on requests assessed as lawful in the previous reporting year, could therefore still be exercised in the current reporting year. In the current reporting year, the TIB did not receive any new requests. However, both services announced requests to extend the use of the investigatory power, and in the run up to this sent presentations to the TIB to inform it about proposed changes in the implementation relating to investigation-specific interception on the cable. The services intend to change the way in which they acquire and filter data. Depending on how that change takes shape, the investigatory power might be used in a more targeted but also less targeted way. In its lawfulness assessment the TIB will of course assess if the way in which the services intend to use the investigatory power is in fact proportionate and as targeted as possible.

## 5.2 Organization requests

Under the ISS Act 2017 the services may use special investigatory powers aimed at people, but also at a group of people making up an organization. In the latter case, the ISS Act 2017 provides scope for new people 'to be added' to the request while the investigatory power is being exercised without prior authorization by the minister. The special investigatory power can then immediately be used against the added people. Only when an extension is requested can the TIB assess whether those people in the new request were categorized correctly as members of the organization.

It is precisely for this reason that the organization requests must comply with certain requirements, which are described in the CTIVD's review report no. 40.[1] The recommendations made by the CTIVD relating to those requirements were adopted by the predecessors in office of both ministers. The TIB's assessment framework also contains these requirements. In summary, therefore, an organization request must show that there is in fact an organization, fluid or otherwise, and that it is necessary to conduct an investigation into that organization. The aspects which must be addressed in the request are cooperative partnership, permanent nature, joint objective and awareness of that objective for the members of that organization. Furthermore it is important that the request makes sufficiently clear who can be regarded as a member of the organization under which circumstances. *Non-targets*[2] may not be included in organization requests because these people – as opposed to targets – cannot be considered members of the organization.

The TIB established that in the reporting period the organization requests by both services for the requested use of investigatory powers have increased in size and scope. As a result, the overview that the TIB needs to conduct its lawfulness assessment has come under pressure. Furthermore, the TIB established an increase in the number of times when it is unclear who can be regarded as a member of the organization under which circumstances. On a number of occasions, that resulted in organization requests which included people who were quite obviously not part of the organization, for example a person who as an outsider provides facilities for the organization's objective. The TIB assessed as unlawful the authorization granted by the minister in a number of organization requests that had been worded too broadly.

Given the above, the TIB saw cause to send a letter to both ministers in November 2020 in which the TIB pointed out that the criteria apply as described in the CTIVD review report 40.

[1] Review report 40 on the use by the AIVD of the interception power and the power to select sigint, CTIVD review report 40, 7 October 2014.
[2] A *non-target* is a person from a *target's* environment against whom a special investigatory power is used to gain (in)sight on the *target*.

## 5.3 Use of the hacking power

One of the special investigatory powers the services are permitted to use is the hacking power.[3] The services may also, if it proves necessary, exercise the hacking power against third parties, using that third party as a 'stepping stone' to reach the target. The investigatory power is also used to obtain information about targets from 'non-targets' who have that information in their possession. This section looks at two topics that struck the TIB in particular when assessing the requests to use this investigatory power.

### 5.3.1 Bulk hacks and determining relevance

In the previous annual report, the TIB explained that various organizations and companies such as telecom and hosting providers often have data that can provide more information about one or more of the services' targets. This data can help answer the services' investigative questions. In some cases, however, this data cannot be requested directly for legal or operational reasons. In those cases, the services can request the relevant minister for authorization to conduct a hack aimed at the company or organization that possesses the data. In practice it may be necessary – from an operational perspective – to acquire untargeted data, which will result not only in the acquisition of information about targets but sometimes also of millions of other people who are not the focus of the services, nor ever will be. The TIB refers to those cases as bulk hacks.

The ISS Act 2017 does not make provisions for specific safeguards to process bulk data sets, except where it concerns bulk data sets obtained through investigation-specific interception (Section 48 ff. of the ISS Act 2017). The services are obliged to assess the information obtained by special investigatory powers as quickly as possible for relevance. Non-relevant data must be destroyed immediately. The services have a year to assess the information for relevance. This period may be extended one time by six months, after which only the information assessed as relevant may be stored for longer. Data of individuals who are not the focus of the services must, in the TIB's opinion, be destroyed as soon as possible after acquisition. Declaring an entire bulk data set relevant has been assessed by the CTIVD to be unlawful.[4]

In certain cases the acquisition of a bulk data set can be an objective in itself, for example where it concerns data of people within a certain geographical region. In the past the TIB referred to this as an investigation-specific hack. The TIB expects the authorization requests in those cases to contain an adequate description of how the services propose to assess for relevance, given that this is a crucial part of how the service intends to actually use the investigatory power and given the infringement involved. If the service intends to declare a large part of the bulk data set relevant, it will weigh heavily in the proportionality assessment, because it means that data about people who are not the focus of the services will also be stored for a far longer period in the services' systems and be made available more widely within the service. The TIB therefore expects the services to

[3] Section 45 of the ISS Act 2017.
[4] Third progress report on the introduction of the ISS Act 2017, CTIVD report no. 66, 3 December 2019.

describe the proposed method of data processing in their requests if they already know the method at the time of requesting the authorization (or extension) or if that is actually the objective. The TIB also expects the services to attempt to reduce the size of the bulk data set as quickly as possible to only the data that is necessary for the investigation, in order to limit the infringement that the use of the investigatory power causes for people who are not the focus of the services.

In the first months of the reporting period, the TIB assessed as unlawful the authorization granted for requests in which bulk data sets would have been acquired. In those cases it was unclear beforehand whether relevance would be determined lawfully later on, or it was already clear that it would not. These cases involved the data of millions of people who were in no way the focus of the services, nor ever would be. The fact that this data would be processed and stored for a long time had to be taken into account and for that reason the use of the investigatory power was not deemed to be proportionate. Later in the year the TIB also assessed as unlawful the authorization given for a similar request. The proposed relevance assessment in that request explicitly left open the option to declare the entire bulk data set relevant. As stated above, declaring a whole data set relevant has already been assessed by the CTIVD to be unlawful. The use was therefore not as targeted as possible nor proportionate.

### 5.3.2 Strategic use of the hacking power

In this reporting period, both services have requested to use the hacking power several times based on a solely strategic substantiation. The proposed use in those cases was not expressly aimed at obtaining information with which to answer specific investigative questions, but mainly aimed at increasing the services' knowledge or options.

In a 'normal' hack for example, the services enter a computer system to copy the information stored or processed within. In a strategic hack, a computer system is entered to obtain a certain access position. That strategic access position could then – in a hypothetical situation – allow the services to gain access to otherwise inaccessible communication, such as encrypted message exchange. The position could also serve as a starting point for the use of other investigatory powers.

When the ISS Act 2017 was drafted, the legislator did not explicitly express an opinion on the question to what extent a solely strategic use of the hacking power is in keeping with the *'proper performance of the services' tasks'*[5]. The TIB therefore assesses these requests within the same assessment framework as regular requests. That means that in these cases the necessity of exercising this power must be demonstrated, the use must be proportionate, subsidiary and as targeted as possible. A further aspect that is assessed is whether the technical risks associated with the use are proportionate. The TIB regards it as advisable that the legislator gives its general opinion on the permissibility of the hacking power used purely on strategic grounds and what the

[5] Section 28 of the ISS Act 2017.

legal framework for that use is.

In the reporting period the TIB assessed requests in which the hacking power should only be exercised strategically. This resulted in both lawful and unlawful assessments.

# 6 Results and findings

## 6.1 Overall view of the requests

In the 9-month reporting period, the TIB reviewed a total of 2,165 requests. In the previous reporting year, 2,355 requests were assessed in 12 months. The number of requests has increased by 22.6% compared with the previous annual report. The number increased particularly in the last months of 2020. This increase, both in number and size, puts pressure on the TIB's capacity to continue properly assessing the requests. The TIB will have to grow in line with the increasing number and the increasing scope and complexity of the requests.

In the reporting period, the TIB questioned the MIVD in 24.7% of cases. This percentage is a slight decrease compared with the previous reporting period, in which the TIB asked questions in 26.5% of cases. In the same period, the TIB questioned the AIVD in 8.6% of cases. In the previous reporting year that was 9.3% of cases. This percentage has therefore also dropped compared with the preceding year. The TIB asks questions to ensure that both it and the services have the same view of the requested use of a special investigatory power, but also because information is sometimes missing which by law must be included in the request.

At the time of the TIB's start in 2018, the quality of the MIVD's requests was relatively high. In the previous annual report several areas of concern were listed. The TIB sees that those areas of concern have not improved sufficiently in this reporting period. It appears on further questioning, that – for example – another, broader use of the requested investigatory power was intended than the one for which the minister granted authorization. That is in part the cause of the increase in the number of unlawful conduct assessments by the TIB regarding the MIVD's requests.

Particularly the limits of the use of special investigatory powers is an area of concern. This applies not only to the proposed acquisition of data from non-targets in bulk and to declare them relevant in their entirety, but also to the insufficient demarcation of requests aimed at organizations. As a result the scope of the requested use is too wide. Depending on the nature of the request, it touches on the proportionality and subsidiarity in particular, but also on how targeted it is.

In the first annual report, the TIB called the quality of the AIVD's requests a point for concern. The AIVD has since taken big steps to improve that quality. The corresponding good results were listed in the previous annual report. The TIB sees that in general the requests in the reporting period were properly substantiated. Deficiencies relating to the formal requirements of a request, such as failing to report the identity or characteristics of targets, hardly occur anymore. However, the TIB has reason to express its concerns about the accuracy of the information presented in the requests and also in the answers to questions raised by the TIB.

In its previous annual report, the TIB had already noted that the AIVD did not always fully inform the TIB and on a number of occasions informed the TIB incorrectly. This only came to light after the TIB had asked questions about the requests. The TIB informed the relevant minister through written decisions and subsequently, meetings were held between the TIB and the AIVD management. The AIVD management pledged to pay particular attention to providing correct and comprehensive information to the TIB.

The TIB established that this pledge has not yet resulted in adequate improvement. Over the past period the TIB has repeatedly established that the information which the AIVD, but also the MIVD, included in its authorization requests later turned out to be incorrect. Both services have repeatedly indicated when answering the TIB's questions that the information in the requests was a misrepresentation of the facts or that the information was factually incorrect. Although there are no indications that the TIB was intentionally given incorrect information, it is cause to express concern, because the ministers involved base their authorization exclusively on the contents of the requests. There have also been occasions where, prompted by the answers to its questions, the TIB questioned the services further and was only then informed by the services that their previous answers were factually incorrect. It is precisely because the TIB has no options to look up information itself and therefore as oversight body is dependent on the information provided by the services, that it is of the utmost importance that it can rely on the accuracy of that information. The TIB therefore expects the AIVD and the MIVD to take significant steps in 2021 to bring this situation to an end.

## 6.2 Results of the lawfulness assessment

As stated above, the TIB assessed 2,165 requests over the preceding period. For 1.9% of the requests by the AIVD, the TIB ruled that the authorization had been granted unlawfully. For 8.1% of the requests by the MIVD, the TIB ruled that the authorization had been granted unlawfully. The number of unlawful requests has risen for both services compared with the preceding reporting period. For the AIVD this is an increase from 1.7% to 1.9% while at the MIVD the number rose from 3.1% to 8.1%.[6]

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 period, 69% of the unlawful requests were later assessed in a revised form to be lawful, because that revision, for example, concerned a more targeted use of the investigatory power. In the other 31% of cases, requests ruled as unlawful by the TIB were not resubmitted by the services or were again ruled unlawful. These cases mainly concern investigation-specific bulk hacks and strategic or other hacks on non-targets or third parties. In the previous reporting year, 86% of the unlawful requests were later assessed in a revised form to be lawful. Therefore there were more instances this year of requests assessed to be unlawful that ultimately remained unlawful.

On several occasions in this reporting period, requests were submitted to the TIB but later retracted whether or not as a result of questions posed by the TIB. It concerned 3 requests by the AIVD and 2 requests by the MIVD. The TIB did therefore not assess these requests further.

In the current reporting period, there were no situations in which the TIB declared itself incompetent to assess a request 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 under Section 30 of the ISS Act 2017 if this could lead to the acquisition of information about journalists' sources or of confidential information between lawyers and their clients.

[6] As stated above, the previous reporting period covered a whole calendar year (from 1 April 2019 to 1 April 2020) whereas the current reporting period is only 9 months.

## 6.3 Assessment of the use of the urgency procedure

The ISS Act 2017 contains a procedure for urgent cases where the investigatory power may already be exercised before the lawfulness assessment by the TIB has taken place. This may only be done if the regular procedure cannot be awaited. However even in urgent cases, the minister must first grant authorization. The granted authorization must afterwards be submitted to the TIB for a lawfulness assessment as soon as possible. If the TIB rules that the granted authorization is unlawful, all information that was obtained using this investigatory power must be destroyed immediately. The TIB also assesses the appropriateness of the urgency procedure itself. If the urgency procedure was used wrongly, the TIB must subsequently determine what should be done with the obtained information.

In the past year, the AIVD applied the urgency procedure in 2.1% of its requests while the MIVD applied the procedure in 1.0% of its requests. In those cases both the use of the investigatory power and the application of the urgency procedure were assessed as lawful. This is an improvement for the AIVD, because in the preceding period there have been some cases in which in the TIB's view there was no immediate operational urgency. In the previous reporting year that occurred in 2.9% of cases where the urgency procedure was applied. The MIVD has no change in this respect because in the previous reporting year the use and application of the urgency procedure were assessed as lawful.

## 6.4 Grounds 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 have been insufficiently substantiated and often the request is not proportionate either. That means that a single request can be included in the tally several times.

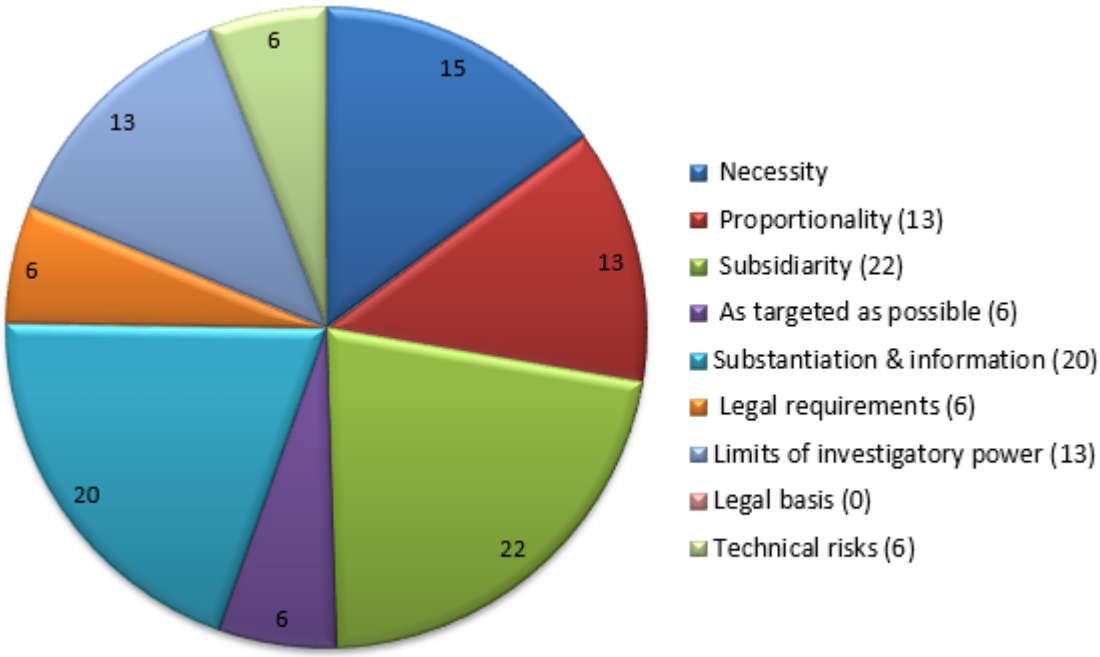


*Figure 1 – Overview of the grounds for unlawful conduct (absolute numbers)*

### Explanation to the assessment elements

The TIB assesses if the use of a special investigatory power is *necessary*, if its use is not disproportionally 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, i.e. 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*) and assesses compliance with the formal requirements set by law. 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.

**Unlawful conduct in previous reporting year**
(1 April 2019 to 1 April 2020)

**Unlawful conduct in current reporting period**
(1 April 2020 to 31 December 2020)

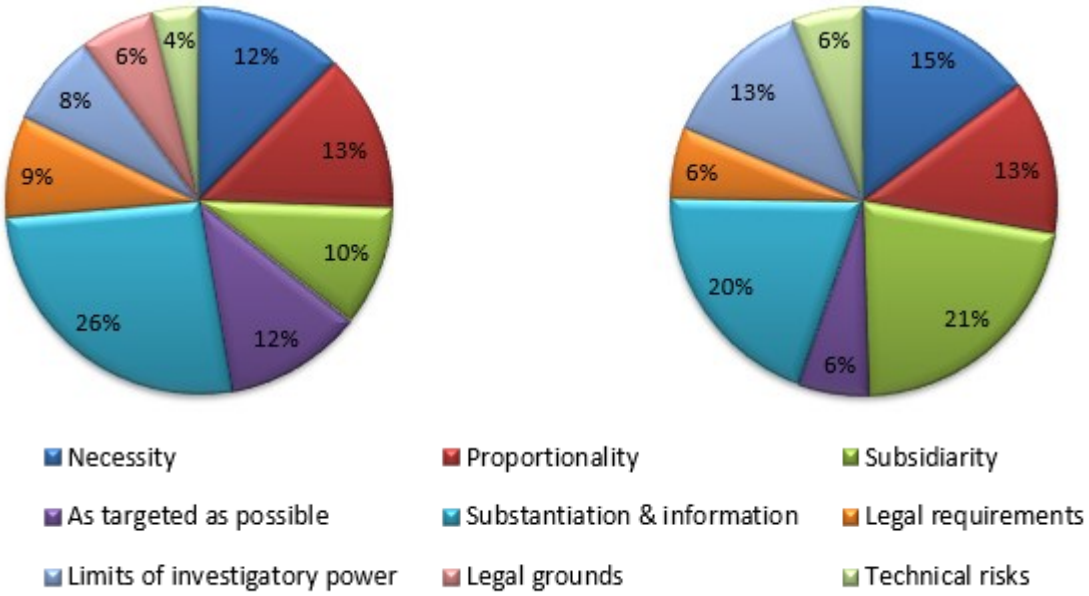


*Figure 2 – Comparison of the grounds for unlawful conduct (percentages)*

Compared with the 2019-2020 reporting year, the relative increase in the number of requests assessed as unlawful based on the substantiation of subsidiarity is noteworthy. That means that there were more occasions in which one of the services wished to use a special investigatory power without being able to substantiate sufficiently that this special investigatory power was the lightest means with which to answer the investigative questions.

On a positive note, the percentage of requests assessed as unlawful based on a use that was not as targeted as possible, was halved. Thus there were fewer occasions in which one the services wished to use a special investigatory power that would lead to the acquisition of more data than required for the investigation. However in the last reporting period, a substantial part of the total consists of cases where one of the services wanted to use a special investigatory power that ultimately proved to be broader (thus less limited in scope) than permissible or than for which the minister had granted authorization. The MIVD requests in particular saw an increase in the number of requests assessed as unlawful.

The number of requests assessed as unlawful because of a lack of formal legal requirements dropped further, as did the number of requests assessed as unlawful because of deficiencies in the information and substantiation provided. Requests assessed as unlawful due to the lack of legal grounds for the requested use did not appear at all in the reporting period.

# 7 Conclusions and looking ahead

The number of requests that the TIB assessed has increased significantly. In contrast to the previous reporting year, the TIB ascertained an increase in the percentage of requests assessed as unlawful in the current reporting period. For the AIVD this is an increase from 1.7% to 1.9% while at the MIVD the number increased from 3.1% to 8.1%. The TIB feels that adequate provision of information is more important than the increase in the number of incidents of unlawful conduct. The TIB urges both services to give the former aspect more consideration.

In the reporting period the TIB did not receive any new requests relating to investigation-specific interception on the cable. In the autumn of 2020, the TIB were given presentations by the services about proposed changes in the exercise of investigation-specific interception on the cable. The services intend to change the way in which they acquire and filter data. Depending on how that change takes shape, the investigatory power may be used in a more targeted but also less targeted way. The services are expected to submit new requests relating to investigation-specific interception on the cable in the first half of 2021.

In the autumn of 2020, the TIB saw cause to send a letter to both ministers drawing their attention to the organization requests. As regards the organization requests, the TIB established an increase in the scope of the use of investigatory powers requested by the services. As a result, the overview that the TIB needs to conduct its lawfulness assessment has come under pressure.

When assessing the requests for the use of the hacking power, the TIB identified a number of issues requiring further attention. These are mainly matters that were not specified in the legislative procedure of the ISS Act 2017. In some requests to conduct bulk hacks it was already unclear beforehand whether relevance would be determined lawfully later on. In a number of cases, the door was explicitly left open to declare the entire bulk data set relevant, contrary to the CTIVD's judgement on this.

There have been occasions where requests were submitted for the use of the hacking power based on a solely strategic substantiation. This was not explicitly addressed by the legislator during the legislative procedure of the ISS Act 2017. The TIB feels it is advisable that the legislator gives its opinion on the permissibility of strategic hacking operations and the relevant legal framework.

This is where the discussion of the main conclusions of this reporting year ends and where we look ahead.

In the reporting period, the TIB conducted several interviews with members of the ISS Act 2017 Evaluation Committee. That committee presented its report on 20 January 2021. The TIB gave its

first response the same day.[7] The TIB feels confirmed by the Evaluation Committee's observation that the TIB "*is of great added value to the oversight system*" and the a priori binding assessment is "*a significant safeguard that was added to the system*."

The TIB however sees, as does the CTIVD, that a number of the proposals made by the Evaluation Committee would mean a decline in the balance between protecting national security and the privacy of the public, and subsequently the safeguards of the rule of law. The proportionality assessment as currently conducted by the TIB would become marginalized. Important investigatory powers such as the power of selection would no longer have to be submitted to the TIB at all. It is the advance assessment of the selection of data obtained through investigation-specific interception that makes it such a significant safeguard. Both the TIB and the CTIVD have raised this issue. Naturally the TIB will closely monitor the legislator's response to the committee's recommendations and it would be more than happy to explain what the consequences would be of the Evaluation Committee's proposals for the balance referred to above.

The parliamentary debate on the proposal to amend the ISS Act 2017 submitted in 2018 will continue this year.[8] The bill amending the Act contains amendments relevant to the TIB, including the possibility to appoint deputy members. The TIB consists of three members and as a result is vulnerable, particularly because the lawfulness assessment requires at least one of the two members to have a judiciary background. The option to appoint substitute members is of great importance to ensure the continuity of the assessment process. In addition, the TIB's secretariat was and is too vulnerable. In 2020 the TIB made a start on strengthening its secretariat from 2 to 3 FTE. Given the increasing number and size of the requests, the TIB will need to be strengthened further in 2021 also.

National security is a pillar of the rule of law which traditionally is the domain of the national government bodies, but the influence of international case law can also be felt here. On the one hand the European Court of Human Rights has the competence to assess whether restrictions in, for example, the right to privacy (set out in the European Convention for the Protection of Human Rights and Fundamental Freedoms) are necessary in the interest of the national security in a democratic society. On the other, the Court of Justice of the European Union can assess whether the national court's rulings based on EU law are in accordance with the Charter of Fundamental Rights of the European Union, which specifies the right to protect personal data in more detail. On occasion both judicial bodies issue rulings that could potentially have consequences for the interpretation of the ISS Act 2017.[9] As a result, these rulings could also have an impact on the

[7] The full first response by the TIB is accessible on www.tib-ivd.nl.
[8] On 10 June 2020 a bill amending the ISS Act 2017 was adopted by the House of Representatives. The bill is currently being debated in the Senate and is unrelated to the plans of the outgoing government's plans with the proposals of the Evaluation Committee.
[9] Most recently the rulings of the Court of Justice of the European Union of 6 October 2020 in the cases Privacy International (C-623/17, ECLI:EU:C:2020:790) and consolidated cases Le Quadrature du Net et al. and

assessment of the requests, both in terms of how the assessment framework should be interpreted and which of the investigatory powers should be included in the requests put to the TIB for assessment. The TIB will therefore also monitor international case law in the coming year.

Since its foundation, the TIB has consulted with the CTIVD, including consultation about legal uniformity. Joint views on certain interpretations of the standards and assessment frameworks were set out in public letters and sent to the relevant ministers and the House of Representatives. In the coming year the TIB will again enter into consultations with the CTIVD in the interest of legal uniformity and intensify this contact in some areas.

In the coming year the TIB will focus its oversight activities on the organization requests, their limitation, and the use of the hacking power within the context as outlined in section 5.

We look forward to bringing you up to date again next year on the TIB's findings, results and developments. The annual report will then give an overview of the full 2021 calendar year.

Ordre des barreaux francophones et germanophones et al. (C-511/18, C-512/18 and C520/18, ECLI:EU:C:2020:929)

# 8 Composition of the TIB

The TIB consists of three members, of which two have a background as judge. The third member has been appointed based on technical expertise. The members are appointed after a selection procedure which involves the judiciary, legislative and executive branches. The committee is supported by a secretariat. The TIB's current structure is as follows:

**M. (Mariëtte) Moussault**
Chair

**A.R.O. (Lex) Mooy**
Member

**A.W.R. (Bert) Hubert**
Member since 1 December 2020

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