Wetenschappelijk Onderzoek- en Documentatiecentrum

Cahier 2022-8

De hackbevoegdheid in de praktijk

Een empirisch onderzoek naar de uitvoering van de hackbevoegdheid (artikelen 126nba, 126uba, 126zpa Sv)

Summary

Wetenschappelijk onderzoek- en kennisinstituut voor het ministerie van Justitie en Veiligheid

Cahier 2022-8

De hackbevoegdheid in de praktijk

Een empirisch onderzoek naar de uitvoering van de hackbevoegdheid (artikelen 126nba, 126uba, 126zpa Sv)

Summary

A. van Uden
C.A.J. van den Eeden

Met medewerking van:
J.J. van Berkel

Cahier
De reeks Cahier omvat de rapporten van onderzoek dat door en in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum is verricht. Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Justitie en Veiligheid weergeeft.

Summary

The hacking power in practice

An empirical study into the implementation of the hacking power (Sections 126nba, 126uba, 126zpa of the Dutch Code of Criminal Procedure)

The Computer Crime Act III (Wet Computercriminaliteit III; hereinafter the Act) came into force on 1 March 2019. The Act sets out a statutory basis for the 'hacking power' in the Dutch Code of Criminal Procedure (Wetboek van Strafvordering; Sections 126nba, 126uba and 126zpa Sv). The new investigative power allows law enforcement officials 'to access computerised systems remotely by stealth, under certain conditions, that are used by suspects, with a view to certain investigative objectives in the area of the investigation of serious criminal offences'. After accessing a computerised system (such as a mobile phone or a server) the police may carry out a number of investigative activities, namely: A) establishing specific characteristics of the computerised system or of the users thereof, such as their identity or location, and documenting such details; B) executing an order to record confidential communications or wiretapping and recording communications; C) executing an order for systematic observation; D) documenting data stored in the computerised system; and E) making data content inaccessible. These activities may only be carried out by specially designated investigating officers who are part of a special team of the Central Unit (Landelijke Eenheid) of the Dutch national Police. The Computer Crime Act III also includes a number of grounds with regard to the use of the hacking power either under or pursuant to an Order in Council, as was the case in the Investigations into Computerised Systems Decree (Besluit onderzoek in een geautomatiseerd werk; hereinafter the Decree).
The current report consists of an evaluation of the process surrounding the implementation of the hacking power in the first two years after the Act came into force. Another report is to follow at the end of 2024, containing the second part of the evaluation, which will focus on the implementation of the Act in full. The principal question in this study was:

How is the hacking power put into practice and are there any particular problems that arise in the application of the hacking power in the investigative practice?

A combination of research methods was used to answer the research question, including document analysis, interviews and case review. This summary provides an outline of the key findings and conclusions, initially focusing on the process surrounding the execution of the hacking power. Next, a number of issues are highlighted in relation to which notable difficulties have arisen.
As a preface to all of this, it is vital to note that both technical and tactical actors are involved with the power and its implementation, the former represented by Digit (Digital Intrusion Team). Digit itself consists of two components: Digit (Police) and Digit (Public Prosecution Service). Implementation of the hacking power is in the hands of Digit (Police), part of the Central Unit of the Dutch national police. Digit (police) is managed and led by Digit (Public Prosecution Service), which is part of the National Public Prosecutors' Office of the Public Prosecution Service. Any intervention

with the hacking power by Digit (hereinafter: intervention) takes place within an ongoing criminal investigation, which is carried out by a tactical police team (such as a team of the district criminal investigation team or
the National High Tech Crime Unit) under the authority of the Public Prosecutor handling the case. This Public Prosecutor bears ultimate responsibility for the criminal investigation in which Digit carries out an intervention, and he/she is accountable to the court when the case is heard by a judge in a trial court.

Hacking power implementation process

Intake and assessment

The encryption of data has emerged in this study as a key reason as to why tactical investigation teams want to make use of the hacking power. Many other (special) investigative powers have often already been deployed and have not led to the desired information. If a tactical team is considering an intervention, it will consult Digit. Not every request, however, will lead to the use of the hacking power. Over the past two years, the majority of requests submitted to Digit (over two-thirds) were not actioned, due to both technical and tactical concerns.
Whenever a tactical team submits a request this is followed by an extensive intake process. This process consists of two procedures that partly take place sequently and partly take place simultaneously: an operational process and procedure for the legal assessment of the intervention. Within the operational process, Digit reviews whether an intervention is technically and tactically feasible. If this is the case, the tactical team will begin working on a (draft) application proposal for the use of the power, with Digit (Public Prosecution Service) monitoring the drafting process. Digit (Police) focuses on making an assessment of the technical feasibility of an intervention and of any potential risks or difficulties.
In addition to the operational process, an extensive, legal assessment procedure is carried out prior to the actual use of the hacking power. The proposed use of the power is discussed inter alia within the Central Assessment Committee (Centrale Toetsingscommissie, CTC) – an internal advisory body within the Public Prosecution Service. During the CTC meeting, attention is devoted both to the tactical relevance of the intervention using the power in the criminal investigation (by the Public Prosecutor handling the case) and the technical side (if necessary, clarified by Digit (Public Prosecution Service)). The CTC issues a positive recommendation in respect of the vast majority of requests. Ultimately, authorisation must be obtained from the Examining Magistrate on the basis of which the Public Prosecutor handling the case will issue an order to Digit (Police). During the assessment process outlined above, Digit (Public Prosecution Service), in consultation with Digit (Police), plays a key role in respect of all the various players involved, both as a source of information and adviser. This applies especially to the technical aspects of any intervention. The remainder of the actors involved rely on this expertise, and the fact that this responsibility rests on the shoulders of one or two persons makes the position of Digit (Public Prosecution Service) vulnerable.

Use of the hacking power

Once an order has been issued, Digit begins working on the application of the hacking power. Between March 2019 and March 2021, orders were issued in 26 criminal investigations, which means that a minority of requests from tactical teams was

granted. Contrary to what the name computer crime suggests, over the past two years the hacking power has mainly been used in criminal investigations into more serious forms of traditional crime such as (attempted) murder, cases involving narcotics, falsification of documents, money laundering, sexual offences, terrorism and membership of a criminal organisation. Only one intervention is related to cybercrime in the narrow sense.

Interventions by Digit can also be extended, which applied for the majority of interventions. The tactical team will often require additional information based on the data that has already been collected. An agreement has now been reached with Digit that interventions can, in principle, only be extended up to a maximum of two times four weeks). An intervention is not extended, for example if a suspect is arrested or if the investigation yields too little information. The same parties that tackle the question of whether an intervention may take place within a criminal investigation at all, including the corresponding timeline, are also involved in deciding whether or not an intervention is to be extended.

Digit has attempted to gain access and/or has succeeded in gaining access to six types of computerised systems, which are phone, phone in combination with another computerised system, server, router, laptop and wireless access point. During the research, phones in particular have been the subject of investigation. In the meantime, a more or less standard method, using a commercial tool, has been developed for these types of interventions (hereinafter: 'standard interventions'). For other interventions (hereinafter: 'customised interventions'), Digit considers how best it can gain access and carry out its investigative activities on a case-by-case basis. These customised types of interventions are more labour intensive for Digit. Furthermore, a computerised system to which access is gained is usually limited to one or two devices.
After access has been gained, Digit carries out a number of investigative activities, laid down in sub A to E (see above). Standard interventions will often entail the selection of a combination of investigative activities: establishing specific characteristics (sub A), recording confidential communications or wiretapping (sub B), systematic observation (sub C), and documenting data stored in the computerised system (sub D). This combination is regarded as a logical choice, given that a phone contains a great deal of information about a suspect's activities – both past and present. In the case of customised interventions, the investigative activities to be carried out are less obvious. In the case of these interventions, the choice seems primarily to be made in favour of establishing specific characteristics (sub A) and the documenting of data (sub D), occasionally accompanied by rendering data inaccessible at a later stage (sub E).

Digit carries out investigative activities both using technical tools as well as manually. A technological tool, in short, ensures that data that is relevant in the context of a tactical investigation (such as chat messages, emails, audio files) can be retrieved from the suspect's device and stored in Digit's digital environment. Cases in which no technical tool is used are referred to as analogue/manual interventions. In line with the legal framework, any technical tools developed by Digit are approved by the Inspection Service (Keuringsdienst), which is part of the Central Unit (Landelijke Eenheid) of the Dutch national Police. The Inspection Service assesses these technical tools based on an inspection protocol. The inspection protocol is based on a number of sections set out in the Decree that aim to ensure that any technical tool is able to collect data in a reliable, honest and traceable manner. In this way, for example, it can be asserted with a greater degree of certainty that the collected data actually

originated from the computerised system of a suspect. Approval of a technical tool by the Inspection Service means that, should a trial court deal with the facts of the case, no clarification need be given as to the precise functioning of the tool, meaning that the investigate methods used can be protected. In the case of manual intervention, clarification must be provided of the working method applied.

The approval of a technical tool is a critical guarantee for the monitoring of the use of the power, which equally applies to the monitoring carried out by the Inspectorate of Justice and Security (Inspectie Justitie en Veiligheid; hereinafter referred to as the Inspectorate). Since the entry into force of the Act, the Inspectorate has been conducting monitoring of the implementation of the hacking power. The monitoring should be system monitoring which means that the Inspectorate monitors the functioning of the legal system. This form of monitoring came about due to the fact that during the legislative process there were concerns about the fact that not all cases in which the hacking power is used would be presented before a trial court. In addition, there were questions about the court's technical expertise.

Completing intervention and gains

An intervention will be terminated once an order has been executed, or otherwise, on the last day of the duration of the order at the latest. After completing an intervention, the technical tool is generally removed entirely (as comprehensively as possible), after which the collected data is transferred to the tactical team. Upon transferring any data, Digit will in principle not verify whether any data that is subject to a professional duty of confidentiality (geheimhoudersgegevens) is present: this responsibility rests with the tactical team. This type of data relates inter alia to communications between the suspect and their legal counsel. Pursuant to Section 126aa of the Dutch Code of Criminal Procedure this type of data should be destroyed. However, Digit has indicated that there currently is no unambiguous set of regulations on how to handle information subject to a professional duty of confidentiality. The destruction of such data under Section 126aa of the Dutch Code of Criminal Procedure is ostensibly contrary to Section 28 of the Decree, which, inter alia, states that the content of the data recorded on the technical infrastructure may in principle not be altered. Removal of part of the data from a file would alter and therefore affect the integrity of that file. On the basis of the Explanatory Memorandum to the Decree this must be ruled out. Up to the present Digit (Public Prosecution Service) has therefore decided that data subject to a duty of confidentiality will not be permanently deleted.
Digit (police) drafts a number of official police reports every time the hacking power is used and the organisation has in recent months been working on getting its house in order in this regard. In terms of reporting, Digit (Public Prosecution Service) has provided a framework for minimal reporting in connection with the protecting of investigative methods. Based on the information in the official report, any 'smart reader' of the report should not be able to defend him or herself against the technical tools used by Digit. Furthermore, Digit (police) must keep detailed records of its activities in its own internal systems ('maximum journalisation').

A limited number of interventions with the hacking power have been examined in greater depth for the purposes of this study, which shows that so far the power mainly yields information that guides the investigation. Contrary to some expectations, the collected data has not yet yielded the definite proof within a criminal investigation. Furthermore, according to the information available, to date a trial court has not yet heard the facts and substance of any case in which the hacking power was used. In

some cases, this will never take place, for example, due to there being no suspect in a given case or because the power (alongside other powers) has not provided sufficient incriminating evidence. As a result, no statements (as yet) can be made regarding the value of the new power as a type of evidence: does the data collected by means of the hacking power contribute to the evidence in a criminal case?

The foregoing outlines the process surrounding the implementation of the hacking power. A number of obstacles and difficulties that have arisen in investigative practice have already emerged. A number of issues will be outlined in greater detail in the following sections, given that difficulties have (likewise) arisen in those areas.

Gaining access

The aim is for the hacking power to be used covertly and remotely. In practice, it is sometimes necessary to be present on location in the vicinity of the computerised system in order to penetrate and gain access. The legislator does not appear to have taken this option into account. In order to be able to get close to a computerised system, Digit occasionally will have to make use of a (special) investigative power, which can only be used if it already happens to have been used by a tactical team within the same investigation as the use of the hacking power is intended. This dependence on the tactical team always constitutes an obstacle to Digit, given that tactical teams may not always intend to use such a power. For that reason, Digit requires a support power, comparable to the way in which this is regulated with regard to the recording of confidential communications (Section 126l Dutch Code of Criminal Procedure). In addition, Digit (Public Prosecution Service) wishes to be able to keep the use of this support power out of the case file in connection with the protection of the methods used. The question, subsequently, is to what extent this covert aspect can still be used to assess whether an intervention is proportionate or not, for example, in connection with any adverse effects of an operation to gain access. If there is no accountability whatsoever (given that the method is protected) and in fact only a limited number of people are involved in the decision-making regarding the method of gaining access, this raises the question whether that assessment of proportionality is being carried out by a sufficient number of officials.

Vulnerabilities and reporting obligation

In order to gain access to computerised systems, Digit makes use of the vulnerabilities of computerised systems. Vulnerabilities are weaknesses in hardware or software that make it possible for third parties to gain access to a computerised system. In order to do so, these vulnerabilities must be rendered ready to be exploited. There are three types of vulnerabilities: known, known-unknown vulnerabilities and unknown-unknown vulnerabilities. A known vulnerability is a vulnerability that is already known to a given manufacturer of a product (e.g. a phone). These types of vulnerabilities are published in various places on the internet and manufacturers of the relevant products regularly develop updates to address the vulnerabilities that are known to them. As long as the manufacturer does not make an update available or a customer does not install the update, the police are able to make use of the vulnerability. An unknown vulnerability (both known-unknown and unknown-unknown) is a vulnerability about which information has not yet been disseminated on the internet and therefore cannot be known a wider audience. Also there is no update available. Until the time of dissemination, however, this is known as a zero day. These types of vulnerabilities can

likewise be used to gain access to a computerised system. A known-unknown vulnerability is a vulnerability that is known to the investigative authorities, but which is not yet known to the manufacturer of the product, resulting in a lower probability that the manufacturer will fix the vulnerability. The police therefore are able to make use of the vulnerability (most likely for a longer period of time than in the case of a known vulnerability). An unknown-unknown vulnerability is a vulnerability that is likewise not known to the investigative authorities. These types of vulnerabilities may be found in products that law enforcement agencies purchase from commercial suppliers to gain access to IT-systems.
Concerns have been raised by various parties regarding the use of vulnerabilities, particularly due to the fact that the existence and use of these vulnerabilities would ostensibly make computer systems less secure. The government has expressed the expectation for the police to preferably make use of known vulnerabilities, while the use of unknown vulnerabilities is regarded as 'a last resort, but an indispensable option to tackle serious forms of crime' (*Parliamentary Papers I* 2017/18, 34 372, G, p. 7). In connection with concerns regarding security aspects, indirectly a reporting obligation has been agreed for unknown vulnerabilities (under Section 126ffa of the Dutch Code of Criminal Procedure, which states that reporting an unknown vulnerability may be postponed, after a written authorization from a examining magistrate). Reporting a vulnerability would ostensibly increase (online) security, given that this vulnerability would no longer be able to be exploited (assuming that the manufacturer has fixed the vulnerability). The reporting obligation does not apply to products purchased from a commercial supplier. A supplier of these types of products generally will not reveal any information regarding the composition of its product, meaning that the party who purchases the product is unaware of possible vulnerabilities used – as a result of which no notification can be made. So the reporting obligation only applies to known-unknown vulnerabilities.

Digit experiences the reporting obligation outlined in the above as a key obstacle. First and foremost, because the reporting obligation similarly also applies to vulnerabilities in systems that are specifically made for and by persons with criminal intentions. This means that these people must ultimately be informed that their system, which is used almost exclusively for criminal purposes, contains a vulnerability. This raises the question to what extent reporting such vulnerabilities increases the level of security. Rather, it seems that persons with criminal intentions in such cases are afforded the opportunity to improve their security. Secondly, the reporting obligation may also complicate cooperation with national as well as international parties, given that in certain countries the use of a vulnerability is considered state secrets. If the Dutch police wishes to cooperate with such countries, this would be problematic due to them being obliged to report on a state secret of a foreign country under Dutch law. The risk of such a scenario is that the relevant vulnerability would no longer be usable and cooperation would become very unappealing for those countries.

Commercial tools

Although the use of an unknown vulnerability was regarded as a 'last resort', Digit has made use of a commercial tool (and therefore most likely of unknown-unknown vulnerabilities) in the vast majority of its interventions. That tool is used for the standard interventions and the tool allows Digit (police) to both gain access and carry out investigative activities. The use of this tool is indispensable to Digit, given that it would otherwise not be able to carry out a large percentage of the interventions. A number of reasons have been cited for this. One of the reasons is that finding an

unknown vulnerability in a IT-system, which is used by almost all Dutch citizens, is very difficult; the reporting obligation is another reason. If it were even possible to locate an unknown vulnerability independently and render it ready to be used, it would have to be reported. This means that the vulnerability in question, which has taken up a lot of time to prepare for use, can only be used a very limited number of times.
It followed from the 2017-2021 Government Coalition Agreement that the use of a commercial tool must be limited in order not to encourage the market for unknown vulnerabilities. It was therefore agreed that a licence must be purchased for each individual case instead of a tool being purchased once, subsequently allowing it to be used for multiple interventions. Given that that tool in the investigative practice has been used for a large number of interventions, it is estimated that this agreement has led to more than twice the purchase price being paid to date – it is estimated that this is in the range of 'several millions' of euros. Given the relatively large number of interventions in which this tool is used, it is unlikely that the agreed licencing model has led to the market for unknown vulnerabilities being less stimulated.

Technical tools

Digit makes use of two types of technical tools: commercial tools (as discussed in the above) and dedicated technical tools developed by Digit (Police). In addition, Digit has the option of taking a non-automated route (manual intervention).
There is a debate regarding the scope of the term technical tool (and the non-automated intervention), primarily between Digit and the Inspectorate. The question of whether something does or does not constitute a technical tool is relevant given that only a technical tool need be assessed and approved and Digit regards assessment as a major obstacle in respect of implementation (please see more information about the assessment itself in the next section). Digit was only able to use its own proprietary technical tools, developed in house, in a small number of interventions. A key reason for this is that developing a technical tool and ultimately getting it assessed and approved is a time-consuming process. This lengthy turnaround time means that Digit was only able to use a small number of technical tools developed in house.
Until now, a 'new' technical tool has been used for each intervention, due to the fact that a new intervention with the hacking power will often require a number of adaptations to the technical tool. There is a desire within Digit to develop a number of standard components that have already been assessed and approved in advance. These could then be supplemented in a relatively short period of time, depending on the needs of the investigation in relation to a specific intervention. This would lead to the creation of a technical tool, including already assessed and approved components, which could be used in a specific case. This approach has so far proved difficult, given that this distinction between new and already assessed components is not made during assessments and each tool is regarded as a new tool in itself that must be assessed in full, including the associated assessment periods.
In investigative practice, non-automated intervention is currently considered more often compared to the early days. In the case of non-automated intervention, Digit must justify its working method in greater detail in order to assert with greater certainty the reliability, integrity and traceability of the data that was collected using the method in question. This does, however, mean that the method will not remain completely protected. This is not regarded as problematic by Digit in all cases.

Assessment of technical tools

Assessment of technical tools presents a major difficulty to Digit. This is related to the fact that the two parties involved (Inspection Service and Digit) regard the assessment process from two different perspectives, which in the case of practical implementation occasionally clash with one another. From the perspective of the Inspection Service the principal focus is on the rules set out by the Decree and on the assessment requirements arising therefrom. This means inter alia that, in line with the Decree, a tool can only be approved if all requirements are met – whether or not supplemented with a number of (additional) substitute safeguards. In this way the integrity, reliability and traceability of the collected data can be stated with one hundred percent certainty. This perspective occasionally clashes with the way in which Digit approaches the assessment process. This perspective focuses principally on the feasibility and the necessity of the rules of the Decree and the assessment requirements in the assessment resulting from the Decree. Digit is critical of the assessment carried out by the Inspection Service, given that it is considered poorly matched to the tools developed by Digit (police). The fact that updates are regularly implemented, for example, is inherent to software and therefore inherent to the resources used by Digit. This is different compared to more traditional technical tools such as GPS trackers, and the question therefore is to what extent the Inspection Service must and can take this into account. Particularly when a technical tool must be approved in advance – the latter resulting from the Explanatory Memorandum to the Decree.
In addition to feasibility, the necessity of the rules and requirements is also given critical consideration by Digit. Contrary to how the Inspection Service views the assessment process, Digit believes it is not necessary for a tool to meet all the assessment requirements. In Digit's opinion there should, be (greater) flexibility to take into account evidential value and risk assessments. Taking into account evidential value means that it is not necessarily a problem if a technical tool were not fully approved, as appropriate accountability would be able to be provided in court. The impact of this, however, would be that the investigative method would no longer remain fully protected. It would then be at the discretion of the court, potentially, to assess the value of the evidence collected. However, this would require that a case in which the hacking power is used is brought to court and that a court has sufficient technical expertise at its disposal to make this assessment. Most likely, a trial judge will deal with not all cases substantively. In addition, the question is whether there is sufficient availability of such expertise at this juncture. Furthermore, putting risk assessments front and centre means that the point of departure should be based far more on the issue of what the risk is if a certain requirement contained in the assessment protocol were not met, instead of the tool having to meet that requirement for approval.

Assessment and safeguards

In recent years, Digit has largely been unsuccessful in using a technical tool that received ex-ante approval, which is chiefly related to the (lengthy) development lead time involved. However, as previously stated, the Explanatory Memorandum to the Decree states that this is in principle mandatory. The development period is at odds with the urgent investigative interests that must exist in order to be able to make use of the power in the first place. It is therefore prudent to consider whether it is always realistic to require the use of an ex-ante approved tool. The Decree also keeps open the option of presenting an tool for assessment ex-post or to omit an assessment entirely – both should be an exception. In practice, this is not the case. The Public

Prosecutor for Digit has concluded that the nature of a widely used commercial tool has so far precluded assessment. This means that in the majority of cases one of the safeguards, an assessment by the Inspection Service, was not executed. Instead in those cases additional technical and tactical safeguards were implemented (please see more information in the next section). In practice, however, it has become apparent that this tool most likely cannot be approved either, given that the tool that Digit has purchased uses a server to which the supplier has access. Although it is true that the data collected, such as the suspect's chat messages, are ultimately stored on the Digit server, this does not alter the fact that the supplier (in theory) has access to the suspect's data during the period access is gained by the investigative authorities and the execution of the investigative activities. Although contractual agreements are in place to ensure that the supplier is prohibited from reviewing the data in question and may only have access to the server for tool maintenance purposes, it cannot be excluded that the supplier could also give itself access to the server at other times. For that reason alone, the tool cannot be approved. Digit argues that a supplier would never access the server to review the data on its own initiative, due to agreements that were made between Digit and a supplier. Violating these agreements would damage a supplier's reputation as well as the financial risks this would entail would be too high. Nevertheless, this does mean that the reliability and integrity of the collected data could be compromised.
If a tool were used, for which Digit (Public Prosecution Service) decides that its nature precludes assessment, then safeguards must be in place to ensure the integrity, reliability and traceability of the data obtained. The Explanatory Memorandum to the Decree shows that these can be technical safeguards. These additional safeguards must be justified in the case file by the Public Prosecution Service. In investigative practice, not only are additional technical safeguards put in place but additional tactical safeguards are likewise provided. The latter type of safeguards relates to measures taken by the tactical team to verify the collected data. The Decree does not take into account that such measures can be taken and similarly are already taken in practice. This raises the question of whether it is not possible for these types of safeguards to be taken into account – before a trial court can do so – when assessing the reliability, traceability and integrity of the collected data.

Monitoring by the Inspectorate

As stated previously, the Inspectorate monitors the implementation of the hacking power. There are a number of barriers in practical implementation, which has led to monitoring by the Inspectorate taking place accompanied by a fair share of debate in practice. Following the Reports (Verslagen) issued by the Inspectorate, Digit (police) has begun to improve a number of elements within its approach. Nevertheless, Digit has decided to disregard a number of aspects identified by the Inspectorate, such as the registration process in relation to the issuing of technical tools. This is related to the fact that Digit does not consider these aspects to be properly feasible within the framework of the Decree. The Inspectorate, however, focusses on the way in which Digit should act in accordance with the legal framework, given that it is up to the legislator to assess the feasibility of that legal framework (and whether any amendment is necessary). Failure to take into account feasibility means that the requirements of the Decree that Digit has decided it will not (or cannot) meet will be aspects that the Inspectorate will continue to flag up and which Digit in turn will disregard. A stalemate of this nature raises the question of whether the intended effects of monitoring can be achieved in the current situation. And subsequently raises

questions regarding what the consequences may be if the Inspectorate identifies specific issues, which Digit then decides not to pursue.

The second obstacle relates to the scope of monitoring. The Inspectorate carries out oversight on the activities of the police rather than on those of the Public Prosecution Service. Within the current study it has become clear that, in practice, the actions of the Public Prosecutor and of those of the police are inextricably linked and that the two are therefore difficult to separate. Digit (Public Prosecution Service) takes the position that virtually all activities carried out by Digit take place under the authority of the Public Prosecution Service and that the Inspectorate therefore does not have a remit to comment on those activities. The Inspectorate believes that it is indeed entitled to supervise those activities, given that they are carried out by Digit (Police) and Digit (Police) occasionally advises Digit (Public Prosecution Service) on those actions. Moreover, the limited implementation of the supervisory remit, under the interpretation of Digit (Public Prosecution Service), would ostensibly lead to the Inspectorate being virtually unable to make statements about any aspects whatsoever. It is therefore necessary to provide clarity who should exercise monitoring over whom and which aspects should be subject to monitoring by the Inspectorate. This dialogue has started.
A third obstacle relates to the issue of what is needed to be able to perform effective system monitoring. The legislative history does not provide much information about how that system monitoring ought to take place, except that the Inspectorate is entitled to review individual cases. It is precisely the question of *how* that causes problems in practical implementation. The Inspectorate wishes to be able to base its monitoring on Digit's internal quality control systems, which is in line with the way in which system monitoring is defined by the Inspection Council. At the time this report was drafted, a quality control system was not in place. Furthermore, there appears to be a lack of clarity about what a quality control system entails exactly. In the near future, it would therefore be prudent to review what should be organised in practice in order to get the system monitoring off the ground.

Interventions with an international component

A Public Prosecution Service Guideline (OM-aanwijzing; Guideline on the international aspects of the use of the power pursuant to Section 126nba of the Dutch Code of Criminal Procedure) regulates what action must be taken in the event data are located on foreign territory. During the period of the study, Digit was involved in a limited number of interventions with an international component, which related to interventions abroad carried out from the Netherlands and interventions in the Netherlands carried out from abroad.
As far as the standard interventions are concerned, in principle the agreement is that a phone from a Dutch suspect located on foreign territory may not be accessed. In the case of customised interventions, whether or not the power is used will depend on the relationship with the relevant country.
The Public Prosecution Service Guideline focuses on interventions with the power abroad, however is not always sufficient. This, for example, applies in cases where a wide range of different computerised systems are involved, such as in the case of a botnet. The Minister of Justice and Security is notified in cases where there is derogation from the Public Prosecution Service Guideline. Interventions involving an international component can be especially complicated politically.

Interventions in the Netherlands from abroad are currently not regulated, including in the Public Prosecution Service Guideline. This presents complications for practical implementation, given that in those cases, complex legal constructions must be devised within which various requests for mutual legal assistance are submitted back and forth. Another more practical issue is that no judicial oversight procedure has been agreed for foreign interventions, whereas such a procedure is in place for other special investigative powers. A judicial oversight procedure of this nature means that, if a foreign country wishes to make use of a special investigative power in the Netherlands and has been granted permission, the Examining Magistrate must grant permission for the actual transfer of data collected using the special investigative power. This is to verify the lawful application of the power.

Separation of duties

The legislative history shows that a strict separation of duties and functions must be in place, which should inter alia prevent Digit (police) from being influenced by tactical teams when assessing the feasibility of an intervention and its execution. In practice, regular consultation takes place between the technical and tactical team as well as an exchange of information, both before the hacking power is used and during the intervention. This study shows that Digit is dependent on the information provided by the tactical team to ensure effective execution. Interventions by Digit are less easy to carry out without that consultation. That is why the separation of duties and functions is a problematic concept in light of the hacking power.

In conclusion

This first evaluation study has focused primarily on the process surrounding the practical implementation of the hacking power. In contrast to the more technical side of an intervention, less attention has been devoted to what the use of this new power means in practice to the tactical teams requesting its implementation and what added value the intervention can have in a criminal investigation. This subject is aimed to be fleshed out in greater detail in the second part of the evaluation. Part 2 of the evaluation also aims to devote more attention to cases that have been heard substantively in a trial court and in which data has been considered substantively. If available, the judgments from the courts may clarify the questions and dilemmas that have emerged on the basis of this initial study. In addition, the second part of the evaluation will look in more detail at the other components of the CCIII Act.
However, on the basis of this initial evaluation, a number of problems have already been identified that clearly complicate the use of the power and which could already be addressed: 1) the way in which access can be gained, 2) the use of commercial tools, 3) the reporting obligation, 4) monitoring by the Inspectorate and 5) the assessment of technical tools.
Let us turn first and foremost to the aspect of gaining access to computerised systems. Access must be gained both covertly by stealth and remotely. However, in practice, it has been shown that when the hacking power is used the police cannot always remain completely at a distance. A support power could be beneficial in these types of situations where operating completely remotely is not possible.
Secondly, the use of commercial tools. Whenever Digit makes use of a commercial tool, a separate licence must be purchased for each individual intervention. Given that a tool is used on multiple occasion, this agreement leads to high costs being incurred.

Investigative practice has indicated that this tool is indispensable to operations. If this tool continues to be used in the same way, it would be prudent to review the agreement on the purchase of individual licences. In addition, attention must be paid how to guarantee the integrity, reliability and traceability of the collected data, for example by means of technical and tactical safeguards. This is important, because under the current inspection regime, this tool will not be approved by the Inspection Service (Keuringsdienst).
Thirdly, the reporting obligation. Indirectly a reporting obligation for unknown vulnerabilities was created from the point of view of security. This reporting obligation applies to all unknown vulnerabilities, including systems that have been developed for and by persons with criminal intentions. Moreover, the reporting obligation can make cooperation with both domestic and international parties more difficult. This therefore raises the question as to whether the reporting obligation as it currently applies can actually improve and advance security in all cases.
Fourthly, the monitoring by the Inspectorate. At the moment it is not possible for the Inspectorate to carry out the system monitoring desired by the legislator, due to the lack of a quality system at Digit. For that reason, it would be good to look at what should be organized in practice in order to get system monitoring off the ground. In addition, it is necessary to gain more clarity about the way in which the monitoring by the Inspectorate can come into its own, while also paying attention to the practical feasibility of the hacking power.
Finally, the assessment of technical tools. The inspection procedure presents a major difficulty to Digit (police). Moreover, it appears to be difficult to put an ex-ante approved tool into use. It would therefore be prudent to *jointly* review, with all relevant actors, the best ways to assess how the integrity, reliability and integrity can be guaranteed, also when using commercial tools. That is after all an interest shared by *each of the* actors involved.

Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) is het kennisinstituut voor het ministerie van Justitie en Veiligheid. Het WODC doet zelf onafhankelijk wetenschappelijk onderzoek of laat dit doen door erkende instituten en universiteiten, ter ondersteuning van beleid en uitvoering.

Meer informatie:

www.wodc.nl