Annual Report TIB 2022

Toetsingscommissie Inzet Bevoegdheden

This annual report has a classified appendix. That appendix contains state secrets and may therefore not be disclosed to the general public. The appendix can be inspected by members of the Committee on the Intelligence and Security Services. The classified appendix describes in detail how the services conduct cable interception and discusses two strategic operations at length.

The Minister of the Interior and Kingdom Relations and the Minister of Defence also classified certain parts of this public annual report as state secret. In the annual report, these parts have been blacked out. As is the case with the classified appendix, the parts classified as state secret can be inspected by members of the Committee on the Intelligence and Security Services.

Summary

Of all requests assessed by the Investigatory Powers Commission (TIB) in 2022, the vast majority were properly and sufficiently substantiated. In general, the quality of the requests has improved and can be discerned across both the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD).

In 2022, the total number of requests (2,902 in total) decreased by 5.8% compared with the previous calendar year. The TIB has no explanation for this decrease. Striking in this respect is that the number of requests by the AIVD fell compared with last year, whereas the number of requests by the MIVD rose this calendar year. For both services, the number of unlawful conduct decisions fell: at the AIVD from 3.3% to 2.1% and at the MIVD from 7.1% to 3.0%. Looking at the unlawful conduct assessments, it is striking that in relatively more cases the TIB came to a decision of unlawful conduct because of a use that was not proportional. As regards the description of the technical risks during hacking operations, the TIB sees a positive trend in the adequate description of those risks. In seven cases, a decision of unlawful conduct was issued because the technical risks were too high.

At the same time, the past year has shown that the services expressly sought out the leeway the law provides and in exceptional cases even crossed the line.

In 2019, the AIVD obtained a bulk data set during a longer running strategic hacking operation. Decisive factors for the lawfulness assessment at the time were the safeguards (commitments in the request) that the bulk data set would be used for a limited number of investigations and that data that was obviously not relevant for that limited number of investigations would be destroyed as soon as possible.

In 2022 it appeared that the AIVD had interpreted one of the areas of investigation mentioned in the request far more broadly than the TIB had thought possible based on the description in that request.

As a result, much more data was kept and, moreover, data that was obviously irrelevant was not destroyed as soon as possible.

The MIVD was found to have later applied a procedure previously deemed unlawful by the TIB in 2022 in the same operation. These findings are discussed in more detail in this annual report.

In 2022 a request for the actual use of cable interception was assessed as lawful. An extension request was later also assessed as lawful. However, the TIB expressed its concerns several times about the continued proportionality of the investigatory power.

In 2022, there were instances where the AIVD provided inadequate information to the TIB. Several examples are given in this annual report. There is no evidence that the AIVD wilfully provided incomplete or inaccurate information to the TIB. The provision of information continues to be a topic of discussion between the AIVD and the TIB.

Lastly a striking point is that the services stated in their requests that they do not have sufficient capacity to actually carry out operations or, if they are able to carry them out, to process the results. Several examples of this are given in this annual report.

Contents

1. Preface

The main purpose of an annual report is to reflect on the past year and describe what went well and what not so well. This annual report looks back to 2022. Fortunately, there are positive developments to report. One is that the quality of the requests submitted for assessment has improved over the years.

However, there are also points for improvement. There is a slight increase in the number of requests assessed as unlawful because the boundaries of proportionality were crossed.

This annual report also looks ahead to the future, more so than in previous years. There are various developments that are important for the investigatory powers of the services and assessment by the TIB. For example, a draft bill[1] has been submitted that intends to give the services greater investigatory powers. The media sometimes portrays an image of services being overly regulated. But there is another side to that. The services already have various far-reaching investigatory powers that they use frequently for the benefit of national security. New employees at the TIB are sometimes taken aback by all that is already permitted and occurs.

1 This is the draft bill for the implementation of interim measures governing AIVD and MIVD investigations into countries with an offensive cyber programme, *Parliamentary papers II* 2022-2023, 36 263. For more information, refer to chapter 5 of this annual report. In the rest of the annual report, this will be referred to as 'the draft bill'.

The TIB has not commented publicly on the need for the expansion of powers because it feels this is a political issue. However, the TIB does consider it important that politicians and the general public are well informed about what the services are already permitted to do (and are already doing), as well as what the expansion entails. The TIB has therefore attempted to provide some examples in this annual report of operations assessed as lawful and as unlawful. The TIB held lengthy internal consultations about how to describe these operations without revealing any state secret information. No names are mentioned of parties or countries involved, nor specific tools used by the service.

> "The services already have various far-reaching investigatory powers that they use frequently for the benefit of national security."

Nevertheless, the Minister of the Interior and Kingdom Relations and the Minister of Defence decided to classify several parts of this public annual report as state secret. The TIB has therefore blacked out these parts of the report. Consequently some parts are now difficult to understand and the TIB is unable to inform the general public as it intended.

It looks beyond the bill for implementation of temporary measures. The services and departments are working on an outline memorandum in which the contours of a more radical change to the ISS Act 2017 will be sketched. As far as the TIB is concerned, the services first need to make fundamental choices about their procedures. Do the services intend to cooperate more closely? Will the ministers be the authorizing party for all operations? What type of oversight is needed? Will oversight include only lawfulness or also effectiveness? This will signal a wholly new phase for the TIB as well. An new phase calls for a new chairperson.

After five years of chairing the TIB, the time has come for me to pass on the baton. From 1 April 2023, Anne Mieke Zwaneveld will chair the TIB. I have every faith that under her supervision the TIB will continue to stand for what it has always stood: an independent review that considers the balance between the services' far-reaching investigatory powers used to safeguard national security and the privacy of citizens.

Mariëtte Moussault,
chairperson TIB

2. The TIB

The Investigatory Powers Commission (TIB) has been operating for almost five years as an independent body within the system of review and oversight of our country's intelligence and security services. Due to its duty of confidentiality, the TIB rarely seeks publicity. At the same time, the TIB feels it is important to inform the general public as best it can about its activities. This chapter describes what the TIB does. The composition of the TIB is described in the last chapter of this annual report.

The Netherlands has two intelligence and security services, namely the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD). Both services have far-reaching investigatory powers in order to conduct their work. For example, they are permitted to intercept communication from citizens, hack computers and intercept information from the cable. These investigatory powers may not be used at will. Investigatory powers that constitute a significant infringement of citizens' privacy are first assessed on whether their use is lawful. Oversight is then conducted on the exercise of those investigatory powers. The review and oversight of these services are carried out by two bodies: the TIB and the Review Committee on the Intelligence and Security Services (CTIVD). The TIB is tasked with an assessment beforehand, the CTIVD with the oversight during and after the fact. In practice we simply refer to this as oversight of the services.

The TIB was introduced into the system of oversight in May 2018. With the entry into force of the Intelligence and Security Services Act 2017 (hereinafter: ISS Act 2017), which conferred greater investigatory powers on the services, provisions for the current prior oversight were also made. The TIB is an independent committee that reviews whether the minister (the Minister of the Interior and Kingdom Relations where it concerns the AIVD and the Minister of Defence where it concerns the MIVD) granted authorization lawfully for the use of certain special investigatory powers, prior to their use. That review is binding. That means that if the TIB rules that an authorization granted by the minister is unlawful, the investigatory power may not be used and the granted authorization lapses by rule of law.

The introduction of a prior, binding review body is wholly in line with European case law on the oversight of the conduct by the intelligence and security services. There is no doubt that where democratic states face real threats such as espionage and terrorism, they must be able to defend themselves against them. States can use surveillance techniques to do so, for example, to intercept private communications. In doing so, it is crucial to provide adequate and effective safeguards against abuse. The European Court of Human Rights has ruled on several occasions that services may use some of the intelligence resources only

after obtaining permission from a body that is independent of the executive power.[2] In the Netherlands, the TIB fulfils that role.

Under Section 32(2) of the ISS Act 2017, the TIB is charged with reviewing the authorization granted by the relevant minister to use certain investigatory powers specified in the Act. For example, reviewing the authorization for a request to intercept telephone communication or hack a computer, but also to hack larger computer systems and the large-scale interception of telecommunications via satellite or cable. The relevant minister grants authorization for the use of an investigatory power by signing the request.

For the sake of readability, we will also refer to reviewing requests or assessing requests as lawful or unlawful instead of reviewing the authorization granted for a request.

The TIB assesses requests on five statutory criteria.

1. Is it necessary to use the special investigatory power? A request must justify why it is necessary *at this time* to use the special investigatory power.
2. Is it proportional to use the special investigatory power? In other words, does
3. the importance of the investigatory power to be used outweigh the invasion of privacy that the use will bring? In doing so, the TIB not only looks at the intrusion on the individual who is the subject of the investigation, but also at the intrusion on the privacy of all individuals or organizations (at least: the individuals considered to be part of an organization) who will be affected by the use.
4. Is the lightest means used to obtain the required information?
5. Is the use of investigatory power as targeted as possible? This means that the investigatory power should not be used more widely than strictly necessary.
6. This criterion has only been incorporated in the law since 14 July 2021.[3] However, the criterion was already being applied before that time. It was laid down in a policy rule at the time.
7. Does the request meet all the formal requirements of the ISS Act 2017?

> “A request must justify why it is necessary *at this time* to use the special investigatory power.”

The legal criteria most be properly substantiated. Furthermore, requests to use investigatory powers must contain adequate and correct information about the relevant facts and circumstances. When the hacking power is used, the technical risks must be explicitly described.

Requests for an investigatory power to be used against a journalist or lawyer are not submitted to the TIB. The minister is not permitted to grant authorization in those cases, only the Court of The Hague may do so.

2 For a good overview of this case law, see in particular the advisory opinion Naar een duurzaam en effectief stelsel van toezicht op de inlichtingen- en veiligheidsdiensten (Towards a sustainable and effective system of oversight of intelligence and security services), Bovend’Eert, Lawson & Winter 2022.

3 The Act of 16 June 2021 amending the Intelligence and Security Services Act 2017, effective as of 14 July 2021, see *Bulletin of acts and decrees* 2021, 335.

The TIB receives both initial requests and extension requests. An initial request is for authorization to use a special investigatory power for the first time against a certain individual or organization. Most requests have a legal maximum authorization term of three months. An extension request is a request where authorization is sought to extend that term. In that extension request, the service must show the achieved results based on which the TIB can assess if extension is necessary and still proportional. On occasion, the initial request may be modified in an extension request, in the sense that authorization is later requested for a broader use of the investigatory power.

The TIB conducts its reviews 52 weeks a year. At the beginning of each week, the TIB receives requests from the services for which the relevant minister has granted authorization. The requests are prepared on its contents by the TIB's administrative support. On Wednesdays and Fridays, TIB members convene to study the requests and the preparatory work and to issue a decision. At the end of the week, the TIB has usually come to a decision on the contents of the requests in approximately 95% of cases. In the remaining cases a decision cannot yet be taken because answers to questions are pending. In rare cases, for example when it concerns a complex hacking operation that will obtain the data of sometimes millions of [redacted][4], the TIB simply wants more time to deliberate.

If the TIB has insufficient information to come to a decision or if there is confusion about the safeguards to be used, the TIB may question the relevant service.

If the TIB decides that the granted authorization is lawful, that decision will be made known to the relevant minister and service as soon as possible, often the same day. The service may exercise the requested investigatory power from that moment on. In the vast majority of cases, the TIB comes to a decision within two to no more than five working days after the request was submitted. The TIB may also add a remark to its lawfulness decision, for example if there is a small failing in the request that has no further impact on the decision.

If the TIB rules that the minister's authorization was not granted lawfully, it provides a substantiated unlawful conduct ruling in writing. An unlawful conduct ruling means that the service may not exercise the requested investigatory power. These decisions are also usually sent to the relevant minister and service in the same week. An unlawful conduct ruling does not hinder the submission of a renewed request, by which the unlawful conduct could removed, for example, by adding additional safeguards.

The TIB's composition is described in the ISS Act 2017. The TIB consists of three members, of which two have extensive experience in the judiciary. The third member is appointed for their technical expertise. The members of the TIB are supported by a secretariat. Since February 2022, the TIB also has deputy members, who can be deployed on the occasions that the TIB cannot meet in full.

4 For purposes of readability, read 'individuals' here.

3. Highlighted topics

This chapter comprises two sections. The first section discusses investigation-related interception on the cable, followed by the technical risks and unknown vulnerabilities in section 3.2. Section 3.3 looks at bulk data sets and determining relevancy. Some strategic operations will then be discussed in section 3.4 This chapter concludes with section 3.5 about information provision by the services and section 3.6 about 'capacity issues'.

3.1 Investigation-related interception on the cable

Since May 2018, the services have had the investigatory power to intercept large amounts of internet traffic on the cable. This investigatory power consists of two parts: taking snapshots and the actual interception for their investigation. Snapshots are taken to verify whether the internet traffic potentially has significant intelligence value. Snapshots are taken using technical and content-related features to examine whether information is actually relevant to the specific investigation assignments.[5] In contrast, the production of cable interception pertains to the use of internet traffic for intelligence investigation.

At the start of 2022, the services were permitted to take snapshots of a number of data streams on one specific cable route, based on a request submitted in 2021. Actual interception for investigation purposes did not take place because that had been ruled unlawful in 2021. In the first quarter of 2022, requests for bulk interception were submitted to the TIB that were no longer intended for snapshotting but for interception for production purposes. The TIB ruled those granted authorizations to be lawful.

As regards the requests to intercept for investigation purposes in 2021 that the TIB considered unlawful, [redacted]. Leads are used to intercept internet traffic that may originate from the service's targets. However, in the vast majority of cases it will concern internet traffic of other individuals. A select number of service staff members may then work with the information from leads to find targets. The selectors are specific, identifying characteristics of targets. These selectors can be used to intercept specific internet traffic of targets. All the other internet traffic on the data streams is not stored and therefore this is a far more targeted form of cable interception than was intended in 2021.

5 *Parliamentary papers II* 2016-2017, 34 588, No. 3 (Explanatory Memorandum), p. 110.

During 2022, the TIB regularly received requests in which the services described which leads they wanted to use in investigations and from which targets or target organization they wanted to intercept selectors. Initially the TIB ruled all these extension requests to be lawful. However, the TIB repeatedly called for a better description of the yield in relation to the size of the infringement.

The TIB also called for a better description of leads, because these were only provided with examples and thus the scope was not defined clearly enough. After the summer of 2022, a service submitted one request in which the leads for an organization had been better described. Only then did it appear that the limits of proportionality and of the criterion as targeted as possible were being interpreted far more broadly than the TIB had concluded based on the requests submitted at the time. The TIB ruled that request to be unlawful. This service resubmitted the request twice after amendments but the TIB arrived at unlawful conduct rulings in both cases because the amendments made were insufficient to ensure the use was more targeted. The service did not include that broader description of leads again in the request, nor in later requests.

[redacted]. The TIB also ruled this request to be unlawful, because the service failed to properly argue why it was necessary to store the bulk data that they would intercept for the requested time period.

3.2 Technical risks and unknown vulnerabilities

The TIB reviews the technical risks for each use of the hacking power, in accordance with the ISS Act 2017. There are two kinds of risk. Firstly, the risk to the availability and integrity of automated devices or systems concerned. If the service enters a system, is there a risk of that system failing? That is relevant where it concerns the internal network of a telecom provider, for example. Customers can be dependent on the telecom provider's service if they need to call an emergency number.

Secondly, the TIB assesses the risk of misuse by third parties. That mainly concerns the question whether state or other actors could misuse our services' knowledge and technical means. Being able to make that assessment is particularly important when using unknown vulnerabilities. Because if another actor is able to successfully copy the method, there is a risk that that actor could then easily enter systems in the Netherlands or of their allies.

The request must contain a separate description of the technical risks. They are part of the proportionality assessment by the TIB in the sense that they are weighed against the operational interests of the services.

Again in 2022, the TIB assessed a great many requests in which authorization was asked for the start or continuation of a hacking operation and in which the estimate of technical risks was a topic of debate. In the previous year the TIB had issued an unlawful conduct ruling in thirteen requests. In those cases the technical risks had not been sufficiently clarified or the TIB was of the opinion that the risks were too great. That number fell in 2022 to seven unlawful conduct rulings.

This should, however, be put in perspective. The services almost exclusively submit combined requests for authorization to both scan and to enter computerized devices. At the start of the operation in those cases, the services do not yet have an adequate, up to date picture of the technical possibilities in each specific case. The TIB respects that. For many years now, it suffices if the services indicate at the start of the hacking operation within which framework they will operate. That general framework describes the technical use for which the TIB feels that the technical risks will not be too great. Many of the hacking operations can be initiated very quickly in this set-up, and follow the pattern of weekly review. These requests (where it concerns the description of technical risks) are assessed very quickly. These requests mainly involve the regular assessment of necessity, proportionality, subsidiarity and the criterion of as targeted as possible, which in about 95% of cases is completed within a few days.

3.2.1 Descriptions of technical risks

Over the past year, the TIB has noticed that the services provide better information about the technical risks associated with a hacking operation. That was not only the case for the requests themselves, but also for the background presentations and presentations explaining the requests that the TIB received in a number of operations in 2022. It generally concerns those cases in which the services want to use an unknown vulnerability. On those occasions, the TIB is given a good, clear explanation including about the hacker who will carry out the operation. The TIB views this as a positive development.

> “Only in exceptional cases has the TIB had to establish that the description of the technical risks was unsatisfactory.”

Only in exceptional cases has the TIB had to establish that the description of the technical risks was unsatisfactory. This can be illustrated by the following example.

[redacted]. There was no further explanation. The TIB questioned the service about this. The AIVD answered that the vulnerability would no longer be used. The questions were not answered in substance. Therefore the TIB repeated its request for an explanation. Authorization for the use had been granted by the minister and that authorization needed to be reviewed. The AIVD then provided the CVE number.[6] According to the AIVD, it was unable to provide further explanation because it had not fully worked out the vulnerability.[7] The TIB was unable to obtain a full picture based on the CVE number alone, but the nature of the vulnerability combined with a commonly used software package raised suspicions that it involved a significant vulnerability. In a previous extension request, the TIB had indicated that it wanted to be informed fully and satisfactorily about the technical risks and not simply be given a CVE number. On the basis of the request alone and without further explanation, the technical risks and proportionality could not be properly assessed and for that reason the granted authorization was ruled unlawful.

6 An organization gives all known vulnerabilities a unique number. The organization has a number of details, based on the CVE number, such as the nature of the vulnerability and which software versions are vulnerable.

7 [redacted].

3.2.2 The use of unknown vulnerabilities

If the services intend to use an unknown vulnerability, the TIB expects this to be submitted to the minister and the TIB first. That is necessary mainly because if the vulnerability is leaked, the potential consequences can be very serious indeed. The vulnerability is, by definition, unknown. Should a third-party, for example a hostile state actor, recognize the vulnerability and subsequently use it against the Netherlands, no one would be able to defend themselves against that.

In rare cases, the TIB assessed the authorization granted to be unlawful because the technical risks were deemed too great and the use thereby not proportional. That example was the use of an unknown vulnerability in a business software package.

The leak of that vulnerability could potentially have far-reaching consequences. The preconditions and risk-mitigating measures to use this unknown vulnerability were not clearly described in the request, which resulted in an unlawful conduct decision. When the service submitted a new request with changes and clarification, the TIB issued a lawfulness decision.

3.2.3 More room for manoeuvre when using unknown vulnerabilities?

The TIB is aware that the services need more room for manoeuvre when hacking, also where it concerns unknown vulnerabilities. In a hacking operation for which the TIB received an extension request in December 2022, the AIVD asked for room to exploit, in addition to the described unknown vulnerability, a 'similar unknown vulnerability' without prior review by the minister or the TIB. After questioning the precise interpretation of the term 'similar', the TIB had to establish that the requested room for manoeuvre was too great to ensure that the use would remain proportional. There were inadequate boundaries that could result in vulnerabilities with a significantly higher risks being labelled as similar. That was reason for the TIB to come to an unlawful conduct decision. The basic principle is still that the use of unknown vulnerabilities must be submitted to the minister and the TIB in advance. Administrative consultation was held about this topic afterwards.

3.3 Bulk data sets and determining relevance

Bulk data sets regularly occur in the services' investigations. Bulk data sets are large collections of data, the vast majority of which concern organizations and/or people who are not the subject of investigation by the services, nor ever will be. The services see long-term operational value in many bulk data sets. The ISS Act 2017 sets no specific rules regarding bulk data sets. That means that these bulk data sets fall under the same regime as 'separate' data. The ISS Act 2017 stipulates that all data obtained using special investigatory powers such as hacking, must be assessed for relevance as soon as possible. As soon as possible to prevent information that is not relevant being stored for longer than strictly necessary. The maximum retention period for data assessed to be irrelevant is 18 months. Only data declared relevant may be stored for longer.

For some time now, the TIB and the CTIVD have called attention to the issues regarding the current provisions of the ISS Act 2017. Over the past years, the services have sought all sorts of legal ways to be able to store the entire bulk data sets for longer. In some cases, bulk data sets have been declared relevant as a whole. In the CTIVD's opinion, that interpretation of relevance is unlawful, because in fact it bypasses the maximum retention period.

A non-binding unlawful conduct ruling about that course of events by the CTIVD's Oversight Department was swept aside by the minister.[8] The complaints procedure that was subsequently submitted to the CTIVD's complaints department ultimately resulted in a binding decision by the complaints handling department that the five bulk data sets in questions should be deleted and destroyed.[9] The government has now presented a draft bill addressing this issue and proposing a solution.[10]

In the requests that the TIB assessed in 2022, the issue of bulk data sets and the proposed data processing arises on a regular basis. In operations where the objective is to acquire a bulk data set, the TIB only issues a lawfulness decision if the request contains the safeguard that the relevance assessment will be conducted in a way deemed lawful by the CTIVD. That rules out the possibility of the services later declaring an acquired bulk data set relevant as a whole.

If a service wants to acquire the same, or partially the same, bulk data set periodically, the TIB expects additional safeguards in a request that prevent the non-examined data being stored in the same way for longer than 18 months. New information may be kept, but bulk data that has been in the services' possession for 18 months may not be acquired again or must be removed immediately after it was re-acquired.

In 2022, the MIVD intended strategic use of [redacted] and to acquire bulk data sets (register files) periodically. It is possible to sidestep the maximum retention period under Section 27 of the ISS Act 2017 by periodic acquisition. As stated above, the TIB expects additional safeguards for periodic acquisition. Data assessed as not relevant, must be deleted and destroyed after a new bulk data set is acquired, before the new set can be used again. The MIVD announced in the requests that it would apply a segregation of duties instead. That would mean that only appointed officers would be able to access the bulk data sets. That safeguard was to accommodate the data not being assessed for relevance and possibly being retained longer than 18 months because the sets could be re-acquired over and over. However, this procedure meant that the relevance assessment under Section 27 of the ISS Act 2017 would not in fact be made. Therefore, the TIB ruled the authorization granted to be unlawful because the law does not provide scope for this procedure.

One of the two MIVD operations was later considered lawful in redacted form. In a following extension request a key word had been changed, which raised questions with the TIB. It then appeared that the MIVD had described [redacted] in the manner described above (and ruled unlawful) [redacted]. The TIB had no alternative but to issue an unlawful conduct ruling again.

In another long-standing strategic hacking operation by both services, the TIB assessed several extension requests in 2022. Initially that operation was only conducted by the AIVD, but was later joined by the MIVD. In mid-2019, the AIVD obtained a bulk data set in this operation. Decisive factors for the lawfulness assessment at the time were the safeguards (commitments in the request) that the bulk data set would be used for a limited number of investigations and that data that was obviously not relevant for that limited number of investigations would be destroyed as soon as possible. Destroying data as soon as possible was referred to as *reduction* . To what remained of the data (in terms of size it was still a bulk data set), the regular legal regime applied. In other words, that set was to be assessed for relevance as soon as possible, but in any case within 18 months.

8 *Parliamentary Documents II* 2020/21, 29924, no. 203 appendix.
9 Decision regarding the complaint by Bits of Freedom about conduct by the AIVD and the MIVD, 15 June 2022.
10 The regulation was included in a memorandum of amendment, with which the draft bill was to have been amended. For more information, refer to chapter 5 of this annual report.

Later in 2022 (long after the 18-month term had expired) the TIB, when assessing a related request, questioned the AIVD about how the reduction had been carried out and how the relevance assessment had taken place. From the answers it appeared that the AIVD had interpreted reduction differently from what was indicated in the requests on which the authorizations had been based. The AIVD had interpreted one of the areas of investigation mentioned in the request much more broadly than the TIB had thought possible based on the description in that request. And so less data was covered by the reduction and more data continued to be stored. What's more, the reduction itself had only been carried out approximately 18 months after it had been acquired, due to staffing and technical restrictions. To sum up, the safeguards that had been decisive for the TIB's assessment had been stripped of its meaning.

After the reduction, the services declared the remaining data set[11] relevant in its entirety. In principle, as stated above, that is not automatically lawful. In this specific case, the CTIVD notified the services on 9 November 2022 that the way the relevance assessment had been carried out had been found lawful, given the special nature of the bulk data set and the specific, special circumstances of this case.

3.4 Strategic operations

A strategic hacking operation is an operation in which the services want to use the hacking power to obtain a strategic position. Previous annual reports have also addressed this fact. In those cases, the TIB gave a hypothetical example of an access position in a computer system, which in turn made it possible to view otherwise inaccessible communication, such as encrypted message exchanges. Nevertheless, it concerns hacking operations that are not primarily concerned with obtaining targets but with taking up a position that could be useful at a later stage in the investigation into a target.

The legislator did not express an opinion, when the ISS Act 2017 was drafted nor with the amendment of the Act on 14 July 2021, 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' (Section 28 of the ISS Act 2017). Nor do the explanatory notes to the draft bill contain a description of what the legislator deems admissible in this context.[12] The TIB has repeatedly asked the legislator to give its general opinion on the admissibility of the hacking power used purely on strategic grounds and what the framework for that use is. The services seek room for manoeuvre but is necessary to clarify where the borders lie for the proper execution of the services' tasks. At this time, the TIB continues to review these requests within its regular review framework.

11 Based on the check carried out on the presence of state secrets, the services remarked that the data set remaining after the reduction constituted only 2% of the entire data set. The suggestion was made to give this percentage. The TIB remarks that this percentage says nothing about the size, in absolute terms, of the remaining bulk data set that had been declared relevant in its entirety.

12 This is the draft bill for the implementation of interim measures governing AIVD and MIVD investigations into countries with an offensive cyber programme, *Parliamentary papers II* 2022-2023, 36 263. For more information, refer to chapter 5 of this annual report.

In 2022 also, the TIB received a number of requests in which the services intended to use the hacking power on purely strategic grounds. These concerned very far-reaching operations, which in a number of cases mainly invade the privacy of individuals who are not the focus of the services' attention and never will be. In 2022, the TIB issued both lawfulness and unlawful conduct decisions. A number of these operations are described in this section. In part for reasons of confidentiality, it is not always easy to indicate why a lawfulness decision was made in one case and an unlawful conduct decision in another, and in fact the operations can only be described in general terms anyway.

The TIB ruled the authorization granted in two of the services' operations unlawful, because the TIB did not consider the operation proportional. The services intended to hack a non-target and to then acquire the data from this non-target's [redacted]. It concerned a non-target with [redacted][13] The nature and amount of the data that the non-target [redacted] has can offer a penetrating view in the personal or business life of each of [redacted] . However, the services failed to clarify adequately whether and, if so, which limits would be used when acquiring this data.

A further unlawful conduct ruling was given for authorization granting both services to conduct a strategic operation on a non-target. It concerned a [redacted]. The services intended to hack the [redacted] of the non-target and to then acquire the data from the [redacted]. That data could in turn yield data from the [redacted]. It concerned sensitive personal data from potentially [redacted].[14] The TIB ruled the granted authorization to be unlawful because even the technical risks in the operation were too great. No new request was submitted in this operation.

The TIB did not rule all strategic hacking operations to be unlawful. The TIB issued a lawfulness ruling in a strategic hacking operation aimed at [redacted]. The service does have to conduct a relevance assessment and the [redacted] that the service rules as not relevant must be deleted immediately with each new acquisition. The service is permitted to take in and maintain a [redacted] for this [redacted]. The service is then able to access the data that the target organization places with and processes at the [redacted].

Another example of a strategic hacking operation ruled lawful in 2022 is a hack on a non-target, where the service was able to secretly obtain this non-target's [redacted] in bulk. The data was analysed by a limited number of officers. The investigation into this bulk data subsequently offered the service in question the possibility of acquiring data from as yet unknown targets.

13 The TIB wished to indicate the size of the non-target here.

14 The TIB wished to give an indication of the number of individuals that could be affected here.

In 2022, the minister granted the AIVD authorization to hack a bona fide non-target, in order to acquire a strategic position in the [redacted] of this non-target that could be used in the future. If a target of the service [redacted] in future, the AIVD would secretly be able to focus on the target through the non-target. The TIB determined in its assessment that the non-target was established in a [redacted]. The request had stated that cooperation could not be sought from the partner service in the country because this partner service [redacted] and had not yet obtained that authorization The TIB ruled the authorization granted to be unlawful because the proposed use was not proportional.

3.5 Information provision by the services

For its lawfulness assessment, the TIB is primarily dependent on the information contained in the requests. Because of the state secret nature of the operations, the TIB is unable to consult public sources, not least because interest from the TIB in a certain topic could reveal what the services are doing. Moreover, the TIB is unable to search the services' systems, unlike the CTIVD. The TIB only has access to the requests. The ISS Act 2017 does offer the TIB the possibility to question the ministers on the requests, and the TIB does so regularly. This is explained in further detail in section 4.1 In practice, these questions are addressed directly to the services and the TIB receives the reply from them. If the TIB feels that it cannot take a sound decision on a request because some matters are unclear or require further explanation, it can ask the services to hold a presentation about a specific operation or a certain topic. The TIB is regularly sent presentations on specific operations.

The past years have repeatedly shown that the information originally contained in the request was inadequate to come to a decision and that in some cases the information was even incorrect. At the time, meetings were held between the TIB and the management of the AIVD to improve the situation. In 2022, there were again instances where the AIVD provided inadequate information to the TIB. The TIB has no reason to believe this was intentional.

> "The past years have repeatedly shown that the information originally contained in the request was inadequate to come to a decision."

In a number of cases it was clearly an administrative error or a misunderstanding and not decisive for the review. The mistakes caused a lack of clarity on the part of the TIB and for that reason questions were then asked. That influenced the decision term somewhat, but in most cases not the decision ultimately to be taken.

In a few cases the incorrect information led to a ruling of unlawful conduct. That concerned an extension request. The request described as yield that thanks to the acquired data, the AIVD had been able to conduct an operational action on two targets. After enquiry that information proved to be incorrect. The AIVD had not conducted an operational action itself, but it had provided the evaluated data to a partner service. That partner service subsequently decided not to act and therefore did not carry out an operational action. There was no yield at all from the extended operation. In the opinion of the TIB, the authorization granted by the minister had been given based on a misrepresentation of the facts in an essential respect.

In a similar case where the TIB had questioned the minister, she withdrew her authorization. In that case, the only yield in a strategic operation had not been achieved within that operation but in a totally distinct operation aimed at an individual.

A further example was the intended use against an individual in the Netherlands. The request stated that he worked in an institution where confidential information was handled. An investigation needed to show if he was possibly working for a foreign intelligence service. The matters presented in the report as facts proved to be uncertain and it appeared that the person involved did not himself have a position involving confidentiality within the institution. The TIB ruled the authorization granted for this request to be unlawful, because there was insufficient necessity for the use based on the actual facts.

In none of the circumstances described above was there any evidence that the AIVD wilfully provided incomplete or inaccurate information to the TIB, but the provision of information continues to be a topic of debate between the AIVD and the TIB.

3.6 Capacity issues

Noticeable this year has been the fact that requests describe a lack of capacity to focus fully on targets/non-targets (individuals or organizations) or to process the yield. One hacking operation serves as an example in which the TIB, after further enquiry, was informed of the fact that data had been acquired in bulk in approximately a ten-month period, but that a start had not even been made to assess that data for relevance. One of the challenges proved to be the lack of capacity to translate the data. Because the TIB is not involved in how the services actually carry out their operations, the TIB in this case decided that the extension itself was lawful.

A second example is a strategic hacking operation of a non-target in another country, in which bulk data was acquired also. The law was pushed to its limits. However, extension requests revealed that the AIVD had to deal with scarce technical capacity. On enquiry during the review of the extension request, it became clear that the operation in question had been on hold for months and that there was no prospect of that situation changing soon. The TIB ruled that the necessity to extend that operation was thereby inadequately substantiated and in this case issued a unlawful conduct ruling.

There are further operations where the services indicated that no yield had been generated because of a capacity problem. For example, authorization was granted for a specific use, but that use was not carried out because of a lack of capacity. In addition, the TIB saw investigations in which, for example, telephone communication was intercepted, but where the yield could ultimately not be processed further because of a lack of capacity. In multiple occasions no action was taken due to either a lack or shortage of capacity (because of other working activities or in isolated cases due to holiday leave).

Section 29(2)(g) ISS Act 2017 stipulates that, where it concerns a request to extend authorization, the achieved results must be made known. The TIB will have to assess in part whether an extension is necessary and proportional, based on the yield. If the yield of the use of a means has not been detailed, this can be at odds with the necessity and proportionality. If the TIB considers an extension request to be lawful, it will generally add a comment in cases of this kind, which means that the TIB expects the yield to be detailed in a further extension or that a more specific substantiation is given for why the extension is necessary.

4. The lawfulness assessment in numbers

The number of requests submitted to the TIB in 2022 has fallen for the first time in its existence. As regards the requests by both services, the percentage of unlawful conduct decisions also fell in 2022. That can be explained in a number of ways that will be addressed in this chapter. As was the case last calendar year, the TIB sees an increase in the size and technical complexity of the requests. Remarkably, 2022 has seen a relative increase in the number of unlawful conduct decisions because the proposed operation was not proportional. The number of unlawful conduct decisions due to a lack of substantiation and information also rose.

Section 4.1 of this chapter presents an overall view of the requests. Section 4.2 looks in more detail at a number of repealed authorizations. Section 4.3 looks at the unlawful conduct decisions. In section 4.4 the use of the urgency procedure is discussed.

4.1 Overall view of the requests

This year the TIB assessed a total of 2,902 requests by both services combined. That is 5.8% fewer requests than last year. Where the number of requests by the AIVD fell in 2022 compared with the previous calendar year, the number of requests by the MIVD rose in 2022. [redacted]

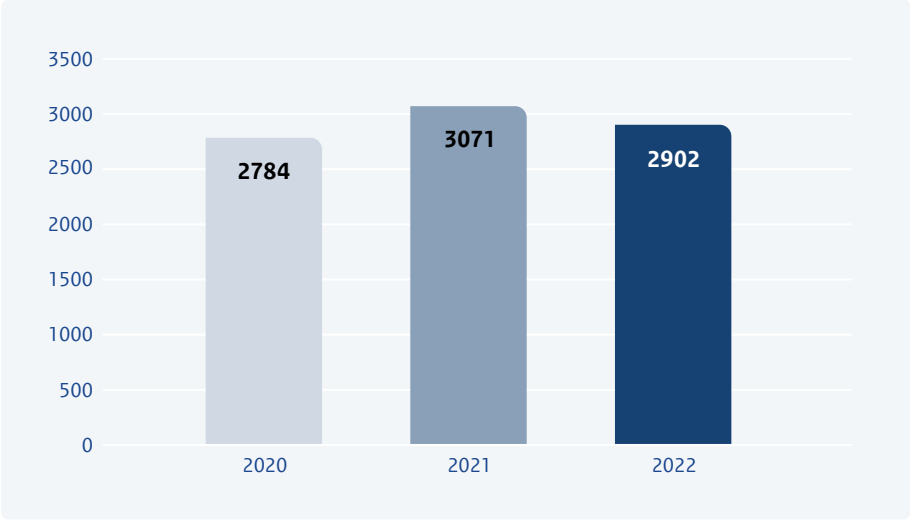
Table 1: a view of 2022 compared with 2021

Figures 2022 and 2021	2022	2021
Total number of reviewed requests	2,902	3,071
Number of requests in which questions were asked	366	383
Number of unlawful conduct decisions	67	119
Number of lawfulness decisions	2,835	2,952
Number of withdrawals (not included)	14	18
Number of urgency procedure requests	129	111

Of the 2,902 requests submitted in total, 67 were ruled unlawful by the TIB. The percentage of unlawful conduct decisions fell at both the AIVD and the MIVD. The decline was even greater at the MIVD. More on this in section 4.3.

It is striking that the TIB issued more unlawful conduct decisions than in the preceding year for failing to have been informed adequately or fully enough to take a proper decision. Finally, proportionality was the most frequent ground for the unlawful conduct decision in 2022, as was the case in the previous calendar year.

Figure 1: number of requests per calendar year



To provide a full overview, this annual report clearly shows how many requests the TIB has reviewed for lawfulness over the past three calendar years.[15] As described above, this shows that the number of requests decreased in 2022 compared with 2021.

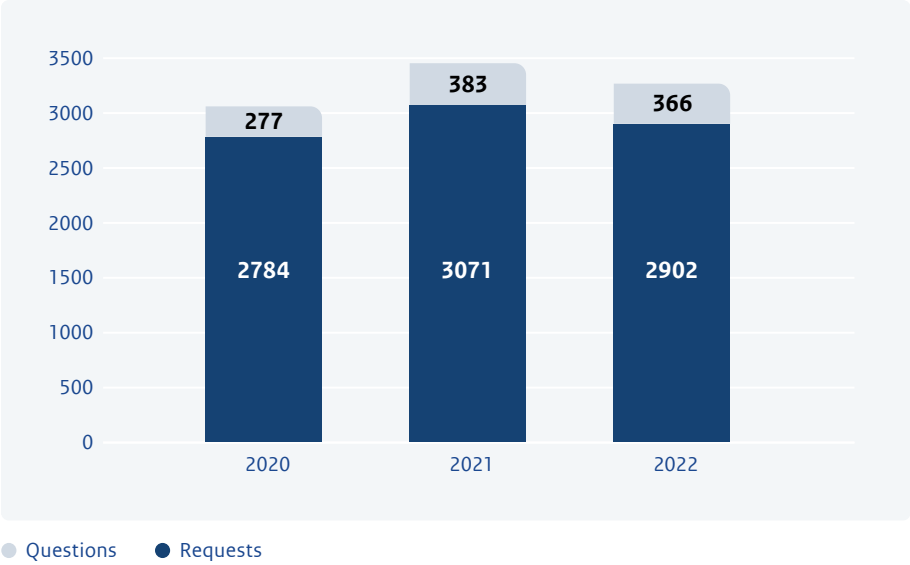
This section will list several percentages to clearly indicate the changes and similarities in the 2022 calendar year compared with the 2021 calendar year.

The graph below compares the calendar years 2020 to 2022. The graph shows a comparison of the total number of requests in a particular calendar year, with the total number of questions the TIB asked the services. In this calendar year, the TIB questioned the services in 366 requests (of the 2,902). In those cases therefore, the TIB did not issue a decision based solely on the contents of the request. Both the number of requests and the number of questions fell compared with 2021. Previously, both numbers had risen. Despite the decline in the number of questions asked, the TIB also issued fewer unlawful conduct decisions. More observations can be made from these figures if we look at the ratios.

15 The first year of review by the TIB ran from 1 May 2018, the day on which the ISS Act 2017 entered into force. The annual report at the time covered the period from 1 April to 1 April. In 2020 the TIB decided to report on calendar years starting from 2021. The report on 2020 was a transition year and covered 1 April to 1 January. The figures from the 2020 calendar year described in this annual report are not derived from previous annual reports but were later calculated by the TIB.

In 2022, the TIB questioned the AIVD in 11.5% of cases, before it could take a proper decision. In the previous reporting year, the TIB made fewer enquires from the AIVD, i.e. in 9.7% of the reviewed requests. The TIB questioned the MIVD in 17.2% of the reviewed requests in that reporting period. That percentage was almost the same compared with the preceding calendar year, in which the TIB questioned the MIVD in 17.9% of cases. For both services combined, the services were questioned in 12.6% of the requests first.

Figure 2: comparison per calendar year of the number of questions and the number of requests



What is interesting about this comparison is that in 2022, the TIB questioned the MIVD in far more requests than the AIVD, i.e. 17.2% compared with 11.5% of the requests. It is also striking that there is a rise in the number of questions asked of the AIVD in the 2022 calendar year compared with the preceding year, namely from 9.7% to 11.4%, whereas the number of questions asked of the MIVD show a slight decline in the 2022 calendar year compared with the preceding year, namely from 17.9% to 17.2%.

In this reporting period, the TIB ruled 2,835 requests in total to be lawful.

As explained briefly above, the TIB may also rule that a request is lawful and add a comment. In that comment, the service may be asked to address or otherwise explain or clarify a specific point in the request if and when it submits an extension for that request. In about 11% of the requests, the TIB added a content-related comment to its lawfulness decision. Unfortunately a comparison cannot be made with the previous calendar year because the number of lawfulness rulings with comments has not been specified before.

4.1.1 Exceptional cases

In once instance in 2022 a request appeared to show an investigatory power to be exercised against a press agency. The request involved the technical support when exercising the power of selection for a partner service. However, investigatory powers exercised against journalists may not be authorized by the minister but authorization must be granted by the Court of The Hague. The TIB therefore ruled the authorization granted to be unlawful. The MIVD later submitted a new request in which the selectors of the press agency had been removed. The TIB ruled that amended request to be lawful.

In 2022 the AIVD was granted authorization once for making what is known as [redacted]. The server was not used exclusively by the target organization [redacted]. To assess proportionality in particular, the TIB asked the service to [redacted]. The TIB asked if they had considered destroying [redacted] the data immediately after the initial acquisition of the entire server contents and only then subjecting the remaining data to the technical analysis. The service responded that they had contacted [redacted] about this and that it appeared that it was technically possible to [redacted] that would not contain [redacted] on the server, but [redacted] that was being abused by the actor and into which the service was conducting its investigation. With the safeguard that data including from [redacted] would not be copied, the TIB was ultimately able to rule the request lawful, because this special investigatory power was no longer to be exercised against a lawyer.

Most of the special investigatory powers that the services are permitted to exercise under the ISS Act 2017 have a legal maximum period of three months. Authorization for the use of the investigatory power may be extended by three months at a time. Many of the services' investigations run for longer than three months. Therefore the TIB regularly receives extension requests for operations running for longer. In particular, the TIB assesses the necessity for continuing the operation and its proportionality. The TIB also reviews the previous request, for example to check if the safeguards included in that request are still the case.

In an extension request for a longer running operation, the TIB found after consulting its systems, that no authorization request had been submitted in the preceding three months. The AIVD confirmed this after being questioned by the TIB on this. In accordance with procedures, the AIVD subsequently informed the CTIVD and started an internal investigation. The AIVD established that in this case and in a limited number of other operations, no authorization requests had been submitted due to human error.

4.2 Repealed authorizations

In a number of times this calendar year, as in previous years, the authorization for a request granted by the minister was repealed after the request had been submitted to the TIB for assessment, but before the TIB had issued a final decision. That happened before the TIB had issued its ruling on the lawfulness of the granted authorization. This year that occurred in fourteen requests. In the previous reporting period, it was eighteen requests. In relative terms, that amount has remained virtually the same, given the total number of requests.

The ISS Act 2017 does not explicitly regulate the repeal of the authorization of a request. It is the TIB's interpretation that repealing a granted authorization is possible and for that reason a written confirmation of the repealed authorization is sufficient in practice.

The granted authorization was repealed in six requests after the TIB had questioned the services. In some cases the TIB's questioning was given as specific reason for the repeal. One example of a request being repealed after questioning was an extension request in which the specific yield was asked for. That had not been specified for several periods, which put pressure on the necessity and proportionality of the extension. The extension request in this case did contain specific yield regarding foreign IMSI number. On questioning, it appeared that this yield was not from the operation in question, but from communication intercepted

from the target in question in another operation. The granted authorization for the request was repealed based on this question.

Other requests were repealed for other reasons, for example because of an administrative error or because an incorrect version of the request had been submitted to the minister or because of new information or new developments.

4.3 Trends in unlawful conduct decisions

In 2022, the TIB ruled that the authorization had been granted unlawfully for 2.1% of the requests by the AIVD. That was 3.3% in the previous reporting period. The MIVD saw a significant drop in the number of unlawful conduct rulings compared with the previous reporting period. In the previous reporting period the number of unlawful conduct rulings was 7.1% while the number of unlawful conduct decisions in the 2022 calendar year decreased to 3%.

A further noticeable change is that the number of unlawful conduct decisions in 2022 decreased, for requests by both the AIVD and the MIVD, but also that the total number of unlawful conduct decisions dropped significantly. Where 3.9% of the requests were ruled unlawful by the TIB in the 2021 calendar year, that was only 2.3% this year.

The main explanation is that the quality of the requests has improved further. Compared with previous years it is noticeable that the services have been able to improve that quality. This has had an unmistakeable effect on the number of unlawful conduct decisions. The TIB sees that improvement across the board for both services.

In part this can also be explained by the fact that in this calendar year, the MIVD partnered with the AIVD in a number of operations and awaited the TIB's assessment on the AIVD request before submitting its own request. On occasion the TIB ruled the authorization granted for an AIVD request unlawful, after which the request was amended and resubmitted. Once the TIB issued a lawfulness ruling, the MIVD request followed. An unlawful conduct ruling is always substantiated in writing and the TIB is aware that the services consult on the TIB's rulings. Furthermore the services themselves appear to take a strategic view to submitting requests. In, for example, cable requests to use broader leads (see section 3.1), the AIVD only submitted one request in which additional leeway was asked for and waited with other requests containing that same wish until the decision had been taken in the first case.

> "There can be a difference of opinion between the intention of the drafter and the interpretation of the reader."

Another explanation could be that the TIB asked more questions about AIVD requests. Looking at the last nine months of 2020 (the reporting period of the Annual Report TIB 2020), the AIVD was questioned in 8.9% of cases. That had risen to 9.7% in the 2021 calendar year and increased further to 11.4% in the 2022 calendar year. The TIB reviews on paper, therefore intention of the drafter and the interpretation of the reader may be seen differently. By clarifying the TIB's questions, the services managed to have fewer requests ruled unlawful.

Finally, the TIB notes that greater attention is paid in organization requests to a clear limitation or demarcation of organization, but also that in extension requests more attention is paid to a proper substantiation of individuals added and why extension of the use was sought. The assessment framework of the TIB and the CTIVD, which was shared with the services with the intention to indicate the points on which this type of request would be assessed in particular, seems to bearing fruit.

When a request to use a special investigatory power is assessed as unlawful, the service can opt to submit a new and amended request to the TIB. That new request could then be found lawful, for example because additional safeguards were attached to the use of the special investigatory power or if there is no longer an independent ground for an unlawful conduct ruling in the renewed request. In 61.2% of the requests initially ruled unlawful, renewed requests were submitted after the unlawful conduct ruling, which were ultimately assessed to be lawful in revised form. In the other 38.8% of cases, requests ruled to be unlawful by the TIB were either not resubmitted or were again ruled unlawful. When the requests are broken down into AIVD on the one hand and MIVD on the other, it is striking that in 76.5% of the unlawful conduct decisions, the MIVD submitted a renewed request, while the AIVD only did so in 56% of the cases.

Compared with 2021, the percentage of resubmitted requests following an unlawful conduct ruling by the TIB decreased slightly. Where 67.2% of the requests initially ruled unlawful by the TIB were resubmitted in the 2021 calendar year, that was only 61.2% this year.

The figure below shows the reasons for the TIB to issue its unlawful conduct rulings in 2022.

The figure relates to both the AIVD and the MIVD. A ruling of unlawful conduct can be taken on more than one ground. For example, the TIB may rule that the use of the special investigatory power is not proportional, but also that the necessity has not been adequately substantiated. That same request is thus included in both grounds in the below figure. The figures are shown in absolute numbers.

Figure 3: reasons for unlawful conduct decisions in 2022, numbers in absolute cases

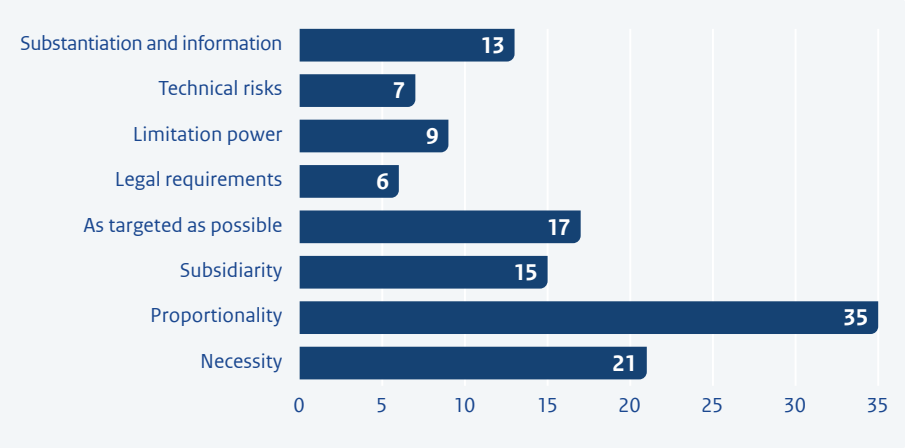
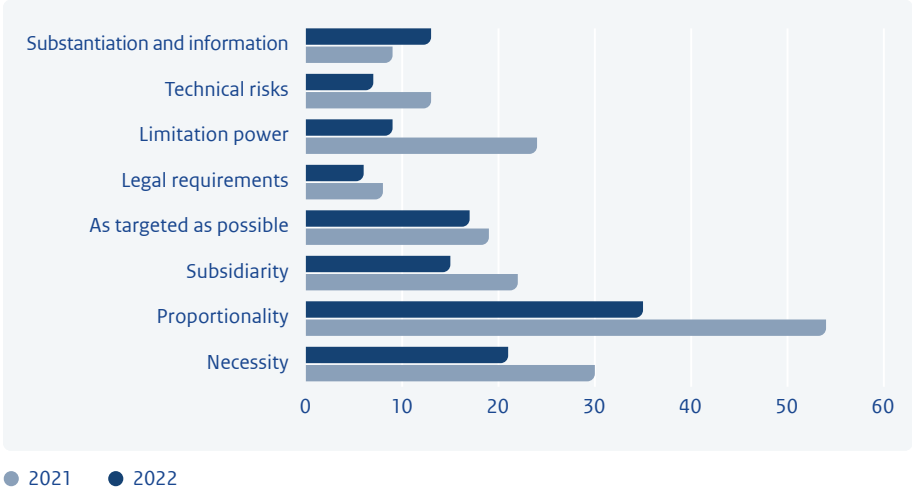


Figure 4: reasons for unlawful conduct rulings



The figures above give a clear picture of the independent grounds for the unlawful conduct decisions in the 2022 calendar year compared with the 2021 calendar year.

That requires some explanation. Where at first glance it might seem like a change for the better regarding proportionality, that view is skewed. Despite the fact that unlawful conduct decisions because of proportionality were given in only 35 cases in 2022, compared with 54 cases in 2021, in terms of percentage, that actually means an increase in unlawful conduct because of proportionality. Of the unlawful conduct decisions in 2021, 45.4% were ruled unlawful in part because of proportionality, while that percentage was 52.2% in 2022. It is not immediately apparent what caused this increase.

The most striking is a significant increase in the number of unlawful conduct decisions because of a lack of substantiation or information. Where 7.6% of unlawful conduct decisions in 2021 were partly because of the lack of substantiation or correct information, that had risen to 19.4% of unlawful conduct decisions in 2022. That ground means that the substantiation was inadequate or lacking and/or the information shared was inadequate or incorrect. One explanation for this increase could be that the TIB had decided that the lack could not be remedied, even after further questioning.

Furthermore it is striking that it is still relatively rare for granted authorization to be deemed unlawful because the technical risks were too great or because it did not comply with a legal requirement.

4.4 Assessment of the urgency procedure

Section 37 of the ISS Act 2017 includes a procedure for urgent cases. In an urgency procedure, the special investigatory power may be exercised before the lawfulness assessment by the TIB has taken place. This may only be done if the regular procedure cannot be awaited and if immediate action is required. However, even in urgent cases, the minister must first grant authorization. The granted authorization must then be submitted to the TIB for a lawfulness assessment as soon as possible. The TIB must be informed of the reasons for the urgency. That means that the TIB must be informed of all the facts and circumstances that are important to assess the urgency request.

When assessing an urgency request, the TIB must therefore also assess whether the situation calls for the lawful use of the urgency procedure.

If the urgency procedure was used wrongly, the TIB must subsequently determine what should be done with the obtained information. An unlawfully invoked urgency procedure does not necessarily mean that consequences will be attached to that unlawful conduct. Each time the matter must be considered anew, depending on the circumstances of the specific case. In addition to the urgency procedure, the TIB must assess the authorization granted for the use. If the TIB rules the urgency procedure unlawful, but the granted authorization and thereby the use of the investigatory power to be lawful, the TIB may be of the opinion that the data obtained by the exercise of the investigatory power, should be destroyed immediately. That did not happen in 2022. Given the circumstances, in a situation such as this, no consequences are generally attached to the unlawful urgency procedure and that establishing that the conduct was unlawful is enough.

If the urgency procedure was lawfully invoked but the granted authorization to exercise the investigatory power was not, then the data obtained through that exercised investigatory power must in all cases be destroyed immediately.

During the reporting period, the services invoked the urgency procedure a total of 119 times. That is in 4.5% of the total number of requests in 2022 compared with 3.6% in 2021. As in the previous reporting period, the TIB ruled that in 2022 the services had not invoked the urgency procedure lawfully in all cases.

4.4.1 Unlawful urgency procedure

Where in 2020 the TIB had ruled that the services had in all cases invoked the urgency procedure lawfully and that the authorization to use the investigatory powers had been granted lawfully each time, that had changed in the 2021 calendar year, as briefly noted above. In that year, the TIB ruled that the urgency procedure had been invoked unlawfully six times and that in four requests the use of investigatory power in itself had been unlawful.

In absolute terms, the number of unlawful conduct decisions was the same in the 2022 calendar year, namely six cases. However, it should be remarked that in 2022 the urgency procedure was applied in more varying operations than in 2021, which means that in the current calendar year the number of urgency procedures found to be unlawful declined slightly.

The TIB questioned the AIVD about the invoked urgency procedure in nineteen requests. In six of those, the TIB ultimately ruled that the use of the urgency procedure had been unlawful and that the regular procedure should have been followed. One reason was that, for example, there had been more than sufficient time to have the TIB assess an authorization granted by the minister, without the need to invoke the urgency procedure. In another instance, the TIB established that the urgency procedure had been invoked because the information on which action was to be taken had stalled because a coordinator was away on an official trip. This was purely an organizational matter and not an independent reason to exercise an investigatory power without prior assessment by the TIB.

The TIB ruled in all cases that no consequences should be attached to this unlawful conduct, because the operational necessity and facts and circumstances of those particular cases did not warrant that.

Based on the contents of the requests, the TIB further established that the services did not invoke the urgency procedure at weekends any one time.

What stands out in positive terms, is that the TIB assessed the use of the special investigatory power itself to be lawful in all cases.

4.4.2 The investigatory powers covered by the urgency procedure

As discussed above, the services invoked the urgency procedure 119 times in the 2022 reporting period. The services may invoke the urgency procedure for each of the special investigatory powers requiring a TIB assessment.[16]

[redacted]

Striking is the fundamental difference between the AIVD and the MIVD in terms of the investigatory powers covered by the use of the urgency procedure.

[redacted]

16 The blacked-out section contains an overview of the number of different investigatory powers covered by the urgency procedure. The TIB is aware that providing numbers broken down into investigatory powers has, in recent years, been designated state secret. However, the TIB felt it warranted to give a breakdown of the numbers here because it only relates to the use of the urgency procedure, and therefore does not give a representative account of the use of investigatory powers in all requests.

5. Draft bill for the implementation of interim measures

On 8 December 2022, the draft bill for the implementation of interim measures governing AIVD and MIVD investigations into countries with an offensive cyber programme was submitted to the House of Representatives (hereinafter: draft bill).[17] This is a draft bill that temporarily extends the services' investigatory powers to allow them greater scope in investigating countries with an offensive cyber programme. The decision was made to lay this extension of investigatory powers down in a single, separate, temporary act. The ISS Act 2017 itself will not be amended. At the same time that this bill was submitted, a memorandum of amendment (hereinafter: the memorandum) was announced. The memorandum supplements the draft bill with two regulations: a prior, binding assessment by the TIB of the use of the 'stomme tap'[18] (real-time traffic and location data interception) and an extension of the legal regulations on bulk data sets and determining relevance in Section 27 of the ISS Act 2017.

The TIB received the first draft of the bill at the end of 2021. The intention at the time was for an emergency act, which was to come into effect several months later. However, things turned out differently. The first version included elements that the TIB considered incompatible with the principles of an effective and adequate system of oversight. For that reason, various meetings were held in the first months of 2022 to discuss the subsequent drafts of the bill. Talks were held with civil servants of the departments and with the ministers and the chairpersons of the TIB and the CTIVD. Those talks resulted in major amendments to the contents of the draft bill.

The amended draft bill was made available in April 2022 for consultation and thereby made public. In outline, the consultation version of the draft bill comes down to an extension of the services' investigatory powers in investigations into cyber actors and to the use of those investigatory powers no longer needing to be assessed by the TIB in advance, but during or after the use by the CTIVD. The expansion of powers is far-reaching. Although the draft bill formally only pertains to countries with an offensive cyber programme, in practice it will also affect other investigations. The TIB envisaged that data acquired in a cyber investigation will also be available for the service's other investigations. Lowering the bar for a bulk hack[19] when it comes

17 *Parliamentary papers II* 2022-2023, 36 263.

18 A 'stomme tap' is the exclusive interception of real-time traffic and location data. It is possible to see who is being called and where that person is at the time, but the conversation itself is not intercepted.

19 A bulk hack is a hack intended to acquire a bulk data set.

to a cyber investigation also means that the acquired data from the bulk data set can become more widely available within the service. That lower bar will then apply to non-cyber investigations as well. In addition to these extensions, the bill also provides for the option the services will have to appeal to the Administrative Jurisdiction Division of the Council of State against decisions by the TIB or the CTIVD.

In its public response to the consultation version[20], the TIB began by stating that it would not express an opinion on the necessity of the proposed extensions, as this was a political issue. The TIB then outlined what the consequences would be of the regulations included in the draft bill and went on to comment mainly on the possibility to continue its oversight activities adequately. In the current situation, there is an independent obligation to describe the technical risks in a request. That independent obligation will cease to apply, which raises the question whether an adequate assessment is even possible. Firstly an important aspect is that the CTIVD, unlike now, will be given binding powers to assess the technical and other risks during the exercise of the operation.

Furthermore, the TIB stated, based on the consultation version of the draft bill, that it presumes that its proportionality assessment would *not* be restricted by the proposed changes, therefore not even if the requirement to describe the technical risks in the request is deleted. These technical risks are part of the proportionality assessment. In order to make that assessment, these risks need to be described and failing that, the TIB may always ask for a description. For that reason the TIB works on the assumption that the draft bill, as it was in the consultation phase, would not affect the proportionality assessment. The draft bill specifies various aspects that the TIB must include in its assessment of cable interception. The TIB already includes the elements described in its assessment. The proposed article does not restrict the inclusion of other aspects and therefore the TIB saw no restriction in its assessment here either.

The TIB stated that it could not agree with the proposed information exchange restricted by clause between the TIB and the CTIVD. This clause meant that if the TIB wanted to give the CTIVD points for attention relevant for the oversight, those points had to be reported to the minister at the same time and the head of service had to be informed in advance. That was unacceptable to the TIB. In the TIB's view, a free exchange of information is essential to carry out the oversight in the context of the draft bill, because the CTIVD would also take over a part of the oversight activities (for example the technical risks during an operation).

All in all, the TIB considered the draft bill as it was at the time of the consultation made oversight possible under conditions. In addition to a substantive response to the draft bill itself, the TIB made use of the possibility to call attention to the 'stomme tap'. Based on a ruling by the Court of Justice of the European Union of 6 October 2020, the real-time interception of telecommunications data (location data) requires a binding assessment by an independent body. That does not exist.

After the consultation phase, the draft bill was amended and submitted for an advisory opinion to the Advisory Division of the Council of State. The Council of State published its advisory opinion on 27 June 2022. The chairpersons of the TIB and the CTIVD sent a letter to the ministers in September 2022, with the TIB again calling to address the issues around the 'stomme tap'. That was not resolved in the draft bill as sent to the Council of State, but postponed until the general review of the ISS Act 2017. The CTIVD called attention to an adequate regulation for bulk data sets, because the draft bill would not resolve all the issues surrounding bulk data sets, although it was necessary to do so.

20 Response to the draft bill for the implementation of interim measures governing AIVD and MIVD investigations into countries with an offensive cyber programme.

The draft bill was presented to the House of Representatives in December 2022. In the final draft bill, the obligation to inform the minister and the head of service has been deleted, so that the free exchange of information between the TIB and the CTIVD becomes possible under this new draft bill. Expansion of capacity was provided for in a timely fashion. The issues of the 'stomme tap' and bulk data sets will be addressed in the draft bill through the memorandum of amendment.

Furthermore, amendments were made to the regulations concerning the technical risks and the assessment of cable interception. The TIB has already informed the minister of Internal Affairs and Kingdom Relations and the minister of Defence that the amendments made can be interpreted as a restriction of the TIB's proportionality assessment.

The further course of the draft bill and the memorandum fall outside the scope of this annual report. It only intends to mention briefly what the situation is at the time of publishing. The draft bill is up before the House of Representatives and its debate is being prepared. As far as the TIB is aware, the memorandum of amendment has not yet been submitted for an advisory opinion to the Advisory Division of the Council of State. The TIB's response to this memorandum can be read on our website. Whether the draft bill will become final, which form the bill will take and when it will enter into force is as yet unclear.

The House of Representatives is expected to be informed in the first half of 2023 about the government's plans regarding the general review of the ISS Act 2017. An outline memorandum is currently being developed that describes those plans.

"The TIB has already informed the minister of Internal Affairs and Kingdom Relations and the minister of Defence that the amendments made can be interpreted as a restriction of the TIB's proportionality assessment."

Composition of the TIB

As of 1 April 2023, the members of the TIB are:

- Ms A.M. Zwaneveld *chairperson*
- Mr E.H.M. Druijf *member*
- Mr O.A. Vermeulen *technical member*

Mr S.M. van der Schenk, senior judge at the Court of The Hague and Mr J. Piena, justice of the Court of Appeal in Amsterdam were appointed as deputies. These deputies may be called up if one of the members is unable to be present due to illness or leave.

The TIB is supported by a secretariat. The TIB's general secretary, Mr L.W. Schroijen, leads the secretariat. The secretariat was expanded with legal and technical advisers in 2022. In part, this expansion was in preparation for interim measures in the context of dynamic oversight, requiring closer consultation with the CTIVD and with a view to possibly introducing the option to appeal.

Toetsingscommissie
Inzet Bevoegdheden