Annual Report TIB 2023

Toetsingscommissie
Inzet Bevoegdheden

This annual report has a classified appendix which 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 of the House of Representatives. The classified appendix discusses some topics in more detail, including cable interception and strategic hacking operations.

Preface

On 1 April 2023, I started my work as the new chairperson of the TIB. My predecessor, committee members and staff members have built a solid foundation over the past few years.

I hereby want to pay a heartfelt compliment for that.

During my introductory period, I was happy to see that both services, the AIVD and MIVD, are strongly committed to our national security and our democratic rule of law . This was also reflected in the volume of work for the TIB. In the past year, the TIB reviewed about 3,400 requests, almost 500 more than the year before that. This marks a significant increase and I believe it shows the strength and commitment of the services. The TIB assessed the proposed use of all powers as lawful in over 95% of cases. So this was different in just under 5% of cases. Of these latter cases though, a significant proportion, about half, were still assessed as lawful after the request had been amended. I believe these figures reflect a level of maturity on everyone's part.

After all, strong services should go hand in hand with a robust review committee.

There have been many geopolitical developments over the past year, with the ongoing war in Ukraine and the attack in Israel and subsequent war in Gaza being the most prominent current events. This was also reflected in the requests submitted to the TIB. In addition, the services focused on criminal subversion, Russia and China, radicalism, Islamic terrorism, right-wing terrorism, anti-institutional extremism, espionage, the Caribbean, unwanted foreign interference and economic security, industrial security, cyber threat, and counter-proliferation and military technology, as shown by the requests submitted.

In the Netherlands, both the House of Representatives and the Senate debated on the Interim Measures Act, targeting countries with offensive cyber programmes, bulk data sets and other specific provisions. This means that a new and complex section will be added to an already complex act, the Intelligence and Security Services Act 2017. Society and politics can hardly keep up with it. In particular, it is not easy to explain the ratio between the far-reaching powers the services already have and the powers that will be added when the Interim Measures Act comes into force. Moreover, it is not clear at this stage what the full implications for the TIB will be. The services will be able to submit unlawful conduct decisions on the subjects covered by the Interim Measures Act to the Administrative Jurisdiction Division of the Council of State by filing a notice of appeal. Needless to say, the TIB is preparing for possible proceedings.

In 2023, the TIB remained in dialogue with both services on the issues on which the TIB has (partly) different views. These include, for example, the necessity and extent of infringements of fundamental rights. Other examples include a description of the planned use of powers to assess technical risks in hacking operations, and the proportionality of intercepting a large number of customer channels on the cable. This leads to a better understanding of everyone's position and also to positive results. In addition, TIB staff contribute to the services' internal training, with the aim of improving the legal quality of requests submitted.

An outline memorandum was published last year with a view to the longer-term future of the Intelligence and Security Services Act, also addressing the organization of review and oversight in the future. The coming years will see further consultation on this topic.

In short, there is still a lot of work to be done. I look forward to the coming period!

Anne Mieke Zwaneveld
Chairperson of the TIB

Summary

For the TIB, the year 2023 was all about the balance between protection and infringement of fundamental rights. That balance was at the heart of the 3,383 requests assessed by the TIB in 2023. This marked a sharp increase (16.6%) from the 2,902 requests assessed in 2022.

In 95.6% of cases, the use of powers was assessed as lawful. This was not the case for the remaining 4.4%. The percentage of unlawful conduct decisions increased slightly compared to last year. For half of the unlawful conduct decisions, the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) submitted an amended request, which was subsequently assessed as lawful.

More and more requests lack the information required to reach a decision on lawfulness. Requests from the AIVD appear to be less complete compared to previous years. During the year, the TIB brought this issue to the attention of the Minister of the Interior and Kingdom Relations and the service management of the AIVD in particular.

Another observation is that the TIB more often issued an unlawful conduct decision due to the service's failure to provide sufficient grounds and/or demonstrate the need for using a special power. It is also notable that services are increasingly invoking the urgency procedure. The TIB was also asked weekly to prioritise a proportion of requests (11.8%). These requests came from the AIVD.

In 2023, the TIB assessed several requests regarding snapshotting, i.e. the acquisition of snapshots of data through cable interception. The requests were assessed as both lawful and unlawful. The main issue in all decisions was the balance between the amount of data to be acquired and its potential use on the one hand, and the requirements of proportionality and the 'as targeted as possible' criterion on the other.

The TIB also reviewed several requests related to the acquisition of bulk data sets and the intended method to assess their relevance. The TIB issued a lawfulness decision only if the request included the assurance that the relevance assessment would be carried out in a manner deemed lawful by the Intelligence and Security Services Review Committee (CTIVD). This rules out the possibility of the services later declaring an acquired bulk data set relevant as a whole.

In the first quarter, a number of hacking operations were assessed as unlawful due to the fact that insufficient information was provided to the TIB on the associated technical risks. Following discussions, this reporting year the services adopted a (new) framework for describing technical risks. This framework has become part of these requests.

As in previous years, the TIB received several requests for assessment in which the services intended to use the hacking power on purely strategic grounds, i.e. purely in order to obtain a position with a view to the future. Two requests that were assessed as lawful will be discussed.

During the year, the TIB formulated further principles in the assessment of requests. The TIB communicated these principles to the services during consultations and in decisions as they pertain to recurring issues.

It is also worth mentioning that the 'stomme tap review' agreement came into force on 1 October 2023. This is a prior review before the real-time acquisition of communication and location data of users of a telecommunications service. The TIB has assessed such requests since then.

Last year also saw several developments on the 'Act on the implementation of interim measures governing AIVD and MIVD investigations into countries with offensive cyber programmes, bulk data sets and other provisions' (hereinafter also referred to as the 'Interim Measures Act'). The Interim Measures Act has resulted in a substantial extension of the powers of the services. For some powers, oversight shifts from structural binding oversight by the TIB prior to the use of the power, to the possibility of

binding ex-post oversight by the CTIVD. The Act also creates an option for services to appeal a decision of the TIB to the Council of State. The Interim Measures Act is expected to enter into force in the summer of 2024. Needless to say, the TIB is preparing for this.

Contents

1. Organization, procedures and composition of the TIB

1.1 What is the TIB

The Netherlands has two intelligence and security services: the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD). Both have far-reaching investigatory powers in order to conduct their work. For example, they are permitted to intercept communications from citizens, wiretap telephones, search homes and conduct DNA tests. They are also allowed to hack computers or computer systems, not only among targets of the services, but also among or through third parties. The services are also authorised to intercept telecommunications via satellite or cable on a large scale. These investigatory powers may not be used at will. The use of powers that constitute a significant invasion of citizens' privacy requires the minister's authorization. When it comes to some of these powers, the TIB must review whether the minister's authorization for that use was lawfully given. Only then can those powers be used. Oversight is then conducted on how those powers were exercised. Review and oversight of the services are carried out by two bodies: the Investigatory Powers Commission (TIB) and the Intelligence and Security Services Review Committee (CTIVD). The TIB is tasked with prior review, the CTIVD with oversight during and after the fact.

'A prior binding review by the TIB is in line with European case law'

With the entry into force of the Intelligence and Security Services Act 2017 (hereinafter also referred to as 'the ISS Act'), the services have been granted more powers. The TIB was established at that time. This chapter describes the TIB's tasks, as well as its procedures and composition.

1.2 Mandate of the TIB

The TIB is charged with conducting prior reviews of the lawful use of some far-reaching powers by the services. 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 for the use of certain special powers in a lawful manner. The TIB's decision is binding. This means that if the TIB rules that an authorization granted by the minister is unlawful, that power may not be used and the authorization granted lapses by operation of law. For the sake of readability, we will refer to reviewing requests or assessing requests as lawful or unlawful instead of reviewing the authorization granted by the minister for a request.

The introduction of a prior binding review body is wholly in line with European case law on oversight of the conduct of 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. To this end, states can use certain resources and techniques to intercept private communications. It is important however to provide adequate and effective safeguards against abuse. The European Court of Human Rights and the Court of Justice of the European Union have ruled on several occasions that services may use the most

far-reaching measures only after obtaining prior permission from a body that is independent of the executive power. In the Netherlands, the TIB fulfils that role.

1.3 Procedures of the TIB

The tasks and procedures of the TIB are set out in Section 32(2) of the ISS Act 2017. Requests to use powers should contain sufficient information about the investigation for which the power is to be exercised and the intended purpose.

The TIB assesses requests on the basis of five statutory criteria.

1. Is it **necessary** to use the special power? A request must justify why it is necessary at this time to use the special power.
2. Is it **proportional** to use the special power? In other words, does the importance of the investigatory power to be used outweigh the invasion of privacy that the use will bring? The TIB not only looks at the intrusion on the individual who is the subject of the investigation, but also at the invasion of the privacy of all individuals or organizations (or the individuals considered to be part of an organization) who will be affected by the use.
3. Is the **subsidiarity** requirement met? Is the lightest means used to obtain the required information? Subsidiarity implies that the service selects the least onerous power that can lead to the desired objective.
4. Is the use of the special power as **targeted** as possible? This means that the investigatory power should not be used more widely than strictly necessary. This criterion has been part of Section 26(5) of the ISS Act 2017 since 14 July 2021. The criterion was already applied before that time and had been laid down in a policy rule.
5. Does the request meet all the **formal requirements** of the ISS Act 2017? This means, among other things, that the user of the hacking power must also explicitly define the technical characteristic of the automated system and the technical risks. In addition, any extension request must include an indication of the results achieved, the 'yield'.

The TIB conducts its reviews 52 weeks a year. Every week, the TIB receives requests from the services for which the relevant minister has granted authorization. The TIB receives these requests at the beginning of the working week. The requests are prepared in terms of their contents by the TIB's administrative services department. Every Wednesday and Friday, the chairperson and members of the TIB meet to study the requests and preparations and give an opinion on the lawfulness of the authorization granted by the minister. The TIB aims to process all requests by the end of the week, by formulating an opinion or by asking questions to the service concerned (in which case no decision can be made at that point). Questions are asked when the TIB has insufficient information to give an opinion or when there is uncertainty about the safeguards to be applied. In exceptional cases, the TIB may take more time to consider the matter.

1.4 Initial and extension requests

The TIB receives both initial requests and extension requests from the services. An initial request is for authorization to use a special power for the first time with respect to 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 the use of powers, usually for another three months. In the extension request, the service must show the most recent results achieved, based on which the TIB can assess if continuation of the use is (still) necessary and proportional. On occasion, an extension request seeks to expand the initial request, in the sense that authorization is requested for a broader use of the investigatory power against more targets or third parties or based on more technical characteristics.

If the TIB decides that the granted authorization is lawful, that decision will be communicated to the relevant minister and service by digital means as soon as possible, almost always on the same day. The service may exercise the requested investigatory power from that moment on.

The TIB may also add a comment 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 decides that the minister has not lawfully granted the authorization, it informs the minister and the service in a substantiated written decision, including by digital means. Such a decision 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. Incidentally, an unlawful conduct decision does not preclude the submission of a new, amended request by which the unlawfulness could be removed, for example by adding additional safeguards.

Requests for a special power to be used against a journalist or lawyer are not submitted to the TIB. Only the District Court of The Hague can grant authorization for such powers at the minister's request. This is provided for in Section 30(2) and (3) of the ISS Act 2017.

1.5 Urgent requests

Section 37 of the ISS Act 2017 states that in the case of immediate urgency, an investigatory power may already be exercised before the minister's authorization is submitted to the TIB. However, the minister must always grant authorization (e.g. verbal authorization) first, even in urgent cases. After that, the urgent request should still be submitted in detail, and as soon as possible, to the minister and then to the TIB for a lawfulness assessment. 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 relevant to the assessment of the urgency request. It is important to keep this period as short as possible because an urgency procedure involves the use of powers – and thus infringes on people's fundamental rights – before a factual lawfulness assessment has taken place. In several operations, the TIB has provided a framework for the time limit for the use of the urgency procedure. A situation can only qualify as urgent if something is going to take place within seven days. The seven-day period starts when the service becomes aware of a situation that requires the use of a power. This period ends when the power must actually be used. If more than seven days elapse between the start and end of this period, but the urgency procedure is still invoked, the TIB will, in principle, assess the application of the urgency procedure as unlawful. With the TIB being available for review at least twice a week, it should be possible for the services to submit requests for all other cases in accordance with the regular procedure. Similarly, if, for example, the TIB is presented with a request on Thursday that needs to be assessed as a priority, it will give its opinion the next day.

In those cases where the urgency procedure has been used, the TIB has to assess not only the lawfulness of the use of the special power in question but also whether the urgency procedure was rightly invoked. When it comes to these requests, the TIB first assesses the authorization granted to use the special power. The TIB then has to assess whether it was justified to claim immediate urgency and that there was not enough time to follow the regular procedure.

If the TIB considers the authorisation granted lawful but the urgency procedure unlawful, the TIB may indicate that the data collected in the exercise of the power should be destroyed immediately. This rarely occurs; usually the TIB deems the mere finding of unlawfulness to be sufficient. If the authorization granted to use the power is assessed as unlawful, the data collected in the exercise of the power should be destroyed immediately. After that, the urgency procedure no longer needs to be assessed.

1.6 Priority requests

The TIB is regularly asked by email to prioritize one or more requests. While this possibility is not explicitly regulated in the ISS Act 2017, the TIB does cooperate in these cases. Priority is requested, for example, when an operational opportunity arises in the short term or when, in the case of an extension of the use, the authorization period for the preceding request has already or almost expired.

1.7 Withdrawn requests

The services may also decide to withdraw a request. They may do so if the lawfulness of the authorization granted has not yet been assessed by the TIB. The ISS Act 2017 does not explicitly regulate the withdrawal of authorization granted for a request. The TIB assumes that the withdrawal of authorization granted is not excluded by law. Therefore, in practice, it is sufficient for written confirmation of the withdrawal to be given by or on behalf of the ministers, which is then processed administratively.

1.8 Principles applied in decision-making

In 2023, the TIB outlined the principles adopted in relation to specific topics. The TIB subsequently informed the services of this in various ways, such as in decisions and consultations but also in comments contained in its lawfulness decisions. The TIB wished to communicate these principles to the services as they pertain to recurring issues.

1.8.1 Stating the correct legal basis

Since 25 July 2022, the TIB has added comments in its lawfulness decisions on requests involving multiple operations in accordance with Section 45 of the ISS Act 2017 to draw attention to the need to state the correct legal basis. This would include, for example, mention of both subsections (a) and (b) of Section 45(1) of the ISS Act 2017 when a particular hacking power is used. In those comments, the TIB expressed the expectation that the correct legal basis would be stated from 1 August 2022 onwards. Since that date, the TIB has issued unlawfulness decisions in all cases where the correct legal basis was not mentioned. In 2023 this still went wrong on one occasion and the TIB reiterated this expectation in an unlawfulness decision.

1.8.2 Proportionality assessment with regard to targets

The TIB found that, increasingly, the proportionality assessment in the requests was in fact a repetition of the justification of the need for use of a power. In the justification, the conclusion was that the use of the chosen means was necessary and, hence, that is was proportionate, with no consideration being given to the degree of invasion of the target's privacy.

In commenting on a lawfulness decision, the TIB explained that the proportionality assessment has led to questions being raised, or an unlawful conduct decision being issued, in several requests from different teams of the services in the recent period. The TIB has indicated that the proportionality assessment should cover two aspects: on the one hand, the necessity of the use of the special power against the target or non-target and, on the other hand, the invasion of the privacy of the target (and of their contacts or the persons close to them) as a result of the use of the special power. Both aspects should be addressed in the proportionality assessment. The TIB subsequently drew specific attention to this, saying that requests in which the proportionality assessment does not (or not sufficiently) demonstrate a weighing of necessity on the one hand and the invasion of privacy on the other, will in principle lead to an unlawfulness decision from 1 October 2023 onwards.

1.8.3 Strengthened proportionality test with regard to non-targets

A special power can only be used against a non-target if the minister has explicitly considered and described the strengthened proportionality test. A non-target is a person or organization close to the target against whom or which a special power is used in order to gain insight into the target through this person or organization. A non-target itself is therefore not the subject of an investigation by the AIVD or MIVD. The bar for the proportionality assessment is set higher when it comes to non-targets. It is assessed whether, in the specific case, operational interests outweigh the interests of the individuals or organizations whose information appears in the data. Overriding operational interests may include situations where there are one or more concrete indications of an immediate threat to

national security. The exercise of the power must not cause disproportionate harm to these persons or organizations in relation to the purpose of the power. The TIB found that it increasingly had to read up on the strengthened proportionality test for non-targets itself.

The TIB explicitly called attention to the strengthened proportionality test and indicated that from 1 December 2023 onwards, any requests in which that test is required but is not described or not adequately described would, in principle, lead to an unlawful conduct decision.

1.8.4 Information about the identity of victims

With some regularity, the services find out that victim data, e.g. personal data, have been acquired by a target of the AIVD or MIVD. They observe this, for example, when a special power is used against a target. Those victim data then end up in the systems of the AIVD and/or MIVD. In those cases, the TIB expects to be informed of the identity of those victims. In any case, Dutch victims and victims that have a direct or indirect relationship to the Netherlands should be named, obviously insofar as their identity is known. If the identity of a victim is unknown but the information made available by the use of the power reveals the sector in which the victim is operating, that sector should be mentioned.

The TIB takes this line because the nature and scope of the personal and other data acquired through the use of special powers by the services are taken into account in the proportionality test.

1.9 Knowledge sharing, information for the general public and letters from citizens

The TIB sees added value in discussing issues beyond the boundaries of its own organization. It believes that this contributes to the proper functioning of the system.

The TIB is in regular contact with the services about the decisions made, of course. If requested, the TIB will explain these decisions orally on a case-by-case basis. Staff from the services periodically visit the TIB to discuss the various unlawful conduct decisions. The explanation of decisions thus provided will help the services in future requests. The TIB also contributes to internal training of the services.

It is also increasingly consulting the CTIVD on specific issues. After all, the TIB and the CTIVD involve the same parties and are subject to the same act. Developments can be rapid, for example when it comes to the use of cable interception powers. Knowledge and insights are exchanged where possible and necessary.

Due to its duty of confidentiality regarding its decisions, the TIB rarely seeks publicity. At the same time, the TIB feels it is important to inform politicians and the general public as best it can about its activities. After all, the image of an effective system contributes to the public trust needed for security, and for a sense of security. For example, on 30 March 2023, the TIB gave a technical briefing to the Internal Affairs Committee of the House of Representatives as part of its debate on the Interim Measures Act[1]. On 21 November 2023, the TIB participated in the expert meeting in the Senate on that act.

[1] Rules on specific statutory provisions for the conduct of investigations by the General Intelligence and Security Service and the Military Intelligence and Security Service into countries with offensive cyber programmes against the Netherlands or against Dutch interests (Act on the implementation of interim measures governing AIVD and MIVD investigations into countries with offensive cyber programmes).

Whenever possible, the TIB will respond positively to media enquiries and requests to contribute to broadcasts. On 17 April 2023, it collaborated on a Nieuwsuur current affairs broadcast in which it was argued that the fundamental rights of Dutch citizens were at stake. The TIB also honoured broadcaster HUMAN's request to collaborate on a TV programme about the realization of the Interim Measures Act ('Zwarte lak en Witte jassen', 8 December 2023).

The annual report also has an important function in providing insight into the work of the TIB. The same applies to the TIB's website (www.tib-ivd.nl).

During this reporting year, the chairperson and secretary-director of the TIB participated in two international oversight conferences. One was the European Intelligence Oversight Conference, a gathering of European regulators in Oslo on 8-10 November 2023. The other, also in November 2023, was the two-day International Intelligence Oversight Forum in Washington D.C.

Finally, the TIB answered questions from citizens and professionals whenever possible. The TIB handled about 170 letters from citizens in 2023.

> 'The TIB feels it is important to inform politicians and the general public as best it can about its activities'

1.10 Composition of the TIB

The requirements for the composition of the TIB are set out in the ISS Act 2017. The TIB consists of three members, two of whom, including the chairperson, have extensive experience in the judiciary. The third member was appointed for his technical expertise. The TIB also has deputy members, who can be deployed at times when the permanent members of the TIB are unavailable. The TIB members are supported by an administrative services department, which prepares decisions and advises the committee.

Until 1 April 2023, Mariëtte Moussault served as chairperson; she was succeeded by Anne Mieke Zwaneveld. Serving as members of the TIB are Eric Druijf and Otto Vermeulen. The secretary-director of the TIB is Lennart Schroijen.

From left to right:. Mr O.A. (Otto) Vermeulen, Ms A.M. (Anne Mieke) Zwaneveld LLM, Mr E.H.M. (Eric) Druijf LLM and Mr L.W. (Lennart) Schroijen LLM

2. Highlighted topics

This chapter discusses issues on which the TIB had to render a decision.

2.1 Provision of information in the requests

In assessing requests, the TIB relies entirely on the information contained in the requests and only has access to that information. Unlike the CTIVD, the TIB is unable to search the services' systems. In addition, since the operations constitute state secrets, the TIB cannot consult public sources. If the TIB consulted certain public sources, this could reveal, implicitly or otherwise, what the services' requests are about. The ISS Act 2017 does offer the TIB the possibility to question the ministers on the requests, and the TIB does so frequently. In practice, the TIB addresses its questions about a request directly to the services and also receives the answers from them.

If the TIB feels that it cannot take a sound decision on a request because some matters remain unclear or require further explanation, the TIB can also ask the services to give a presentation about a specific operation or a certain topic.

In recent years and also in 2023, in a number of cases the information originally provided in the request was insufficient for the TIB to reach a sound decision. Sometimes that information was actually incorrect. Usually the inaccuracy was an administrative error or a misunderstanding and was not decisive for the assessment. However, due to the resulting lack of clarity within the TIB it had to ask questions in those cases in order to reach a decision. As a result, it took longer for the TIB to make an assessment.

2.2 De facto extension requests

The ISS Act 2017 requires an extension request to state the results achieved through the previous use of the power. On several occasions, the TIB considered in a decision that an extension request, in accordance with Section 29(2), opening words and under (g), of the ISS Act 2017, should state the yield (results) of the previous use of the relevant power. In this context, the TIB argued that de facto extension requests, where the authorization period ended no more than one year ago, should also state the results of the use of the relevant power. After all, previously obtained results of an operation may be important in assessing a request for extension - also when the operation has been halted for one or more months. The same applies if an operation is given a (slightly) different objective, but still involves the use of a certain power against the same target. After all, previously obtained results of an operation are important in assessing a request for use/extension. The services are aware of this approach and usually comply with it. Nevertheless, situations do arise where the services take a different view with regard to stating previous results in a (de facto) extension request and do not explicitly mention those previous results of the use of the power in the request. This has led to serval unlawful conduct decisions.

2.3 Lenient attitude to obvious mistakes

The TIB noticed that requests in 2023 regularly contained mistakes. By this, the TIB means, in brief, that a request contains a careless mistake, for example, a 'cut-and-paste error' that causes issues in the flow of a sentence, sentences or paragraphs to be mentioned twice, or parts of sentences to be omitted. In such cases, the TIB is prepared to adopt a lenient attitude. On one occasion, a top secret (TS) annex was missing, which still had to be requested by the TIB.

Some extension requests included a sentence or paragraph that originated from the initial request but no longer applied. One request stated that the use of a special power based on two features was still ongoing even though permission to exercise that power had ended some time ago. The TIB asked for an explanation and the service's response revealed that the text of the request had inadvertently suggested that the power was still being used, but that this was explicitly not the intention and had not been the case either. The request was subsequently assessed as lawful.

In addition, some requests were withdrawn by the services after it was found that the request had been submitted erroneously, an incorrect version had been submitted or the request had been submitted to the TIB due to an administrative omission. The TIB will cooperate in such cases, even though the ISS Act 2017 does not provide for them.

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

2.4 Capacity issues

Although there were fewer instances of services having capacity issues this year, this issue will still be discussed in the annual report as capacity issues did occur a few times in 2023. In one hacking request, the TIB found that (partly) due to capacity issues, the power had been used for only a limited part of the requested features, while authorization for a much broader use had been requested and granted. Furthermore, in 2023, several requests explicitly stated that the yield from the use of the power had not been specified due to lack of capacity, while the TIB must assess (partly) on the basis of such yield whether an extension is (still) necessary and proportionate. On several occasions, the TIB also found that due to limited translation capacities, (part of) the yield had not been specified while the service still requested an extension of the use of a special power.

All this may be at odds with the necessity and proportionality criteria and may even lead to an unlawful conduct decision by the TIB. The TIB did not consider any of these requests to be unlawful for this reason. However, in its lawfulness decision the TIB did include comments saying that in any subsequent extension the yield should be specified, and if not, that further justification should be given as to why extension is necessary.

Given its great importance, the TIB continues to draw attention to this issue.

2.5 Investigation-related interception on the cable

Since the ISS Act 2017 came into force in May 2018, the services have had the power to intercept large-scale internet traffic passing through the cable. Such internet traffic takes place on fibre customer channels that are used to carry internet traffic. This power to intercept cable communication is twofold. The first part involves taking snapshots. Snapshots are taken using technical and content-related features to examine whether the information transmitted over the customer channel is

actually relevant to the specific investigation assignments.[2] The second part consists of the actual targeted interception of the cable customer channel for intelligence investigations, the actual production of cable interception.

The TIB assessed several requests in 2023 related to interception of cable customer channels. Some requests were assessed as lawful, others as unlawful. In addition, extension requests relating to interception for production purposes were assessed by the TIB as lawful.

During 2023, a bill – the Interim Measures Act – amending the legal framework regarding bulk interception powers was debated in the House of Representatives[3]. The bill was passed by the Senate at the time of writing this annual report. Among other things, the Interim Measures Act creates a separate legal basis for snapshotting. It also stipulates that the current Section 26(5) of the ISS Act 2017 – the general requirement that any use of snapshotting powers should be as targeted as possible – will be repealed. The Interim Measures Act only covers investigations targeting countries with offensive cyber programmes against the Netherlands or against Dutch interests. The Interim Measures Act did not apply in 2023 as it had not yet come into force. This reporting year, therefore, the assessment of requests has been based on the existing provisions of the ISS Act 2017, including the 'as targeted as possible' criterion. This also applies, therefore, to the snapshot requests assessed by the TIB.

The special power of cable interception should also be used in a manner that is as targeted as possible. In implementing this requirement, the TIB drew on a criterion previously put forward by the service itself, namely whether the potential intelligence value of the proposed interception of one or more designated customer channels is significant. In the TIB's view, this criterion adequately expresses that only those customer channels are intercepted that are likely to yield the data most useful for the investigation - in qualitative or in quantitative terms. Using the above criterion, the TIB assessed each of the customer channels listed in the requests.

At the end of the 2022 calendar year, the TIB assessed a snapshot request as unlawful.
In the first quarter of 2023, the service concerned submitted a new, amended request for snapshots on various customer channels on a specific cable route. The TIB considered that the service had given too generic an interpretation to the concept of 'as targeted as possible'. Without further substantiation, the mere fact that a party offers worldwide internet traffic – and also, therefore, in the focus area – is insufficient. The requirement that the use of the requested power must be as targeted as possible under Section 29(2)(h) of the ISS Act 2017 was not met. The TIB ruled that the authorization given by the minister in response to the new, amended request had not been granted lawfully either.

In mid-2023, other requests were made regarding snapshotting of various customer channels on the same cable routes. Those operations are the successors to a snapshotting operation that had been assessed as lawful by the TIB in 2022 as part of a cyber threat investigation. Compared to that operation, these new requests saw a (significant) broadening of the scope of snapshotting in several respects: more customer channels, more cable routes, and the use of the power was no longer limited to cyber threat investigations.

The TIB issued an unlawful conduct decision in relation to these requests because it was likely that, contrary to the ministers' commitments, Dutch-Dutch traffic[4] would also be intercepted. In addition, the TIB also assessed the requests as unlawful due to the fact that the minister had granted authorization to share an

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

3 *Parliamentary Papers II* 2022-2023, no. 36 263, 'Act on the implementation of interim measures governing AIVD and MIVD investigations into countries with offensive cyber programmes'.

4 *Parliamentary papers* II 2017-2018, 34588, no. 76, p. 3.

extract of a captured snapshot with a foreign service. As the extent of the extract was not further substantiated, it was not possible to weigh up the potential associated infringement.

With regard to some customer channels mentioned in another request, the TIB found that those channels met the criterion of expected potential intelligence value. However, this was not the case with regard to a number of other customer channels in the same request. Under the ISS Act 2017, the TIB can only assess requests as entirely lawful, or as unlawful. Regarding a request in which some of the customer channels met the criterion and some did not, the TIB could not but decide to assess the request in its entirety as unlawful.

> 'The TIB can only assess requests as entirely lawful or as entirely unlawful'

In autumn 2023, the TIB assessed the new, amended cable requests from both services regarding snapshotting of various customer channels on cable routes as lawful. In those decisions, the TIB considered that from the minister's statements in a Memorandum[5], it understands that the minister qualified the commitment made earlier, in 2018, regarding Dutch-Dutch traffic. The TIB considered that this had created a different situation. For Dutch citizens, it cannot be ruled out that if the services use cable interception, they may also intercept Dutch-Dutch traffic in wider investigations. The previous ground for unlawfulness has thus been removed. In addition, these requests state that the sharing of information with foreign partner services is excluded, thereby also removing that ground for unlawfulness. The TIB also ruled that these are customer channels whose potential intelligence value is significant and that they therefore meet the criterion used.

> 'In autumn 2023, the TIB assessed several cable snapshotting requests as lawful'

In the last quarter of 2023, the two services submitted requests for snapshotting a different type of data. The TIB assessed those requests as unlawful. The requests lacked sufficient justification as to why the proposed operation was as targeted as possible, given that there was no further delineation of the data to be acquired. As a second ground for unlawfulness, there was insufficient justification as to why it was necessary for the service to intercept this data traffic in bulk, and why it was necessary to take snapshots of this traffic. The lack of subsidiarity also provided grounds for this unlawful conduct decision, since the request did not explain why cable interception was the lightest means to be used in order to answer the questions in the relevant investigations.

2.6 Technical risks and unknown vulnerabilities

In accordance with Section 45(4)(a) of the ISS Act 2027, the TIB reviews the technical risks relating to the use of hacking powers. Section 45(4)(a) requires that a request for a special power, hacking, must include a description of the technical risks. The request must contain a separate description of those technical risks. The technical risks are weighed against the operational interests of the services and are also part, therefore, of the proportionality test by the TIB.

[5] As part of the legislative debate in the House of Representatives on the draft bill for the implementation of interim measures governing AIVD and MIVD investigations into countries with offensive cyber programmes, a Memorandum in response to the report was submitted to the House of Representatives on 4 September 2023, see *Parliamentary Papers II* 2022-2023, 36 263, no. 9 (Memorandum in response to the report).

2.6.1 Description of technical risks and new format

In 2023, the TIB assessed several requests seeking authorization for an initial hacking operation or continuation of such an operation. The TIB issued an unlawful conduct decision for some of those requests. The reason for this is as follows.

When assessing the technical risks, the TIB looks at two types of risks in particular: the risk to the availability and integrity of the automated system concerned and the risks of misuse by third parties. The first risk involves the possible failure of a system, while the second involves other actors/state actors who could potentially misuse our services' knowledge and technical resources.

In the first quarter of 2023, the services updated the description of the technical risks. This update created a generic text that no longer allowed the TIB to review technical risks in concrete cases. Methods of describing the intended hacking operation were no longer described exhaustively. The requests only mentioned a regular modus operandi to be adopted by the services. The requests no longer described what that modus operandi would consist of in a concrete case. The TIB subsequently ruled in several requests that, for that reason, no proper assessment could be made as to whether the technical risks could be adequately curtailed or mitigated. In those cases, the technical risks had not been sufficiently clarified or the TIB was of the opinion that the risks were too great.

In response to the unlawful conduct decisions, the services adopted a (new) format for describing those technical risks in hacking operations. That framework was discussed with the TIB and became part of requests related to this. In the second quarter of 2023 and beyond, the TIB no longer arrived at unlawful conduct decisions regarding hacking operations on this ground. The framework has a positive effect.

2.6.2 Use of unknown vulnerabilities

If the services intend to use an unknown vulnerability when exercising the hacking power, it will first be submitted to the minister and the TIB. An unknown vulnerability is a weakness in software of which the creator/developer of the software has not yet become aware. Putting this explicitly before the minister and the TIB is necessary mainly because if the unknown vulnerability is leaked, the potential consequences can be very serious. 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 a request submitted in 2023, the TIB found that the authorization had not been lawfully granted because it was not sufficiently clear from the request whether the service intended to use an unknown vulnerability. The request was inconclusive on this point and the TIB could not but conclude that the authorization had been granted unlawfully for that reason.

> 'Following the unlawful conduct decisions, the services adopted a (new) format for describing technical risks. This has a positive effect'

2.6.3 Presentations by the services

Over the past years, the services have increasingly provided the TIB with better information about the technical risks associated with a hacking operation. This trend has continued into 2023. This reporting year, too, the services gave several presentations on this topic. The TIB remains positive about this development. These presentations mainly concern cases where the services want to deploy an unknown vulnerability, or requests where the TIB has asked questions or requested further explanation in the form of a presentation.

2.7 Bulk data sets and relevance assessment

Bulk data sets play a major role in the services' investigations. Bulk data sets are large collections of data, the vast majority of which concern people and/or organizations that are not, and never will be, the subject of investigation by the services. The services see long-term operational value in many bulk data sets.

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. The guiding principle here is that the invasion of the privacy of persons who are not and never will be the subject of investigation should be limited to what is strictly necessary. The maximum retention period for data whose relevance has not (yet) been assessed, including any extension, is 18 months. Only data declared relevant may be stored for a longer period.

With regard to the deadline for a relevance assessment, the ISS Act 2017 does not stipulate any specific rules regarding bulk data sets. That means that such bulk data sets fall under the same regime of Section 27 of the ISS Act 2017 as 'separate' data. In 2023, the TIB received several requests related to the intended relevance assessment mode for bulk data sets. The TIB only assesses a request as lawful if it contains the safeguard that the relevance assessment will be conducted in a way deemed lawful by the CTIVD. This means that the services should state that after acquiring a bulk data set they will not, subsequently, automatically declare it to be relevant its entirety. 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 for longer than 18 months. New information may, of course, be kept, but bulk data that have been in the services' possession for 18 months may not be acquired again or must be removed immediately after having been re-acquired. This is to avoid an arrangement that enables an item of legislation to be circumvented or State control to be evaded, effectively rendering Section 27 of the ISS Act 2017 inoperative.

In the first half of 2023, the TIB handled requests that involved a long-term hacking operation aimed at a non-target for the purpose of periodically acquiring a bulk data set. Questions were raised by the TIB about how the service intended to process the data from the bulk data set(s). It followed from the answers that no overall relevance assessment would be carried out on the data in the bulk data set. The TIB understood this response to mean that the relevance assessment would be carried out when a new statutory regulation applied. As a result, it issued a lawfulness decision - after all, reviewing the timeliness of relevance assessments is not part of the TIB's remit. That assessment is reserved for the CTIVD. However, the TIB did state that, in its view, an assessment that will take place in 18 months at the earliest does not meet the 'earliest possible relevance assessment' criterion laid down in Section 27(1) of the ISS Act 2017.

Another request was also assessed by the TIB as lawful. In that decision, the TIB commented that it understood the service to mean that both the initially acquired bulk data set and the set acquired in the interim would be destroyed after 18 months if no transitional law applied at that time.

In autumn 2023, the TIB also assessed another request related to bulk data sets as lawful. The service had indicated that the non-assessed parts, and the parts assessed as irrelevant, of all acquired files would be deleted and destroyed after 18 months. In that decision, the TIB mentioned that it adopts the principle that the period for a relevance assessment starts at the time a file is acquired.

However, the TIB assessed another request as unlawful in 2023. That request concerned a strategic hacking operation against a non-target. As part of this hacking operation, the minister had authorized the service to acquire files of this non-target periodically to see if a target made use of this non-target.

It followed from the methodology described that it was possible that (the same) data of persons who were not, and never would be, the focus of the services' attention would be acquired, stored and processed by the services over and over again. The data assessed as 'irrelevant' were apparently acquired over and over again regardless of that assessment. The TIB issued an unlawful conduct decision because the procedure was not compatible with the legal system for relevance assessment as stipulated in Section 27 of the ISS Act 2017 and the rationale behind that provision.

Meanwhile, the government has submitted a supplementary bill to the bill for the Interim Measures Act[6]. This supplementary bill envisages a different system in which the services will be given the option to annually extend the retention period of bulk data sets not yet assessed for relevance.[7] In anticipation of the entry into force of this bill, the Minister of the Interior and Kingdom Relations, the Minister of Defence and the CTIVD have made administrative agreements not to apply the statutory period of 18 months any longer, but to act in the meantime as if the Interim Measures Act already applies.[8]

2.8 Strategic operations

A strategic hacking operation is an operation in which the services intend to use the hacking power to obtain a strategic position within a network. Previous annual reports have also addressed this issue. This type of hacking concerns operations that are not primarily concerned with obtaining data from targets but with taking up a position that could be useful at a later stage in the investigation into a target.

The legislator has never commented on the extent to which such a strategic hack fits in with 'the proper performance of the tasks and duties of the services'. The TIB has repeatedly asked the legislator to give its general opinion on the admissibility of the hacking power being used purely on strategic grounds and to state the framework for such use. The TIB is currently reviewing such requests within its regular assessment framework.

> 'The use of hacking powers on strategic grounds possibly invades the privacy of individuals who are not, and never will be, the focus of the services' attention'

In 2023, as in previous years, the TIB received several requests in which the services intended to use the hacking power on purely strategic grounds. These cases concerned operations possibly invading the privacy of individuals who are not the focus of the services' attention and never will be. In 2023, the TIB issued lawfulness decisions as well as unlawful conduct decisions on the requests related to this. This section gives a brief description of a number of these operations.

6 The regulation was included in a memorandum of amendment with which the draft bill was to be amended. For more information, refer to chapter 4 of this annual report.

7 Such a request for authorization would be made by the head of service to the minister. The request should state why the bulk data set has to be retained for a longer period, and the CTIVD will provide binding oversight.

8 Administrative agreement between the Minister of the Interior and Kingdom Relations, the Minister of Defence and the CTIVD, see *Parliamentary Papers II* 2022-2023, 36 263, no. 36

The first operation concerned a request seeking authorization to hack a non-target. The purpose of that hack was to gain a strategic position within the internal network of this non-target, which position could be used in the future. The TIB assessed this request as unlawful in 2022 because the technical risks to the integrity of the system in the operation were too high. In 2023, the TIB assessed the new, amended request as lawful. The technical risks had now been sufficiently addressed and the risks were therefore acceptable and proportionate. In its assessment, the TIB considered that the actual use of the strategic position would be submitted by separate request.

In 2023, the TIB also assessed another request involving a long-term hacking operation against a non-target as lawful. This, too, was a strategic operation, because through this authorization, a position was taken that allowed the service to conduct a targeted investigation into a specific target at a later point in time.

The extension in 2023 of a strategic hacking operation assessed as lawful in 2022 was assessed as unlawful by the TIB. This concerned a hack against a non-target where the service was able to acquire bulk data covertly. The investigation into such bulk data subsequently offered the service the possibility of acquiring data from as yet unknown targets. In 2023, a request was submitted for a substantial expansion of the use of hacking powers against this non-target. The acquisition of those data could be enriched by linking with other data that would be acquired from the non-target. In particular, that expansion would significantly increase the invasion of privacy of individuals who are not and will never be the subject of investigation by the service. Given that circumstance, the TIB considered the extension of the invasion no longer proportionate to the objective of the operation to be achieved with it. The TIB ruled that the extension, but especially the expansion of the use of the hacking power, was no longer proportionate and therefore the authorization for the request had not been lawfully granted.

2.9 IMSI catcher

A basis for using an IMSI[9] catcher can be found in Section 47(4) of the ISS Act 2017, which stipulates that the services are authorized to use a technical device to obtain the number or technical feature for which the power will be used. The IMSI catcher works as follows. The IMSI catcher poses as a mobile phone base station to which nearby mobile phones log in. The mobile phones leave attributes such as their IMSI and IMEI numbers when logging in, and are then routed to a real mobile phone tower.

The services and the TIB have different views on the legal basis for the use of the IMSI catcher. The joint position of the AIVD and the MIVD is – in brief – that Section 40 of the ISS Act 2017 may provide a basis for deploying an IMSI catcher during tracking/observation, because the IMSI catcher qualifies as a recording device. According to the service, the head of service is authorized to use this power. The TIB does not share this view and considered that Section 40(1) of the ISS Act 2017 grants a power to observe and, as part of this, record data, with or without the use of recording devices. In the TIB's view, however, an IMSI catcher cannot be classified as a technical device that purely and solely records data, and its use should be submitted to the TIB. As also stated in the Explanatory Memorandum to Section 47 of the ISS Act 2017, an IMSI catcher involves the use of active scanning equipment. It follows from this that an IMSI catcher actively interferes with the handling of mobile telephone communications. In the TIB's view, the fact that the current generation of IMSI catchers does not capture content does not alter this. As a result, several requests in which this issue arose have been assessed as unlawful by the TIB.

9 International mobile subscriber identity-catcher.

2.10 'Stomme tap'

As early as on 6 October 2020, the Court of Justice of the European Union ruled[10] on the *real-time* collection of data on users of a telecommunications service and their communication traffic. The legal basis for this in the Netherlands is Section 55 of the ISS Act 2017 (the 'stomme tap'[11]). In its ruling, the CJEU considered that the *real-time* collection by public authorities of data on users of a telecommunications service and their communication traffic restricts the right to privacy to such an extent that authorization for this must be subject to a binding lawfulness assessment by a judicial or otherwise independent body. Such lawfulness assessment should take place before the real-time collection of data or, in urgent cases, within a short time after such collection has started.

The real-time collection of data on users of a telecommunications service and their communication traffic is called 'stomme tap'. In the Netherlands, the intelligence and security services are authorized to collect such data, but since the authorization for the use of this power was given by the head of service, it was not subject to a prior binding lawfulness assessment by the TIB. This will change when the Interim Measures Act comes into force. In the meantime, a provision was made by the TIB and the minister in the form of an agreement.[12] This agreement was signed on 29 September 2023 by the Minister of the Interior and Kingdom Relations, the Minister of Defence and the chairperson of the TIB and entered into force on 1 October 2023. Setting out all arrangements regarding the procedure, the agreement provides a temporary provision pending a legal basis.

'The European Court of Justice ruled that real-time collection of telephony data restricts the right to privacy to such an extent that a prior binding lawfulness assessment is required'

Since 1 October 2023, the TIB has received several dozen requests from the services regarding the use of this special power under Section 55 of the ISS Act 2017 for assessment. This number is included in the total number of requests assessed by the TIB in 2023. None of these 'stomme tap' requests were assessed as unlawful by the TIB. However, the TIB did raise questions on a number of requests before a sound decision could be made. In addition, for some of these requests, the TIB issued a lawfulness decision but included a comment.

2.11 International solution for satellite interception

In the short term, the rollout of 5G in the Netherlands will continue to take shape. This could pose a problem when intercepting specific satellite communications. The services have been looking for an international solution to continue intercepting these satellite communications in the future. However, relocation of part of the current interception site should not affect the applicable safeguards mentioned in the ISS Act 2017. Therefore, the services, departments, CTIVD and TIB entered into discussions in 2023 on applying the legal framework. It is expected that these discussions can be concluded in the first half of 2024, and the review and oversight framework can then be adopted and published.

[10] Judgment of the Court of Justice of the European Union dated 6 October 2020, ECLI:EU:C:2020-791, La Quadrature du net and others

[11] A 'stomme tap' is when only data are intercepted ('metadata'). This makes it possible to see who a person is calling and where that person is at that point in time. However, the content of a conversation is not intercepted.

[12] Government Gazette of the Kingdom of the Netherlands: 2023,26548 'Convenant toetsing stomme tap'.

2.12 Special case

Section 30(2) and (3) of the ISS Act 2017 states that in cases involving the exercise of a special power against a journalist or lawyer, this is only permitted if authorised by the District Court of The Hague.

In one case, the TIB ruled that the extension request pertaining to an individual covered a lawyer's (script of) confidential communications and assessed this as unlawful. The request concerned the use of the power to wiretap telephones, which involved the scripts of several conversations between a lawyer and a person other than the lawyer's client. As indicated above, the power to wiretap telephones had been granted in an earlier request with respect to the person concerned, not the lawyer. In that context, the TIB put questions to the service about the application of Section 27(2) of the ISS Act 2017 and the scripts of those conversations. The service believed that Section 27(2) of the ISS Act 2017 did not apply to the conversations between that person and the lawyer, because that person was not the client of that lawyer. For this reason, the service did not ask the District Court of The Hague for authorization to process the conversations.

The TIB did not follow the service's reasoning, considering as follows.

The law, the Explanatory Memorandum and CTIVD report no. 52 show that the scope of Section 27 is not limited to the situation where the special power is used against the lawyer's client. Therefore, in the TIB's view, the use of special powers aimed at persons other than the lawyer's client may also fall under Section 27(2) of the ISS Act 2017 and depends on the content of the communication in question.

The yield as described showed that the lawyer talked to that person about the conversations with the client, among other things. This is why the TIB ruled that the intercepted communications between that person and the lawyer were confidential and subject to the protection of privilege. The further processing of those conversations requires authorization from the District Court of The Hague.

In addition, the request also did not explicitly state how the communications (and their scripts) would be handled in the future while it was reasonably foreseeable that the individual concerned would again have contact with that lawyer during the requested extension period. The TIB ruled that the minister had not lawfully authorized the extension of the use of the wiretapping power.

The TIB informed the CTIVD about this decision. Consultations then took place between the TIB and the CTIVD in which this decision was discussed. During these consultations, the CTIVD expressed its views on the purport and scope of Section 27(2) of the ISS Act 2017. The CTIVD agrees that whether or not a conversation is privileged depends not only on the formal status of the interlocutors, but also on the content of the communication in question. This means that a conversation between a lawyer and a person other than his client can still be privileged if it involves confidential communication.

3. Review by the TIB in figures

2023 showed a sharp increase in the number of requests assessed compared to 2022. Interestingly, the percentage of unlawful conduct decisions in 2023 also increased proportionately. This chapter first presents an overall view of requests reviewed by the TIB in 2023. Next, the unlawful conduct decisions and the reasons that led to the unlawful conduct are discussed in detail. We then zoom in on urgency and priority requests and the requests that were withdrawn.

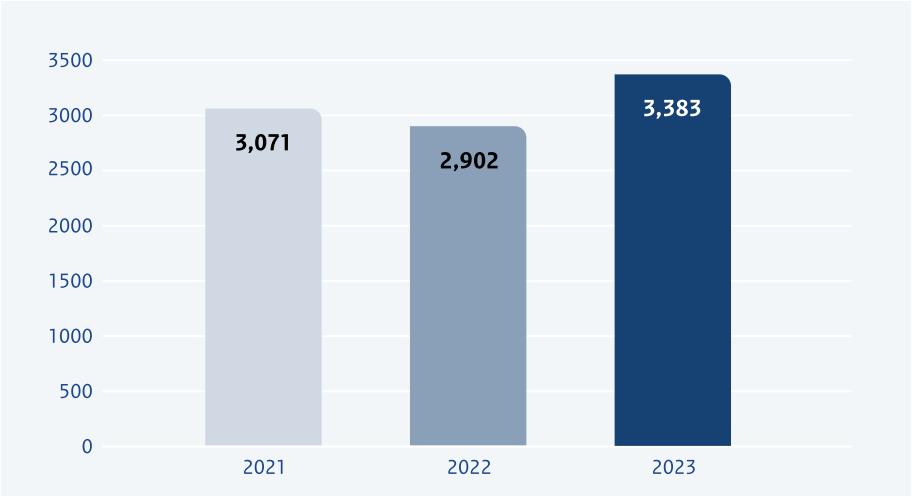
3.1 Overall view of the requests

The TIB assessed a total of 3,383 requests from the two services in 2023 – a sharp increase from last year, up 16.6%. This is striking because in 2022, on the contrary, there had been a 5.8% drop in the number of requests.

Table 1: assessment of requests

Figures for 2022 and 2021	2021	2022	2023
Total number of reviewed requests	3,071	2,902	**3,383**
Number of requests in which questions were asked	383	366	**371**
Number of unlawful conduct decisions	119	67	**148**
Number of lawfulness decisions	2,952	2,835	**3,235**
Number of withdrawals	18	14	**12**
Number of urgency procedure requests	111	129	**193**

Figure 1: number of requests assessed per calendar year



In this reporting year, the number of requests submitted by the AIVD rose by 22% and the number of requests submitted by the MIVD dropped by 5%.

In 2023, the TIB assessed a total of 3,383 requests, 148 of which it assessed as unlawful. The percentage of unlawful conduct decisions rose at both the AIVD and the MIVD.

Figure 1 clearly shows that in 2023, there was a sharp increase in the number of requests assessed by the TIB compared to the previous two years. This is the highest number of requests assessed since the TIB was launched in 2018.

3.1.1 Requests in which questions were asked

Sometimes the TIB has to ask questions because there are ambiguities that stand in the way of a sound decision. In 2023, the number of requests in which the TIB asked questions remained almost the same in absolute numbers compared to the previous year, but slightly decreased in relative terms. The AIVD was asked slightly fewer questions this year than in the previous year, the MIVD slightly more.

3.1.2 Requests where a comment was made

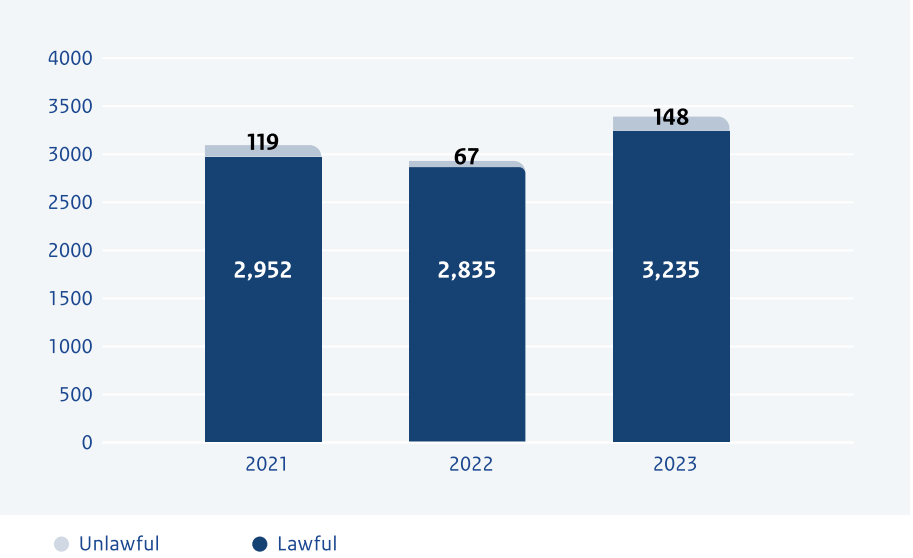
In a number of cases, the TIB included a comment in a lawfulness decision. The number of comments in 2023 is almost in line with the previous year's number, which means that it decreased slightly in relative terms. The 2022 annual report was the first to look at the number of lawfulness decisions where the TIB made a comment; no comparison can be made with 2021.

3.2 Development of unlawful conduct decisions

In 2023, a total of 148 requests were assessed by the TIB as unlawful. A comparison with the two previous years shows that the relative share of unlawful conduct decisions fluctuates, but remains consistently low in relation to the total number of requests reviewed.

In 2021, unlawful conduct decisions accounted for 3.9% of requests, compared to 2.3% in 2022. In 2023, the number of unlawful conduct decisions increased; this calendar year 4.4% of requests were assessed as unlawful.

Figure 2: Number of lawfulness and unlawful conduct decisions per calendar year



At the AIVD, the number of unlawful conduct decisions almost doubled this reporting year to 4%, compared with 2.1% of requests in 2022 and 3.3% in 2021.

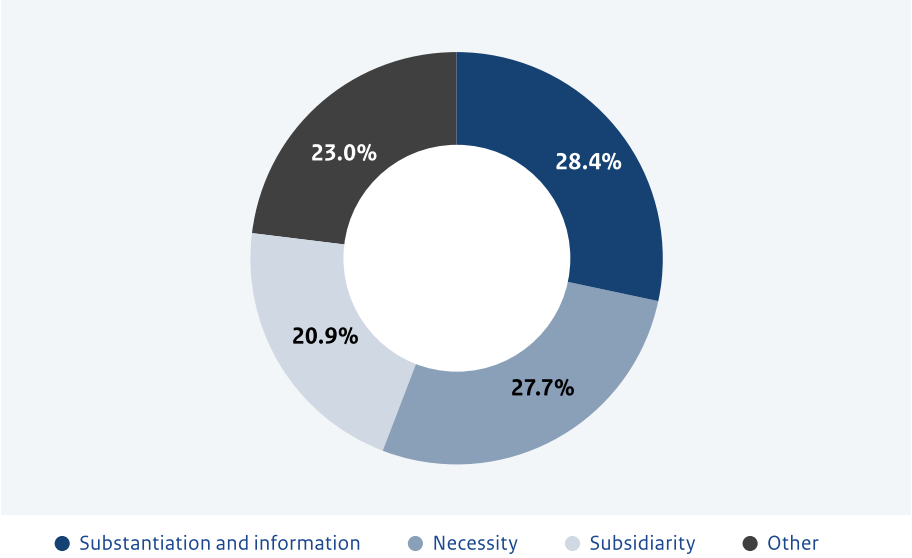
At the MIVD, the number of unlawful conduct decisions even more than doubled, rising to 6.3% from 3% in 2022. In 2021, the rate at the MIVD was 7.1%.

3.3 Reasons for unlawful conduct decisions

In 2023, 148 requests were assessed as unlawful for various reasons.

The main reason for an unlawful conduct decision is flaws in the reasoning of a request. In those cases, the TIB considered itself insufficiently or incompletely informed to make a sound decision. The second most common reason is the lack of a need to exercise the power (necessity requirement) as an independent ground for an unlawful conduct decision. This is followed by the absence of a reason why the exercise of a less intrusive power would not suffice (subsidiarity requirement). More often than in previous years, the services sufficiently explain why the exercise of the power in question is proportionate (proportionality requirement), which is therefore less often a reason for an unlawful conduct decision. There is no immediate explanation for this.

Figure 3: Ratios between reasons for an unlawful conduct decision



3.4 Resubmitted requests following an unlawful conduct decision

When a request to use a special power is assessed by the TIB as unlawful, the service can opt to submit a new and amended request to the TIB. The AIVD submitted an amended and new request in almost half of those unlawful conduct decisions, the MIVD in just over half of those cases. The figures decreased at both services compared to the previous year. This means that in 2023, both services submitted fewer new and amended request to the TIB.

Half of the new and amended requests were eventually assessed by the TIB as lawful. This is a slight drop compared to previous years. The other half were again assessed as unlawful.

One third of the requests reassessed as unlawful in the second instance were submitted a third time. Just under half of these requests submitted for a third time were assessed as lawful. The remainder was not resubmitted.

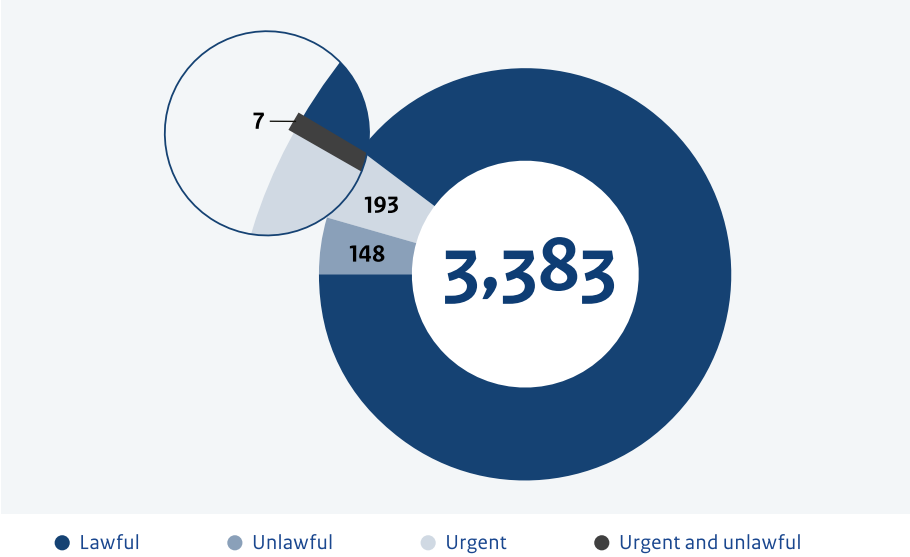
3.5 Urgency procedure

The number of urgency procedures has increased in recent years. The urgency procedure was invoked a total of 193 times in 2023, compared to 129 times in 2022 and 111 times in 2021. One explanation for part of the increase in 2023 lies in the fact that the AIVD requested the use of the urgency procedure 24 times, for several different powers, in an investigation covering several operations.

In 2023, the TIB decided on seven occasions that the urgency procedure had not been lawfully invoked. As in 2022, there were no instances where the TIB ruled that the data collected had to be destroyed immediately for that reason alone.

In one case, the TIB ruled that the urgency procedure had been invoked unlawfully and also assessed the use of the power as unlawful. As a consequence, the data collected in the exercise of that power had to be destroyed immediately by operation of law.

Figure 4: Number of lawfulness decisions, unlawful conduct decisions and urgency decisions



3.6 Priority requests

In this reporting year, the TIB was asked to prioritize a request in over 400 cases. All those priority requests came from the AIVD. Since this is the first year in which such requests have been registered separately with the TIB, no comparison can be made with previous years. However, the impression is that this is the highest number of priority requests so far. Initially, priority was requested only for operations where an operational opportunity arose at short notice. This reporting year, it seems that for more and more requests priority was asked because the authorization period for the previous request had (almost) expired and the services had failed to notice this in time.

3.7 Withdrawn requests

In 2023, there were 12 occasions when the authorization granted for a request from the services was withdrawn by the minister after the request had been submitted to the TIB for review. Over the years, the number of requests withdrawn after they having been submitted to the TIB has steadily decreased.

4. Interim Measures Act and other developments

On 8 December 2022, the Minister of the Interior and Kingdom Relations and the Minister of Defence submitted a draft bill to the House of Representatives of the States General, the 'Act on the implementation of interim measures governing AIVD and MIVD investigations into countries with offensive cyber programmes, bulk data sets and other provisions', also known as the Interim Measures Act. Simultaneously with the introduction of this draft bill, a memorandum of amendment (hereinafter, the Memorandum) was announced. The Memorandum supplements the draft bill with two regulations: a prior, binding review by the TIB of the use of the 'stomme tap' (real-time traffic and location data interception) and an extension of the legal regulations on bulk data sets and the declaration of exemption from the relevance provision of Section 27 of the ISS Act 2017.

4.1 Interim Measures Act

The Interim Measures Act creates a new regime of investigations by the services into countries with offensive cyber programmes. An offensive cyber programme aims, among other things, to surreptitiously obtain, by digital means, confidential information, economic and technological know-how or other information from citizens or organizations which these countries use to their advantage.

The Interim Measures Act has resulted in a substantial extension of the powers of the services. For some powers, oversight shifts from, for example, structural binding oversight by the TIB prior to the use of the power, to the possibility of binding ex-post oversight by the CTIVD. It also creates an option for services to appeal a decision of the TIB and the CTIVD to the Council of State.

> 'The Interim Measures Act creates a new regime of investigations by the services into countries with offensive cyber programmes'

The TIB has expressed its views on the Interim Measures Act to ministers and parliament on several occasions. It did so in a letter to the Minister of the Interior and Kingdom Relations and the Minister of Defence dated 14 April 2022 (reference BWP3221331), the TIB's response dated 11 January 2023 during the internet consultation (letter with reference NWP8221357) and during the technical briefing to the House of Representatives on 30 March 2023. On the occasion of the technical briefing to the Senate on 21 November 2023, the chairperson of the TIB provided insight into the differences in oversight under the Interim Measures Act and the ISS Act 2017. See Table 2.

Table 2: ISS Act 2017 versus Interim Measures Act

ISS Act 2017	Amendment in response to the Interim Measures Act
Use against all targets, non-targets, third parties Individuals, intelligence services, armed forces, but also parties in a broader context: companies or institutions or more diffuse proxy organizations	Same for countries with offensive cyber programmes
Binding review: In advance by TIB Binding oversight: Afterwards by CTIVD complaints department	Binding review: Partly in advance by TIB Binding oversight: During and afterwards by CTIVD Afterwards by CTIVD complaints department
No possibility of appeal	Appeal with the Administrative Jurisdiction Division of the Council of State
Exploration of data streams on the cable in a targeted manner and for verification purposes	Exploration of data streams on the cable in a non-targeted manner and for exploration purposes
Cable interception focused on investigation (production) Proportionality test	Cable interception focused on investigation (production) Proportionality test to be specified
Option to add only for servers, (home) routers, phones, laptops etc. exclusively used by the target	Option to add for all servers, (home) routers, phones, laptops etc. used, also from non-targets
In principle, streaming services and NL-NL traffic destroyed as soon as possible	Streaming services and NL-NL traffic may be retained
Assessment period with regard to data obtained through hacking: as soon as possible maximum retention period of 18 months	Assessment period with regard to data obtained through hacking: not as soon as possible no maximum retention period
No sharing of shapshot data with foreign countries	Sharing of shapshot data with foreign countries
Description of technical risks when using hacking powers	No description of technical risks when using hacking powers cf. Section 45(4)
Authorization for 'stomme tap' by the heads of the services	Authorization for 'stomme tap' by the TIB (and under an agreement since 1 October 2023)

In the committee meeting in the Senate on 21 November 2023, Mr Nicolaï (from Partij voor de Dieren) asked the TIB to clarify which disagreements between oversight bodies and the services the Council of State refers to in its advice on the Interim Measures Act, and whether there are any expectations about disputes that will (continue to) exist after the Interim Measures Act comes into force.

The TIB also informed the Senate on 7 December 2023 in a letter (reference BWP2231316). This letter again focused on possible future disputes, among other things. Several parties raised questions partly in response to this letter. The Minister of the Interior and Kingdom Relations responded to these questions in the Memorandum issued in response to the Senate's report on the Interim Measures Act on 19 January 2024. Following this, new questions were asked. By the time of writing of this report, the Senate had completed its debate on the draft bill.

4.2 Introduction of the appeal procedure

Section 13 of the Interim Measures Act creates the possibility of appeal to the Administrative Jurisdiction Division of the Council of State (hereinafter: 'the Division') against certain binding decisions of the TIB and the CTIVD. The section mainly contains procedural rules and deadlines for filing a notice of appeal and a statement of response. Several issues may be addressed in the appeal procedure, including the 'as targeted as possible' criterion in cable interception cases or the addition of non-exclusive actor infrastructure. However, it cannot be ruled out that more issues will be addressed.

The TIB's decision is reviewed by the Division. In effect, this means that an 'indirect' review takes place, as the TIB reviews the authorization given by the minister concerned, based on a request by the service concerned. In this 'layered' lawfulness assessment, it may be assumed, according to the legislative history, that the Division will review the decisions of the TIB and CTIVD with a certain degree of restraint.

The possibility of appeal to the court regarding a decision of an oversight body is common in regular Dutch administrative law. Internationally, however, it remains peculiar that only the reviewed party can lodge an appeal with the court against the independent party that provides prior binding reviews of requests for the use of powers by the intelligence and security services. After all, it is for this very reason that the TIB consists of two members with at least six years of experience as judges. In addition, the TIB carries out independent and effective oversight as required by the ECHR and the Court of Justice of the European Union.

4.3 How the TIB prepares for the Interim Measures Act

In spring 2023, the TIB started mapping out the potential impact of the Interim Measures Act and preparing to adapt parts of its own modus operandi. These preparations included commissioning an independent opinion from an external legal firm in view of possible proceedings before the Division. The Interim Measures Act provides for the TIB and the CTIVD to exchange relevant information. This is an important step forward.

> 'The announced broader review of the ISS Act 2017 merits effective and structured consideration'

The possible effective date of the Interim Measures Act is not known at this time. It is expected that the Division will adopt a further elaboration of the appeal procedure in procedural rules once the Interim Measures Act is in force. Once those procedural rules are known, the TIB can finalise its modus operandi on this point.

The Interim Measures Act provides for changes in a number of areas ahead of the announced broader review of the ISS Act 2017. This review merits thorough and structured consideration, covering all relevant developments in the work of the services as well as technological and legal developments.

5. Outlook

As part of this annual report, the TIB would also like to briefly look ahead. After all, things will change in the coming years, for the TIB itself, but also in terms of its cooperation with the CTIVD and technological developments, including geopolitical developments.

5.1 The TIB as an organization

The TIB was founded in 2018 and has since grown to 16 individuals (members, deputy members and staff). In the period ahead, the TIB will have to keep evolving in the permanently changing environment in which it operates. For this reason, a new knowledge system is being implemented, among other things.

The TIB's working environment is characterised by the daily handling of large numbers of state secrets and a high workload. Members and employees of the TIB have no opportunity to work from home because of the risks involved. Naturally, the content of requests submitted to the TIB and the subsequent decisions of the TIB cannot be discussed with third parties. Due to the nature of the work, high demands are made on the quality of employees and flexibility of the organization. This is why the TIB pays a great deal of attention to individual development and team cooperation.

After more than five years, and given the necessary growth of the organization, the priority for 2024, like last year, is to further professionalise the internal organization. For instance, since 2023, the TIB has had an organization and workforce (O&F) plan, which identifies tasks and activities. Following on from that O&F plan, work will continue in 2024 to establish a structural training plan and ongoing team development. In 2024, the TIB will also work with an annual plan that guides the organization's goals and products.

In addition, in 2024, the website will be updated and a public leaflet about the TIB will be released for the first time. The TIB's communication policy will be updated.

A decision on the relocation of the Ministry of General Affairs from Binnenhof to Bezuidenhoutseweg in The Hague is expected in the course of 2024. Since the Ministry of General Affairs is the 'landlord' of the TIB, this move means that the TIB will move as well. In order to ensure the continuity of its services, the TIB will continue to work 'as normal' during the renovation and relocation process. The TIB is preparing for this.

Organizational agility is needed not only to advise and decide on the constant flow of requests submitted to the TIB on a weekly basis. The TIB's Rules of Procedure are expected to be reviewed in 2024. The internal and external review framework that applies to the annual flow of requests will be fleshed out.

5.2 Review and oversight in the future

The announced review of the ISS Act 2017 should identify how to structure the further integration of review and oversight. Previously, in their response to the Outline Memorandum[13] the TIB and CTIVD indicated their preference for introducing an oversight body that carries out end-to-end oversight.
The provisional name for this oversight body is the 'National Security Authority' (*Autoriteit Nationale Veiligheid*). Joint exploration and development of this initiative started in 2023 and will continue in 2024 and beyond. In the longer term, this will make it possible to effectively align the ex-ante review and ex-post oversight and establish a normative framework for the whole chain.

Together with the CTIVD, the TIB will do what can – and should – be done in 2024. Where necessary and required, for example when it comes to technical developments and cyber, the TIB is organizing information exchange with the two services and the CTIVD.

In the coming years, technological developments such as artificial intelligence, topics such as facial recognition, quantum computing and deep fakes will also require the TIB's attention. The TIB estimates that these developments are moving faster than the review of the law. The recalibration of the (technology-independent) normative framework for the entire chain thus offers the opportunity to anticipate technical developments more proactively. The starting point remains that the balance between the protection of fundamental rights on the one hand and their infringement on the other is effectively maintained, now and in the future.

Geopolitical developments and tensions in the world are also expected to remain high on the agenda of the services, and hence the TIB, in the coming years. Examples include the conflicts in Ukraine and the Middle East. Services and oversight bodies maintain increasingly frequent and intensive contacts with foreign sister organizations partly because of this. This also calls for clear and verifiable ground rules for exchanging information and data with those foreign sister organizations.

The TIB will therefore continue to maintain and expand contacts with foreign oversight bodies, within and outside the EU, in the coming years. The TIB does this by participating in international conferences. These contacts also provide insight into the different forms of review and oversight in other countries. The experience so far is that the choices made in the Netherlands are a best practice for several countries.

> 'The balance between protection of fundamental rights and infringement of fundamental rights calls for a strong oversight body: a National Security Authority.'

[13] Outline Memorandum on amendment to ISS Act 2017 dated 1 September 2023, reference 2023-0000547038.

Toetsingscommissie
Inzet Bevoegdheden