Summary

Investigating, prosecuting and obstructing cybercrime

The Netherlands has a fast, stable and reliable digital infrastructure that is heavily used, both domestically and internationally. This gateway position offers economic opportunities, but also creates obligations. Illegal activities take place on Dutch servers or are knowingly or unknowingly facilitated by web hosting companies based in the Netherlands.
To investigate cybercrime, the Dutch police have set up the specialised National High Tech Crime Unit (NHTCU) (*Team High Tech Crime*, *THTC*) at the national level, as well as specialised cybercrime teams at the regional level. The cybercrime teams work together with the NHTCU in a national structure and support the regional crime squads and local teams in building knowledge to assist with standard criminal investigations into cybercrime.
As investigating and prosecuting perpetrators of cybercrime can be difficult for several reasons, the police and the Public Prosecution Service sometimes opt for alternative interventions outside of the criminal investigation process when tackling cybercrime. Examples of such alternative interventions are disrupting criminal activities by taking servers offline, as well as focusing on prevention through public awareness campaigns, such as the recent Dutch campaign warning against WhatsApp fraud. In addition, public-private partnerships are sought on an ongoing basis and various projects have been launched to help counter various cybercrime offences.

The aim of this study was to gain more insight into the approach by the police and the Public Prosecution Service to complex types of cybercrime. In addition, this study has examined to what extent criminal investigations have helped to improve the information position in relation to suspects (who are often anonymous in the online domain) and their modus operandi, and how this information could be used not only to track down and prosecute suspects, but also to put a stop to illegal online activities.

Research methods

We used various research methods to answer the research questions. By reviewing the relevant literature and conducting desk research, we gathered background knowledge to gain an overview of the approach used to tackle cybercrime.
In addition, we analysed police files of criminal investigations into high-tech cybercrime. For this purpose, we examined eight files of completed police investigations from the period 2014-2018. Seven of those files were made available by the NHTCU, and one was made available by a cybercrime team at the regional level. We also studied three public-private partnership projects.
At the start of the study, a meeting was organised with a number of experts from the police and the Public Prosecution Service. We asked them to compile a list of high-tech criminal investigations. As this study was aimed at gaining more insight into the possibilities and dilemmas the police and the Public Prosecution Service encounter in their approach to cybercrime, we also asked them about criminal

investigations affected by bottlenecks identified in previous research on organised cybercrime. By examining the police files, we determined which methods were used during the criminal investigations, how the investigations proceeded and what results they produced.
Lastly, we conducted forty-two interviews with police officers, public prosecutors specialised in cybercrime and employees of private parties to gain a more complete picture of the approach to cybercrime. Our interviews with public prosecutors and police team leaders who handled the selected cases enabled us not only to ask overarching questions, but also to gain more insight into information and considerations that may not have ended up in a file but did play a role in the choices they made during the investigation. The interviews also provided an insight into the dilemmas and problems the police encounter.

The bulk of the data was collected by the NHTCU, as this team mainly investigates the type of cases that fall within the scope of our study.

Results: criminal investigations into cybercrime

In contrast to the regional cybercrime teams, almost none of the investigations of the NHTCU were started in response to a police report. Although in theory it is possible for the NHTCU to launch an investigation on the basis of a police report, in practice high-tech crime is rarely reported to the police. This state of affairs was also reflected in the files we examined for this study. The only investigation that started in response to a criminal police report was a case at a regional unit. Of the seven NHTCU investigations we examined, six were started following a tip-off from a private party and/or an alert from a foreign police force.
As the number of cases exceeds the investigation capability of law enforcement, choices have to be made about which cases are taken up by the investigation services. Whether a case is taken up depends both on the policy priorities that have been set and on the seriousness of a case.
Although the primary aim of a criminal investigation is to track down and prosecute suspects, an investigation can also be started from a more strategic point of view; for instance, to gain more knowledge about a cybercrime phenomenon or a particular criminal modus operandi, to be better able to investigate and stop this form of cybercrime. Sometimes investigations do not even target cybercrime in the narrowest sense of the word but types of crime related to it, such as a case involving encrypted communication. One reason for taking up that case was the fact that encrypted phones were widely used in organised crime, which was impeding non-cybercrime investigations. However, the technology behind the phones was so complex that the investigation ended up at the NHTCU. Although it was mentioned several times in the interviews that were conducted for the present study, that it is sometimes difficult to explain why the NHTCU also takes up these kinds of cases, it is also widely recognised that these are precisely the kinds of cases that need to be taken up, as they have such a big impact on tackling organised crime.

Goals

Officially, criminal investigations into cybercrime are only to be started if evidence is available that can be used to track down and prosecute possible suspects, as that is a precondition for the use of investigative powers. However, many cybercriminal investigations do not lead to the identification of a suspect. Sometimes this becomes evident soon after the start of an investigation, and the police then consider whether other goals can be achieved with the gathered information, such as gaining insight into a particular criminal phenomenon, so as to use that knowledge in subsequent criminal investigations or deploy countermeasures.

In practice, the police apply a flexible approach to the investigation goals formulated at the start of an investigation, also because it is not known at the outset what information the investigation will yield and, therefore, which goals it will serve. Goals can sometimes be changed as the police gather additional information during the investigation. For example, when it emerges that no suspect can be identified or that a suspect cannot be prosecuted, the emphasis will shift to the use of countermeasures to stop this form of cybercrime. Conversely, over the course of an investigation it can emerge that more can be done than was thought at the outset.

Investigative tools and methods

The investigative activities in the files we examined, especially in the initial phase of an investigation, mainly consisted of demanding access to and securing server data. A detailed investigation of server data provides insight into the type of data stored on a server and how a server is used. Sometimes this was done by physically securing a server and other times by making a forensic copy or snapshot. Subsequently, digital evidence was examined in more detail. In addition, these criminal investigations made extensive use of internet wiretaps and looked into network traffic. Based on the information thus obtained, the police were able to plan the further direction of the investigations. These data were also examined to ascertain whether the suspect’s identity might be revealed somewhere. It should be noted that the use of these tools did not yield the same amount of information in every investigation.

Furthermore, the files we examined also showed that when no suspect could be identified, generally only digital investigation methods were used. When Dutch suspects were identified, the investigation often shifted to a more tactical approach that also involved using more traditional (offline) investigation tools and methods. Thus, in addition to internet wiretaps, telephone taps were used to learn about contacts between suspects and with others, as well as matters that concerned them. This was often combined with financial investigations to map money flows in order to establish criminal activities like money laundering.

In all five files we examined in which Dutch suspects were identified, undercover investigative powers were used. These powers were used both online and offline. This is striking, as these special investigative powers are normally rarely used in non-cybercrime cases. This may reflect the seriousness of the cases we examined, but it may also imply that in tackling these new cybercrime offences, new ideas are emerging about the use and the severity of existing investigative powers.

Possibilities for prosecution

Suspects were identified in five of the eight files we examined. In four cases, the prime suspects were Dutch nationals. Two of these cases resulted in convictions: a ransomware case and a phishing case. In the ransomware case, community service orders and a suspended prison sentence were imposed, and in the phishing case, prison sentences of five years were imposed. This is also the heaviest punishment imposed so far for this particular offence. In the third case, which concerned DDoS attacks, an alternative settlement was imposed due to the young age of the accused and the police conducted ‘knock and talk’ interviews to warn off the buyers of the illegal service. The case relating to encrypted communication has yet to come to court. In the dark web case with two foreign main suspects, the largest Dutch providers of the illegal products were prosecuted. The police conducted ‘knock and talk’ interviews with some of the other providers and buyers of the products.

Although the NHTCU investigations in particular do not always lead to the identification of suspects who can be prosecuted, launching a criminal investigation does have added value for these types of offences, where prosecuting suspects is difficult. Autonomous, independently operating criminal groups can easily replace a criminal infrastructure. Interventions that focus only on disrupting the infrastructure have a short-lived effect, as new infrastructure will be created and activities will be continued elsewhere. It is therefore important to continue to conduct criminal investigations aimed at identifying and prosecuting suspects. Furthermore, in a number of cases the NHCTU investigations into facilitators, while not yielding a main suspect, did yield information on other forms of crime that could subsequently be used in other criminal investigations or to deploy countermeasures.

Countermeasures

Our study shows that criminal investigations and countermeasures to obstruct criminal processes go hand in hand, as that is the most effective way to tackle cybercrime. In the context, we also refer to the approach used to tackle the infiltration of the public sphere by organised crime, which specifically targets the criminal business model. The interplay between criminal investigations and countermeasures is important because knowledge gained from criminal investigations can be used to gain and update knowledge about these criminal processes. If interventions are limited to countermeasures, only a small part of the criminal process is made visible. By contrast, when suspects are arrested or criminal assets are seized, the entire process can be reconstructed and the key players can be identified. Criminal investigations not only build up knowledge but also have a disruptive effect because they deter potential offenders.

From a legal perspective, the implementation of countermeasures in the context of criminal investigations sometimes gives rise to debates. The police have a broader task than the Public Prosecution Service. This raises the question of what mandate the Public Prosecution Service has with regard to countermeasures. Countermeasures sometimes also require the use of special investigative powers that require authorisation by a public prosecutor or examining judge. This can be problematic when it becomes evident soon after the start of an investigation into a cybercrime offence with a major social impact that no suspect can be identified. In that event, deploying an alternative form of intervention would be desirable. However, there is currently no legal basis for the use of investigative powers for the purpose of disrupting criminal activities. The interviews we conducted show that this does not yet lead to problems in practice, but attempts to resolve this issue do sometimes approach a grey area.

Dilemmas in tackling cybercrime

Over the course of this study, it became clear that the wishes of investigative officers are sometimes at odds with the policy and legal frameworks, leading to areas of tension in the approach to cybercrime.

Information position

The tension in the approach to cybercrime relates first and foremost to the information position in the criminal investigation process. For the police to be able to investigate crimes efficiently and make informed choices in the criminal investigation process, it is important to build up a good information position. To build up an information position on the activities of (international) criminal groups, facilitators and other perpetrators, the police would like to monitor those activities on a continuous basis together with other parties, not necessarily in the context of specific investigations. To achieve this, the NHTCU aims for a data-driven way of working. This includes, for example, examining whether links can be established between data from different criminal investigations in terms of similarities in their modus operandi or the malware used. However, the Public Prosecution Service and the police are not allowed to use investigative powers for the sole purpose of improving their information position. In addition, data from different investigations may not be automatically linked. When information is secured, this is done in the context of a specific criminal investigation. However, within the framework of the Police Data Act (*Wet politiegegevens*, Wpg) information may also be used in other investigations, provided this has been authorised. This basic principle that the police may not use investigative powers to improve its information position sometimes creates difficulties. The police want to gain a good overview of what is going on, as it enables them to respond effectively and efficiently.

Getting to the bottom of cybercrime phenomena requires investigations spanning years. Investigations into cybercrime phenomena consume a lot of time and capacity and often (primarily) yield results in terms of stopping and disrupting cybercrime, but less frequently lead to the identification and prosecution of perpetrators. Such less easily measurable alternative interventions are sometimes difficult to reconcile with the policy-based quantitative targets. While the choice between meeting quantitative targets or increasing the knowledge position is not always so black and white, in practice it often presents a dilemma.

Sharing information

The second major finding of our study concerns problems around sharing information. These problems relate first and foremost to the notification of victims. At present, responsibility for this is not clearly assigned to a specific party. With certain offences, such as hacking, the number of victims is often so large that notifying the victims is not a task that can simply be added to the workload of the investigative officers. In addition, the process of notifying victims is complex. Often, abstract data sets such as IP addresses are the starting point. Furthermore, sharing this information can present legal complications. What seems logical and obvious to do in practice is not always legally permitted. This creates a lack of clarity and inefficiency.

In one of the criminal investigations we examined, this meant that several Dutch parties were notified later than desirable and by means of a difficult indirect process. As a result, these Dutch parties were exposed to potential danger for an unnecessarily long time.

In addition, the difficulties also relate to public-private partnerships. Public-private partnerships are an essential component of the integrated approach to cybercrime. Partnerships with private parties enable incorporating other expertise in the approach to cybercrime and enable both the police and the private party to gather additional information.

However, there are also practical objections to such partnerships. Public and private parties have different, and possibly conflicting, interests. The parties should remain aware of this throughout the term of their partnership. Furthermore, the laws and regulations concerning the sharing of information can make such types of cooperation difficult. This includes not only the Police Data Act (Wpg), but also the General Data Protection Regulation (which has replaced the Persona Data Protection Act (*Wet bescherming persoonsgegevens*, Wbp)), the Network and Information Systems Security Act (*Wet beveiliging netwerk- en informatiesystemen*, Wbni) and, where applicable, duties of confidentiality. While it is advisable to exercise a degree of restraint in sharing information, a lack of clarity among parties about the legislation can lead to excessive reluctance to share information.

International cooperation

In tackling cybercrime, the police in many cases depend on international cooperation. Even smaller cases often have an international component. International cooperation is therefore an important part of the criminal investigation process. The NHTCU cooperates frequently and well with various European criminal investigation services, such as services in the UK and Germany, as well as the FBI in the United States. This cooperation includes sharing investigative information, the coordinated search and arrest of suspects and the coordinated deployment of crime disruption activities.

Although good international cooperation can bring success, the officers interviewed in our study stated that the long processing time of international legal assistance requests is one of the biggest bottlenecks. The length of time that teams have to wait for the results of such a request varies greatly. While the interviewed investigative officers are positive about Europol's role, they also noted that success is very dependent on the capacity and priorities in cooperating countries. Each country has limited capacity for handling legal assistance requests. That also applies to the Netherlands. The reality is that by the time a response is received, sometimes the requested information has long since vanished. What has improved in international cooperation compared to a few years ago is that the services in various countries have more knowledge, and contacts with many countries are also improving.

In conclusion

This study has highlighted a number of points that raise the question of how the frameworks that apply in tackling traditional crime relate to the approach used to tackle (complex) cybercrime. Therefore, it could be beneficial to conduct a critical review as to whether the current laws and regulations are adequate to facilitate the collection, processing and analysis of information for the purposes of tackling cybercrime. In addition, the parties involved need to draw up clear frameworks within which information can be shared. This will ensure that when information is urgently needed and parties are willing to share it, they are able to share such important information