Toetsingscommissie
Inzet Bevoegdheden

Annual Report TIB 2021

Binnenhof 19
2513 AA Den Haag
www.tib-ivd.nl

Disclaimer: No rights may be derived from this translation and under all circumstances the official Dutch text of the *Jaarverslag TIB 2021* prevails.

It was TIB's intention to report on bulk interception and 'strategic operations'. These are special investigatory powers that require particular clarity in terms of scope and impact, not least because of the legislative proposal currently submitted to internet consultation in which the services are intended to have more scope to conduct bulk interception and 'strategic operations'. However, the Minister of Internal Affairs and Kingdom Relations and the Minister of Defence feel that some sections offer too great an insight into the services' modus operandi and should therefore be classified as state secret. The TIB has therefore blacked out these sections. The Intelligence and Security Services Committee will be sent an unredacted version.

Summary

The review process

In the 2021 calendar year, the TIB assessed a total of 3,071 requests by the AIVD and the MIVD. The number of requests is growing each year and the scope and technical complexity of the requests is also on the increase. For 3.3% of the requests by the AIVD, the TIB ruled that the authorization had been granted unlawfully. That was 1.9% in the previous reporting period. For 7.1% of the requests by the MIVD, the TIB ruled that the authorization had been granted unlawfully. That was 8.1% in the previous reporting period. These percentages/figures could have been higher. In some cases the TIB asked questions about the proposed requests at which the Minister subsequently repealed the request.

In 2021 the AIVD unlawfully applied the urgency procedure six times (which involves using the procedure before the binding decision by the TIB). The use itself was found to be unlawful three times, two of which involved a journalist. Compared with the previous reporting period, there is a marked increase in the number of special investigatory powers ruled to be unlawful because they were either not proportional or not as targeted as possible.

Cable interception

In 2021 two requests were submitted to intercept cable internet traffic. The TIB ruled the requests for production (i.e. the actual interception of internet traffic on the cable for the intelligence process) as unlawful. In the first request it was likely that a significant amount of internet traffic from people, including Dutch citizens, would be stored and a part of that data would be shared unseen with a foreign partner service. However, there was no specific description of the expected yield that would justify the interception. In the TIB's view, the second request failed to provide sufficient clarity on the safeguards. That could lead to a situation in which analysts would be able to track which websites were visited when by Dutch citizens.

Information provision

The TIB established that in 2021 the AIVD failed to correctly or fully inform the TIB about the content of requests. In a number of cases that was clearly an administrative mistake or a misunderstanding. In three cases this led to a ruling of unlawful conduct. In none of those cases did information appear to be withheld on purpose.

In addition, the TIB was informed in 2021 that since 1 May 2018 both services used an unknown vulnerability to enter an automated device or system, without reporting this in the authorization request. That also happened in cases where, at the time of drafting the request for authorization, it was already clear that the vulnerability would be used. The TIB was unable to carry out its legal task to assess the technical risks in those cases because essential information was missing. This annual

report describes one case in which the TIB would not have come to a ruling of lawfulness if that information had been shared in advance.

Table of contents

About the TIB

The TIB is an independent review committee charged with reviewing the lawfulness of the authorizations granted by the minister of Internal Affairs and Kingdom Relations and the minister of Defence for the use of certain special investigatory powers by the General Intelligence and Security Service (hereinafter: AIVD) and the Military Intelligence and Security Service (hereinafter: MIVD). The TIB's assessments include the authorization for a request to intercept a phone or to hack a computer, but also to hack larger computer systems and for the large-scale interception of telecommunication via satellite or cable. The relevant minister grants authorization for the use of an investigatory power by signing the request. In practical terms therefore, the TIB assesses the contents of that written request. For readability purposes, this report will refer to assessing requests or reviewing requests as lawful/unlawful instead of assessing the authorization of the minister for requests.

The different aspects that the TIB assesses can be found mainly in the Intelligence and Security Services Act 2017 (ISS Act 2017). In its lawfulness assessment, the TIB assesses whether it is necessary to use the investigatory power. The importance of the investigatory power to be used is weighed against the infringement of privacy the use will cause (proportionality). The next aspect to be assessed is to see whether the lightest remedy was used to obtain the required information (subsidiarity). Lastly, the use of the investigatory power is assessed to see whether it is as targeted as possible. The TIB's ruling is binding. That means that if the TIB rules that an authorization granted by the minister is unlawful, that investigatory power may not be used.

The TIB's composition and investigatory powers are incorporated in the ISS Act 2017. The TIB consists of three members, of which two have extensive experience in the judiciary. The third member was appointed for their technical expertise. The members of the TIB are supported by a secretariat. Since February 2022, the TIB also has deputy members.

Preface

Since last year's annual report appeared, much has changed in the world. The images of destroyed cities, displaced people and victims appear on our television screens every evening. You could wonder if under these circumstances, assessing the investigatory powers used by the Dutch services is an unnecessary luxury. Surely it is better to relax all rules to combat cyber threats, such as the previous minister of Defence suggested in an interview with NRC newspaper: "Countries such as Russia and China do what they like, but we have ethical principles and rules."

However, as far as the TIB is concerned, assessing far-reaching investigatory powers is certainly not a luxury. On the contrary, our constitutional state is a precious commodity, not a possession to be taken for granted. It is a complete package which means you cannot cherry-pick the safeguards you want or put them aside when they are inconvenient.

On the other hand, national security in our country and that of our allies is under pressure. Security is a precious commodity too. Striking the right balance between protecting our national security and the privacy of the general public is crucial for a democratic state to function properly. Since its foundation in 2018, the TIB stands for striking that balance. As an independent assessing body, the TIB studies the requests of both services in detail on a weekly basis and assesses the granted authorization on lawfulness.

At this time, or rather particularly at this time, the privacy of citizens needs to be protected in addition to national security. The general public in the Netherlands should feel free to communicate by phone, by the internet, or by whatever means. Intercepting communication can be crucial but must be overseen effectively.

The services have asked the legislator for more scope to conduct cyber investigations. At the time of writing this annual report, the draft bill was under consultation. The TIB was partly involved in drafting the bill. Each time, the TIB pointed out the need to uphold the legal safeguards. Effective oversight of the services serves as a safeguard to protect the privacy of the general public, but is also important because of the trust that the public places in the constitutional state.

In the coming year, the TIB will conduct its review process thoroughly and keenly to retain the right balance between the protection of our national security and the privacy of the general public.

Mariëtte Moussault,
Chair of the Investigatory Powers Commission

1. Developments in the review process

In 2021 it emerged during the TIB's regular review process that the services had again failed to inform the TIB fully or correctly on a number of occasions. However, the services took the initiative to inform the TIB themselves in the first quarter that they had failed to inform the TIB fully and correctly in the use of unknown vulnerabilities in hacking operations. These incidents are discussed in section 1.1.

During the past year, the services twice submitted requests to intercept internet traffic on the cable. The TIB ruled the authorization for requests for production (i.e. the actual interception of internet traffic on the cable for the intelligence process) as unlawful. At the end of 2021, the TIB did consider lawful the authorization for an AIVD request to explore certain data flows of internet traffic on the cable (snapshotting). That is discussed in section 1.2.

Furthermore this section discusses the following developments. Section 1.3 sketches the new legislation relevant to the TIB. Section 1.4 takes an in-depth look at strategic hacking operations, following on from the previous annual report. Finally, section 1.5 reports on drafting the assessment framework for organizational requests.

1.1. Information provision from the services

1.1.1. Incorrect information regarding operations

For its lawfulness assessment, the TIB is primarily dependent on the information contained in the requests. Partly because of the state secret nature of the operations, the TIB is unable to consult public sources. Moreover, the TIB is unable to search the services' systems, unlike the CTIVD. The ISS Act 2017 offers the TIB the possibility to ask the ministers questions based on the requests, and the TIB regularly does so. In practice, these questions are addressed directly to the services and the TIB receives the reply from them.

In 2019 and 2020 it repeatedly emerged that the originally provided information in the request was incomplete or even incorrect. At the time, meetings were held between the TIB and the management of the AIVD to improve the situation.

However, in 2021 the TIB again received information from the AIVD that was incomplete or incorrect. In a number of cases that was clearly an administrative mistake or a misunderstanding and not decisive for the review. In three cases a ruling of unlawful conduct was ultimately made based on the full and correct information. The authorization for those requests had partly been based on information that proved to be factually incorrect. The AIVD reported in those three cases that the information had emerged as facts from their own independent investigation. But each time after enquiring from the AIVD, the TIB learned that that information was incorrect. In none of the cases

did this appear to have been done on purpose. The provision of information continues to be a topic of discussion between the AIVD and the TIB.

1.1.2. Incorrect information regarding use of 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? And what are the consequences, for example, for the users who depend on that system? These are relevant questions, 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 reviews 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 can easily enter systems in the Netherlands or with our allies.

Over the past years, the TIB repeatedly stressed that unknown vulnerabilities may only be deployed if their use is explicitly substantiated in a request. The TIB should be fully informed about the proposed use of an unknown vulnerability so that the technical risks can be properly assessed. The TIB then includes that information in its proportionality assessment.

Mid-2021, the director of the MIVD and the director-general of the AIVD notified the TIB that internal investigation had revealed that since 1 May 2018 an unknown vulnerability had been used in a number of operations, without that information being included in the request. They indicated that the technical risks reported in the requests were in line with the technical risks connected to the use of the unknown vulnerability.

The TIB conducted an analysis of the operations in question. One operation involved entering [redacted] to obtain data from [redacted][1]. The request stated that it was unknown how entry would actually take place and that therefore the technical risks had been described in general terms only. In retrospect it appeared that the service in question had known in advance how to hack using the unknown vulnerability, and that on top of that, the vulnerability had been unencrypted when exploited. The unencrypted exploitation of an unknown vulnerability can lead to both the 'exploit code' and the susceptible automated device or system becoming known to others, for example to other countries with signals intelligence capacity. That means a risk of third parties gaining access to the same automated device of [redacted] using the same unknown vulnerabilities.

[1] The TIB was not allowed to use the word written here. For readability purposes, the term 'people' can be used in those cases.

In July 2021, the TIB concluded in its letter to the ministers that it would not have ruled the request as lawful if it had been aware of the relevant facts and circumstances that were known to the service at that time. The TIB also stated that its focus on a single operation in the letter did not mean that it agreed with the services' conclusion that the described technical risks were in line with the risks involved in the use of the described unknown vulnerabilities.

1.2. Investigation-related interception on the cable

During the drafting stage of the ISS Act 2017, the services' new investigatory power to be able to intercept large amounts of internet traffic on the cable attracted a lot of public and political interest. That investigatory power does not need to be targeted to specific people or organizations under investigation by the services. The services are allowed to conduct far broader investigations into phenomena and subjects to expose known and unknown threats. The investigatory power involves both intercepting internet traffic on the cable to determine if it potentially contains enough intelligence value (known as snapshotting) and intercepting certain data flows within that internet traffic for a certain length of time (production).

Cable interception may not be conducted without a prior lawfulness assessment by the TIB. The TIB reports annually on this investigatory power, in light of its special nature.

The TIB received requests from both services in June 2021. Both ministers granted authorization to use cable interception on [redacted]. These requests to intercept cable internet traffic were for both snapshotting and production purposes in two areas investigated by the services. The TIB ruled that the proposed use of that cable interception was not proportional, not subsidiary and not as targeted as possible.

It was not proportional because the services' interest was not proportionate to the infringement of privacy. Compared with a previous request, 6-8 times more internet traffic would be intercepted while several important safeguards were removed. It was likely that a significant amount of the internet traffic from people including from Dutch citizens would be stored and a part of that data would be shared unseen with a foreign partner service. The requests did not contain any specific description of the expected yield that would justify the interception. Nor was it clear from the requests how the services would conduct their work in as targeted a way as possible. It was unclear which technical filters would be used. In addition, there was insufficient substantiation that this means of cable interception was the lightest remedy to conduct the investigation assignments. The services have other legal, more targeted acquisition options regarding telecommunication service providers and providers of data storage. The services were unable to explain convincingly why untargeted cable internet traffic needed to be obtained from a number of these providers.

The requests were therefore ruled to be unlawful. The TIB substantiated its ruling in detail and afterwards also provided an explanation in a meeting with the ministers and the services.

In November 2021 new requests were submitted for both snapshotting and production purposes. Prior to that, a delegation of the TIB was sent a number of presentations relating to the technical aspects of conducting cable interception.

The TIB ruled the requests for production as unlawful. That was because as regards the intended cable route, the potential intelligence value had not been adequately substantiated, for example by advance snapshotting. The request referred to investigation results relating to snapshotting on another cable route. That was particularly relevant because the intended cable route involved traffic in an opposite direction to the one used in the investigation referred to. Therefore there was insufficient evidence that the use on this cable route was as targeted as possible. That in itself was a ground for unlawful conduct.

In its ruling, the TIB expressly raised the issue of the continual lack of clarity on whether or not the use is as targeted as possible, and thereby also on the proportionality. The aim was to only store cable internet traffic if it has certain characteristics. Even after questions had been raised it remained unclear which specific safeguards or limits would be linked to determining those characteristics. The TIB established that the use of the investigatory power would potentially provide a view into the internet traffic between millions of people. That could lead to a situation in which service employees could track which websites were visited when by Dutch citizens. In fact, its use would lead to a similar result as the one submitted to the TIB in June 2021.

The TIB did rule that request that concerned exploring the cable (snapshotting) as lawful in December 2021. That means that for the period of one year, the services will be able to use the investigatory power to intercept the aforementioned cable route in order to assess its potential intelligence value.

1.3. Developments in legislation and regulations

1.3.1. Report by the Evaluation Committee ISS Act 2017

The Coalition Agreement of the Rutte III government agreed to evaluate the ISS Act 2017 within two years of its introduction on 1 May 2018. The ISS Act 2017 Evaluation Committee took on this substantial task and presented its final report to both Houses of Parliament and the general public on 20 January 2021.[2]

The TIB posted a short news message on its website the same day, saying it was pleased with the Evaluation Committee's observation that the TIB "*is of great added value to the oversight system*" and the advance binding assessment is "*a significant safeguard that was added to the system*." At the same time, the TIB draws attention to this Committee's proposals to limit the TIB's substantive review in future and even to put an end to a review by the TIB for the use of a number of investigatory powers. The TIB warned that this would mean a decline in the balance between protecting national security and the privacy of the public, and subsequently the safeguards of the rule of law.

That warning was repeated by the chairpersons of the TIB and the CTIVD in an interview with NRC newspaper on 7 March 2021. One of the ISS Act 2017 Evaluation Committee's proposals included restricting the TIB's review to the acquisition of data only. The manner in which the services intend to handle the acquired data would not be included in the review. In the interview, the TIB's chairperson said that he feared the proportionality check would be eroded if that proposal were to be adopted.

The TIB's chairperson gave an explanation to committees of both Houses of Parliament during a technical briefing about the ISS Act 2017. The chairperson pointed out that the new proposal means that important aspects of an operation would no longer be weighed.

By way of illustration he sketched the situation where the services were able to hack a telecom provider with millions of users to obtain telephone and traffic data of just a couple of targets. That might be a necessary move, but it is not automatically proportional. As the situation is now, the TIB would, in the context of the proportionality issue, be able to take into account whether the data of innocent users would be destroyed immediately or not. The TIB would also be able to take into account whether or not an acquired dataset would be declared relevant in its entirety, which de facto means that the telephone and internet data of millions of users could be retained indefinitely. The consequence of the strict distinction as proposed by the ISS Act 2017 Evaluation Committee is that those aspects would no longer be taken into consideration.

[2] Evaluation Committee report entitled "*The 2020 Evaluation of the ISS Act 2017*", accessible on rijksoverheid.nl.

For the TIB that could mean having to issue more rulings of unlawful conduct than now, or becoming nothing more than a rubber stamp. That could damage national security or the privacy of the general public.

An extensive amendment to the ISS Act 2017 is expected during this current government's term.

1.3.2. Limited amendment of the ISS Act 2017 in 2021

The ISS Act 2017 was amended mid-2021. The government had already seen cause to amend the Act on a number of points in 2019, which concerned several safeguards that had to be added to the Act. Those safeguards, the criterion of as targeted as possible where it concerns the use of special investigatory powers (including cable interception) and the accelerated weighting of cooperation with foreign services had already been set out in binding policy rules.

In addition to recording the above policy rules in the Act, some minor amendments were also made. Most important to the TIB was the addition of a legal possibility to appoint deputy members, making it possible to replace a member in case of absence or inability to be present. That need for substitution was underlined during the pandemic. Fortunately in the whole of 2021, Covid did not cause any delays in the review of requests.

1.4. Strategic hacking operations

As reported in the 2020 Annual report, both services made a repeated request last year for using the hacking power with no more than a strategic substantiation. That means that the proposed use was not specifically aimed at obtaining information, but mainly aimed at increasing knowledge or options. In the previous annual report 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.

The legislator did not express an opinion, when the ISS Act 2017 was drafted nor when the opportunity arose to amend the Act as discussed in section 1.3.2., 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). The TIB feels it is advisable that the legislator gives its general opinion on the admissibility of the hacking power used purely on strategic grounds and what the framework for that use is. Until that time, the TIB will continue to review these requests within its regular review framework. That means that the criteria of necessity, proportionality, subsidiarity and as targeted as possible must be reflected in the contents of the request.

In the 2021 calendar year, both services submitted requests to be allowed to conduct operations that were purely strategic in nature. Several extension requests in these operations were also submitted. In a number of cases that led to lawfulness rulings and in others to rulings of unlawful conduct. Given the state secret nature of the operations, the TIB is unable to provide further details in this report. However, the TIB can disclose here that in the 2021 calendar year it reviewed a

number of requests for which authorization had been granted that could be described as being vastly wide-ranging in nature. The TIB ruled 8 operations as unlawful partly or solely because the TIB did not consider the operation proportional. One case involved the intention to take a position with [redacted]. From that position [redacted].

In two other cases lawful authorization had been granted to conduct an operation as a result of which a strategic position was obtained with several parties. These were longer running operations and their yield was not always sufficiently transparent. Precisely in the case of a hack on a non-target, where the privacy of a great many users is affected, will the requirements on the yield be high. That information is therefore essential to review the necessity and proportionality of the request to extend the use. The TIB asked the services in 2021 to list in their extension requests what yield the use specifically provided per party. That gave a very mixed picture and sometimes the yield proved to be very limited. In those cases the TIB ruled that the extension of the use against those parties was not proportionate and therefore unlawful.

1.5. Organization requests

Under the ISS Act 2017 the services may use special investigatory powers aimed at people, but also at a group of people making up an organization. In the latter case, the ISS Act 2017 provides scope in some cases for new people 'to be added' without prior authorization by the minister to the request while the investigatory power is being exercised. The special investigatory power can then immediately be used against the added people. Only when an extension is requested can the TIB assess whether those people in the new request were categorized correctly as members of the organization. It is precisely for this reason that organization requests must comply with certain requirements, which are described in the CTIVD's review report no. 40.[3]

The TIB established that in the course of 2020, the organization requests by both services had increased in size and scope for the requested use of investigatory powers. As a result, the overview that the TIB needs to conduct its lawfulness assessment came under pressure. Furthermore, the TIB established an increase in the number of times when it was unclear who was regarded as a member of the organization under which circumstances.

With a view to the importance of a foreseeable review of organization requests, the TIB and the CTIVD made a start in the first half of 2021 with developing an assessment framework. The oversight bodies consulted a number of times with the services' official staff in 2021, mainly to establish whether the implementation of the assessment framework was feasible or could lead to unforeseen, negative effects when put into operation. The assessment framework was adopted by the TIB and the CTIVD in December 2021.

[3] Review report 40 on the use by the AIVD of the interception power and the power to select sigint, CTIVD review report 40, 7 October 2014.

The assessment framework for organization requests specifies the requirements taken as starting point for the assessment of organization requests. That includes the requirements set by the oversight bodies to a description of an organization. The assessment framework also specifies the oversight bodies' expectations for describing the scope of a request. The assessment framework contains various examples of reviewed requests.

From 1 February 2022, the oversight bodies will use the assessment framework when reviewing requests. The assessment framework has not been published. Instead it has been classified as state secret because the document contains several examples of requests in ongoing intelligence operations. The document has been drafted for practical use by the services' processers who draw up the requests.

In advance of the framework's introduction, the TIB questioned the description and demarcation of organizations in a large number of operations in 2021, because it found them to be insufficiently clear. That resulted in many authorization and extension requests being clarified and demarcated in greater detail.

During the 2021 calendar year, the TIB ruled in 13 cases that the authorization for a granted request was unlawful because there were issues with the description and demarcation of an organization. In a number of cases it was completely unclear who could be added when. That could lead to the services intercepting or hacking communication from totally innocent people without any prior assessment. In other cases the scope had been defined in such broad terms that people who would obviously not be able to contribute to the investigative questions being answered could still be added. In other words, on paper investigatory powers could be used against people without there being a need to.

2. The lawfulness assessment in numbers

The number of requests that the TIB assessed has increased in 2021. The TIB not only sees an increase in the number of the services' requests, but also an increase in their size and technical complexity. In 2021 there was a rise in the percentage of rulings of unlawful conduct in the AIVD's requests. The percentage of rulings of unlawful conduct in the MIVD's requests dropped. Particularly striking in 2021 was the rise in the number of unlawful conduct rulings where the TIB ruled that the proposed operation was not proportional.

2.1. Overall view of the requests

In the 2021 calendar year, the TIB assessed a total of 3,071 requests for lawfulness. That is the total number of requests by both services.[4] The previous annual report had already remarked on the sharp increase in the number of requests by both services. In 2020 there was a marked rise not only in number, but also in scope and technical complexity – a trend that continued in 2021.

This year is the first time the TIB reports on a current calendar year. The fact that previous reports were issued on 'broken' periods was prompted by the starting date of the Investigatory Powers Commission (TIB) on 1 May 2018. For this annual report, the TIB created an overview of the number of requests it reviewed for lawfulness over the past three calendar years.[5] These figures show that, in 2021 too, there was an increase in the number of requests. Partly in light of that, the staffing level of the secretariat was expanded over the course of 2021 as described in section 4.

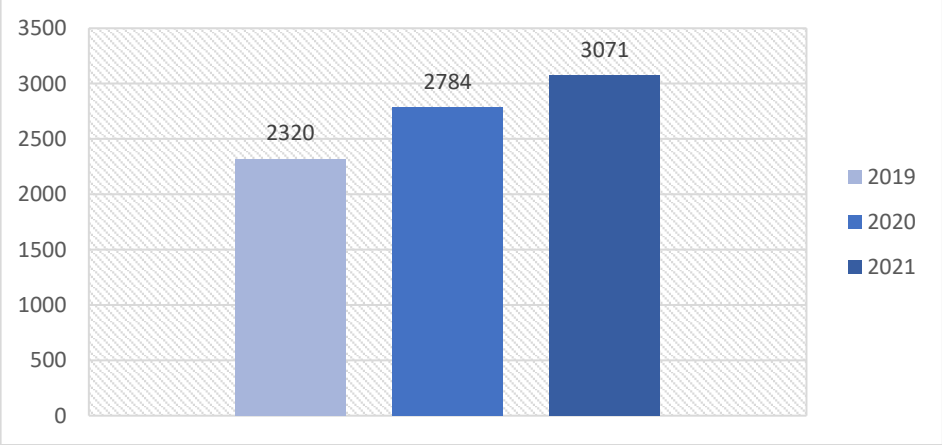

Figure 1: number of requests per calendar year

[4] There is no overview here of the number of submitted requests per service, as the ratio between requests by the AIVD and the MIVD is classified at the time this annual report was drafted.

[5] The first year of review by the TIB ran from 1 May 2018, the day on which the ISS Act 2017 entered into force. For that reason it was not included in the overview.

As mentioned above, the TIB also sees an increase in scope and technical complexity, mainly in strategic hacking operations, a category of requests described in section 1.4. The TIB ruled in a number of cases that the proposed operation was not proportional. Partly because of that, the number of rulings of unlawful conduct based on the proportionality criterion rose in 2021.

In that year, the TIB questioned the AIVD in 9.7% of cases. In the previous reporting period, the TIB questioned the AIVD in 8.4% of cases. The TIB questioned the MIVD in 17.9% of cases in 2021. That was 24.7% in the preceding reporting period. The graph below shows the number of questions that the TIB posed compared with the number of requests assessed on lawfulness. By and large it is clear that in an increasing number of reviewed requests, the TIB asked further questions. That coincides with the TIB's impression of the past year – in more cases than previous years the TIB decided to first ask further questions instead of immediately coming to a ruling of unlawful conduct.

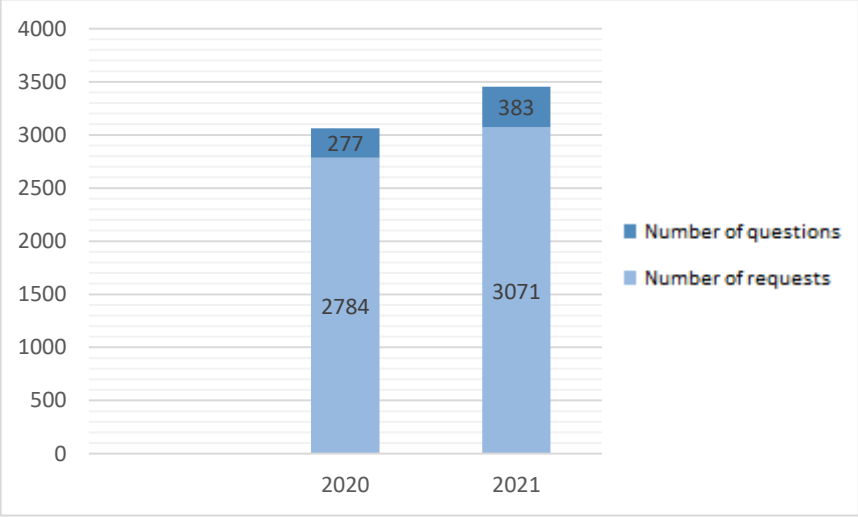

Figure 2: number of questions compared to the number of requests per calendar year

2.2. Repealed requests

In 2021 some requests were repealed before the TIB had issued its ruling on the lawfulness of the granted authorization. That was the case in a total of 18 requests, 7 by the MIVD for which the Minister of Defence had signed and 11 by the AIVD for which the Minister of Internal Affairs and Kingdom Relations had signed.

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

Requests were repealed mainly after the TIB had asked questions, for example about the way in which a special investigatory power would be used specifically. Although it is not clear in all cases, the TIB suspects that by repealing the requests, a ruling of unlawful conduct was prevented more than once. In some cases the TIB's questioning was given as specific reason for the repeal.

One example is a request for an extension of an operation against a target organization. A number of people had been added (see section 1.5). The request did not elaborate why these people belonged to the target organization nor why the service wished to use the investigatory power against them. The TIB asked questions about this. Subsequently the minister involved stated that those people were not part of the organization and that the request was therefore repealed.

The increase in the number of repealed requests by both services is striking – in the previous reporting period there were only a few cases (3 AIVD requests and 2 MIVD requests).

2.3. Grounds for unlawful conduct rulings

As stated above, the TIB assessed 3,071 requests in total in 2021. For 3.3% of the requests by the AIVD, the TIB ruled that the authorization had been granted unlawfully. That was 1.9% in the previous reporting period.

The MIVD saw a 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 8.1%. That had dropped to 7.1% in 2021.

When a request to use a special investigatory power is assessed as unlawful, the service can opt to submit a new and amended request. That new request could then be found lawful, for example because additional safeguards were attached to the use of the special investigatory power. In the reporting period, 67.2% of the unlawful requests were later assessed in a significantly revised form to be lawful. In the other 32.8% of cases, requests ruled as unlawful by the TIB were either not resubmitted by the services or were again ruled unlawful. That percentage was more or less the same as in the previous reporting period. There was a slight decrease, from 69% in last reporting period to 67.2% in 2021.

The figure below shows why the TIB arrived at its ruling of unlawful conduct. 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.

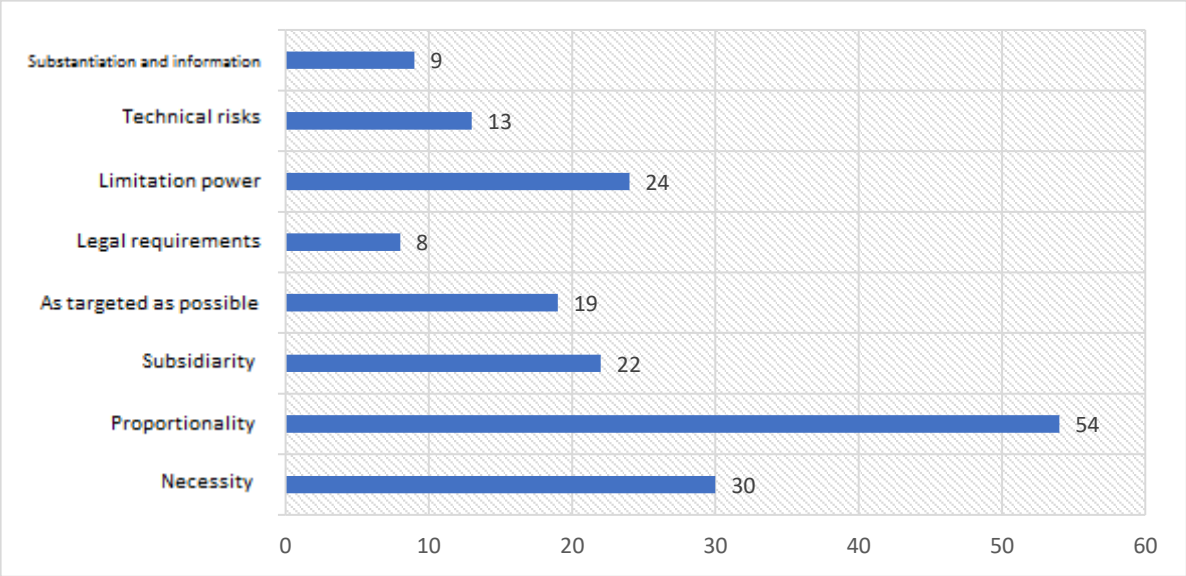

Figure 4: grounds for unlawful conduct rulings 2021, numbers in absolute terms

Explanation to the review elements
The TIB assesses if the use of a special investigatory power is necessary, if its use is not disproportionally detrimental compared to the necessity (proportionality), if the goal can also be achieved through less invasive investigatory powers (subsidiarity) and if the investigatory power is as targeted as possible. In addition, the TIB also assesses other aspects of lawfulness. The ISS Act 2017 sets down requirements for a request such as an indication of the proposed goal of an operation. Are these legal requirements met? In addition, the ISS Act 2017 specifies the scope within which the services may act. One example is when a request concerns a journalist. The minister is not permitted to grant authorization, only the Court of The Hague may do so. The TIB reviews whether the limits of the Act are not exceeded. Furthermore, it is important that the requests to use investigatory powers contain sufficient correct information about the relevant facts and circumstances, but also that the required elements relating to the proposed use of the investigatory power are adequately substantiated. Where the hacking power is concerned, the technical risks must be explicitly described.

The above figures show the grounds for unlawful conduct. Thus proportionality is often an independent ground for unlawful conduct, whereas it is relatively rare that granted authorization is deemed unlawful because it did not comply with a legal requirement.

In three different requests in 2021 the minister granted authorization for the use of a special investigatory power against a person, who according to the TIB should have been designated a journalist. The minister should have asked the Court of The Hague to authorize the use. In one case, further investigation revealed that the authorization granted by the Court was still insufficient reason to designate the person in question as a journalist.

The significance of the information above becomes clearer when the 2021 figures are compared with those of the preceding period (1 April 2020 to 31 December 2020). See the graph below.

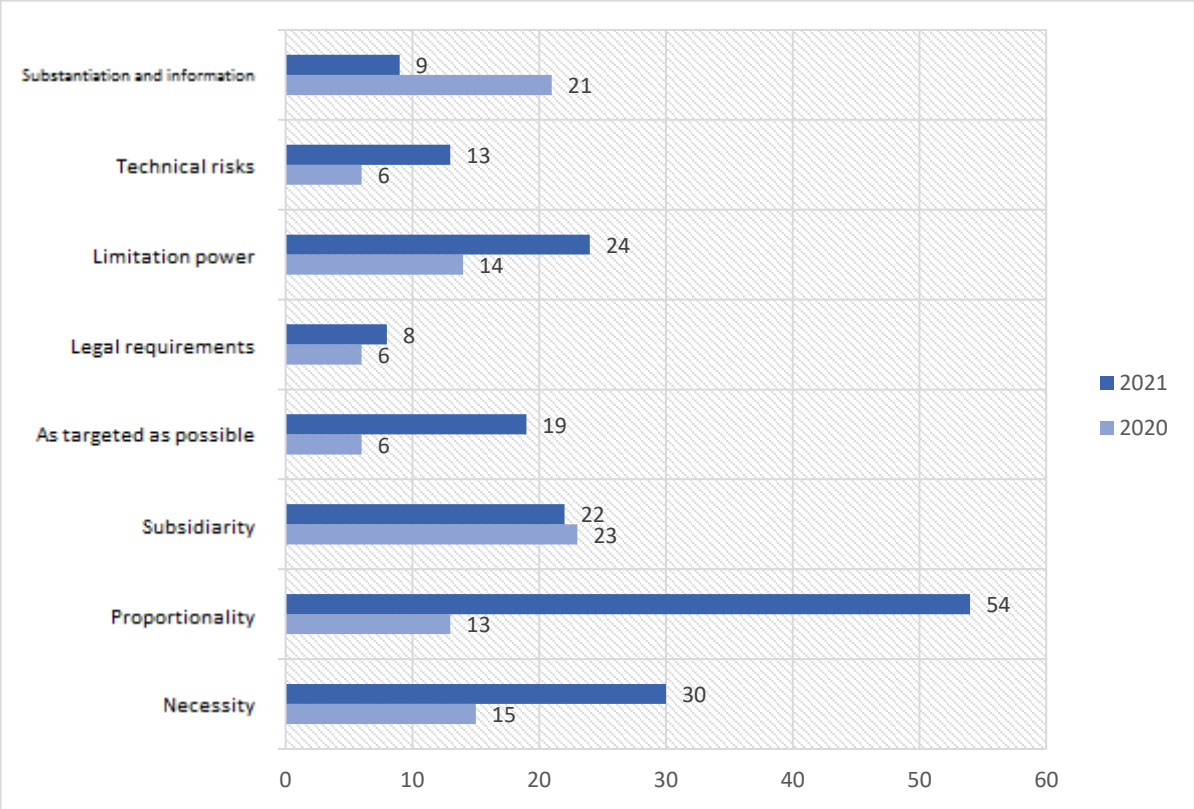

Figure 5: comparison grounds for unlawful conduct reporting periods 2020 and 2021, numbers in absolute terms

Compared with last reporting period a number of things stand out. Most striking is the marked increase in the number of times that the TIB ruled that the use of the special investigatory power was not proportional. Where in the past reporting period that was an independent ground for unlawful conduct in 13 cases, in this reporting period that had risen to no fewer than 54 cases. A significant increase is also visible for the criterion as targeted as possible, which is closely connected to proportionality. That increase cannot be explained only by the increase in the number of requests in 2021.

On a positive note, the number of rulings of unlawful conduct because of a lack of substantiation and information has more than halved. One explanation is that in more cases the information was shared with the TIB after questions had been asked.

2.4. Assessment of the use of the urgency procedure

The ISS Act 2017 contains a procedure for urgent cases where 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. However even in urgent cases, the minister must first grant authorization. The granted authorization must afterwards be submitted to the TIB for a lawfulness assessment as soon as possible. If the TIB rules that the granted authorization is unlawful, all information that was obtained using this investigatory power must be destroyed immediately. The TIB also assesses the appropriateness of the urgency procedure itself. If the urgency procedure was

used wrongly, the TIB must subsequently determine what should be done with the obtained information.

In 2021, the TIB assessed a total of 3,071 requests for lawfulness. The urgency procedure was invoked in 3.6% of those requests. In the previous reporting period, the TIB 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. That was different in 2021.

In this reporting year, the AIVD applied the urgency procedure in 101 different operations. In 3 of those, the TIB ruled that the use of the special investigatory power was unlawful. Those cases concerned hacking a target's telephone and also hacking and intercepting a target's mobile phone. In the latter case the TIB concluded the use was unlawful because the target should have been designated a journalist. The minister should have asked the Court of The Hague to authorize the use.

Where the AIVD is concerned, the TIB concluded that the urgency procedure was used unlawfully in 6 cases. The regular procedure should have been followed in those cases. The TIB ruled in all 6 cases that no consequences should be attached to this unlawful conduct, because the operational necessity and facts and circumstances of those specific cases gave rise to it.

In this reporting year, the MIVD applied the urgency procedure in 10 different operations. The authorization granted for one of those operations was ruled by the TIB to be unlawful.

3. Looking ahead

The TIB expects the number of requests by both services to further increase in 2022, in part because of the additional investments recently pledged in the field of national security.

Legislation is set to change as well in 2022. A major amendment of the ISS Act 2017 is currently being prepared. In that context, a framework memorandum is being developed and a number of analyses have been conducted, shared with the House of Representatives and made public.

The government is meanwhile working on a bill to amend the ISS Act 2017 in some areas in anticipation of the major amendment. According to the government, that is necessary to continue to protect The Netherlands against countries with an offensive cyber programme. The government recognizes that this is only possible if sufficient safeguards and effective oversight is in place.

In both cases the TIB considers it important to continue to strike a balance between protecting national security and ensuring the privacy of the general public. The TIB will continue its efforts in that area.

4. Composition of the TIB

The TIB's composition and investigatory powers are incorporated in the ISS Act 2017. The TIB consists of three members. Two of those have extensive experience in the judiciary while the third member is appointed based on technical expertise.

For the whole of 2021, the TIB has been at full strength in terms of composition. The review process was not disrupted during the entire year as a result of the covid pandemic. However there have been some weeks in which requests were not assessed by the full commission. That was mainly because a member was on leave or unable to be present. From February 2022, it has become possible to call in a deputy member in those cases.[6]

At the beginning of 2022, Mr A.R.O Mooy, LLM, stepped down as member of the TIB, leaving a vacancy. At the time of drafting it has become clear that he will be succeeded by Mr E.H.M. Druijff, LLM on 1 May 2022. More on his appointment on our website. At the time of publishing this annual report, the composition of the TIB is as follows.

Ms M. Moussault, LLM
chairperson

Mr A.W.R. Hubert
technical member

The commission is supported by a secretariat. The TIB's general secretary, Mr L.W. Schroijen leads the secretariat.

[6] See also Section 1.3.2.