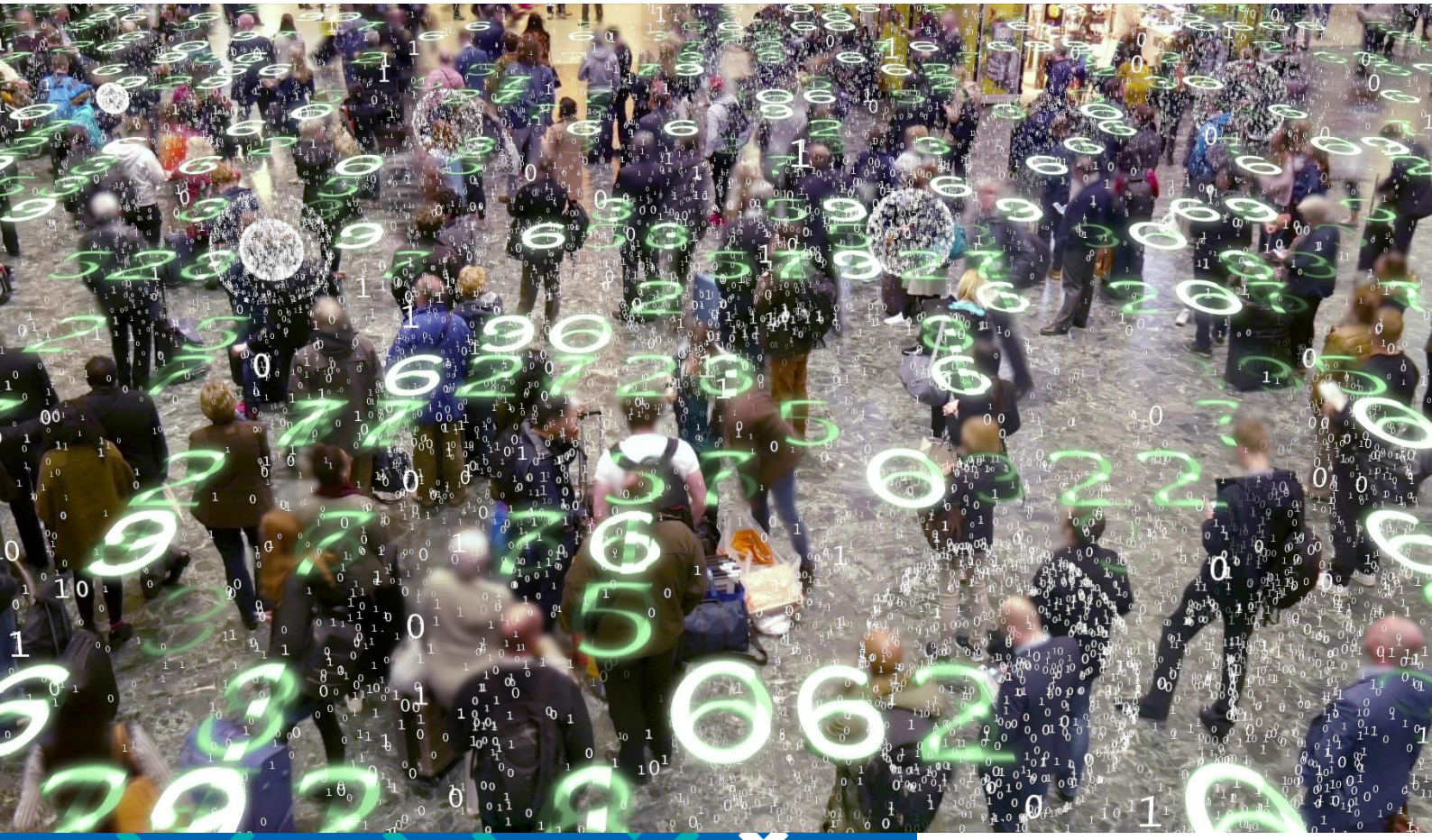
De rol van encryptie in de opsporing

Belemmeringen en mogelijkheden

Auteurs: Jurjen Jansen[1,2], Saskia Westers[1], Wendy Schreurs[2], Maike Berkenpas[1], Greg Alpár[3] & Wouter Stol[1,2,3]

[1]NHL Stenden Hogeschool, [2]Politieacademie, [3]Open Universiteit



NHL STENDEN hogeschool

Open Universiteit

POLITIE Politieacademie

De rol van encryptie in de opsporing
Belemmeringen en mogelijkheden

Datum	Februari 2023
Versie	1.0
Uitgever	Cybersafety Research Group
	NHL Stenden Hogeschool
	www.cybersciencecenter.nl
Vraagarticulatie	Minister van Justitie en Veiligheid
Opdrachtgever / subsidieverstrekker	Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)
Publicatietitel	De rol van encryptie in de opsporing: Belemmeringen en mogelijkheden
Publicatiejaar	2023
Publicatietype	Onderzoeksrapport
Auteurs	Dr. Jurjen Jansen Saskia Westers MSc Dr. Wendy Schreurs Maike Berkenpas BSc Dr. Greg Alpár Prof dr. Wouter Stol
Met medewerking van	Kimberly Bluhm
Met dank aan de begeleidingscommissie	Prof. mr. B. Niemeijer (VU Amsterdam, voorzitter) Dr. ir. J. Henseler (Hogeschool Leiden) Dr. R.S. van Wegberg (TU Delft) B.A. Boonen MSc (Ministerie van JenV) Dr. I.W.J. van der Vegt (WODC, lid tot juli 2022) Dr. L.M. van der Knaap (WODC, lid vanaf juli 2022)

Summary

Encryption is increasingly common in all forms of crime. There are broadly two reasons for this. First, encryption is commonly integrated in software and hardware and is therefore easily accessible to criminals. Second, the ability to hide relevant information and communications greatly facilitates criminal activity. Consequently, law enforcement increasingly encounters encryption in criminal investigations. This raises the question of what role encryption plays in these investigations, which is the focus of the current study.

Encryption poses a dilemma to policy makers and legislator. This dilemma can be seen, for example, in a resolution on encryption adopted by the European Council on 14 December 2020. On the one hand, encryption is considered crucial to protect the fundamental rights and digital safety and security of citizens, governments, businesses and society. On the other hand, encryption hampers law enforcement and judicial authorities in the exercise of their legal powers to protect society and citizens.

The Dutch Minister of Justice and Security supports this resolution and has requested the Dutch Research and Documentation Centre (WODC) to study the impact of encryption in criminal investigations. This study aims to provide insights to support the consideration of the dilemma of encryption. The researchers have chosen to discuss 'the role' of encryption, instead of talking about 'the impact' of encryption. The choice of the term role, which seems more neutral, was taken to prevent the impression that the current study is biased or prejudiced. The main research question that this study aims to answer is: What is the role of encryption in police investigations? This question is elaborated in three sub-questions: (i) What is the nature of encryption that is encountered in criminal investigations?; (ii) Does encryption affect the conduct of criminal investigations, and if so, how?; (iii) Does encryption affect the outcome of criminal investigations, and if so, how?

This is an exploratory study, as there is limited information available on this topic. To answer the main question and sub-questions, desk and field research have been carried out. Desk research consisted of a literature review, media analysis and an analysis of court decisions. In addition, sixteen exploratory interviews were held with nineteen professionals of the Dutch police, the Netherlands Public Prosecution Service and the Netherlands Forensic Institute. Based on their knowledge and experience, they were able to give an expert judgement on the subject. An online questionnaire was also administered to Dutch police employees, which was fully completed by 177 operational specialists (response rate 20%). Lastly, in-depth interviews were conducted with three Netherlands Public Prosecution Service staff and five staff members from the judiciary.

Sub-question 1: What is the nature of encryption in criminal investigations? First, the role of encryption in criminal investigations was examined. This study suggests that encryption is common in all type of crimes, but the extent to which it is common differs according to crime. The most significant factor affecting the significance of encryption to investigation may be the prevalence of seized mobile phones in criminal investigations, as mobile phones are usually protected by some form of encryption. Other significant forms of encryption include encrypted chat services, locked devices other than mobile phones (e.g., laptops), encrypted e-mail services and crypto phones. It is difficult to determine the extent to which encryption affects criminal investigations. However, interviewees perceive that encryption has become increasingly central to criminal investigations in the last few years, even though this cannot be substantiated by statistics. They acknowledge that the prevalence of this depends heavily on the type of crime.

When focusing on different categories of crime, encryption is most common in subversive crimes, and to a fairly large extent, in high-impact crimes. It is less prevalent in common crimes. When focusing on specific types of crime, encryption mostly plays a role in drugs offences, child pornography and cybercrime – both cyber-dependent and cyber-enabled crime. Furthermore, interviewees suggest that encryption plays a significant role in all types of organised crimes.

Some interviewees distinguish two types of encryption: technology-driven encryption, in which messages are automatically end-to-end encrypted (e.g., WhatsApp); and human-driven encryption which is used to deliberately encrypt information (e.g., crypto phones). Interviewees describe human-driven encryption as an indicator of crime. However, this impressionistic perception does not mean that this is always the case. After all, it is not prohibited by law to use crypto phones. Moreover, some individuals use encryption for their own safety, for instance journalists or individuals who want to protect trade secrets.

Sub-question 2: Does encryption play a role in the progress of criminal investigations, and if so, how? Encryption plays a role in the conduct of criminal investigations. One of the key factors is prioritisation. Cases get prioritized when it is in the interest of Dutch society. Another important factor to continue the investigation when encountering encryption is the perceived likelihood to gaining access to the encrypted data. However, how likely it objectively is to succeed and get access to encrypted data cannot be quantified.

To gain access to encrypted information, law enforcement agencies have roughly two options: bypassing encryption and cracking encryption. Both options may require a lot of capacity, but this is not always the case. Bypassing can take place by finding the encryption key, guessing the key, enforcing the key, exploiting a leak in the encryption software, gaining access to readable text when using the device, and by locating a copy of the readable text. Cracking encryption – or gaining access to a computer system using forensic tools – requires specialised software and hardware. Participants in the study mentioned that cracking is often outsourced to another party or department, such as the Netherlands Forensic Institute. In case of international cooperation, Europol may play a role. The success of cracking encryption depends on the cryptographic algorithm used and the key length. A general rule is that the longer the key is, the more difficult it is to crack it. Firmly quantifying the time required is not included in the scope of the current study.

When focusing on the use of investigative powers, the Netherlands Public Prosecution Service determines whether capacity and time of the police or the Netherlands Forensic Institute will be used to crack encrypted data. The investigation department has the decryption order (art. 126nh paragraph 1 of the code of criminal procedure) and hacking powers (art. 126nba, 126uba and 126zpa of the code of criminal procedure). However, little use is made of these powers since they may only be used under strict conditions. Furthermore, regarding mutual legal assistance, law enforcement agencies depend on, among other things, laws and regulations, whether requested data are delivered (on time) and whether they are useful for the investigation.

Encryption can also affect the duration of investigations. One outcome may be that due to encryption an investigation can be terminated, which happens when there is not enough evidence or when the encrypted data (presumably) cannot be decrypted. Nonetheless, even without cracking or circumventing encryption, a case is not immediately lost. Evidence can be gathered in other ways, which may still lead to a successful conviction.

Thus, encryption may create obstacles in criminal investigations. On the other hand, once encryption is circumvented or cracked, an investigation might accelerate. One respondent stated that after decryption, a case that traditionally would take months to a year can now be completed in a few weeks. It was also noted that encryption does not always have an obstructive influence, as suspects sometimes voluntary unlock their device. Finally, the learning capacity of Dutch police organisation and affiliated parties, such as the Netherlands Public Prosecution Service, the Netherlands Forensic Institute and the judiciary is constantly evolving. The increasing knowledge and experience of cracking and bypassing encryption, as well as the deploying alternative investigation strategies to complete the evidence, may reduce the processing time of cases in which encryption is present.

Sub question 3: Does encryption play a role in the outcome of criminal investigations, and if so, how? The role of encryption in the outcome of criminal investigations includes such issues as the extent to which encryption affects the identification and/or localisation of relevant persons and the successful discovery of evidence. In general, encryption hampers the identification and/or localisation of relevant persons and assets of collaborations or (criminally relevant) relations between persons, assets and locations, and the possibility of establishing (detecting) criminal activities. The main barrier is the reduction of direct access to evidence. Also, unencrypted and retrieved data differ in their investigative utility. Lastly, retrieved data regularly arrive late, not at all or are not usable.

Although it is not clear what kind of data – and thus evidence – is missing, respondents mention that not being able to circumvent or crack encryption does not always lead to termination of an investigation. In cases where it is not successful, alternatives can be used to still gather the evidence needed in a case. Think for example about the significance and use of metadata in investigations. Although encryption may have made it more difficult and challenging, law enforcement agencies still often succeed. For example, interviewees and respondents indicate that there is a relatively high success rate in retrieving information from devices and applications with technology-driven encryption (by default). Human-driven encryption (consciously applied), on the other hand, seems to be more difficult to circumvent or crack. However, we cannot substantiate this with statistics.

In addition, decrypted data is highly valued. It is generally seen as more reliable than (witness) statements. According to interviewees, this information is less likely to have been altered by third parties. The open communication of suspects – who feel safe behind encryption – is valuable. Interviewees also indicate that decryption is beneficial to create an idea of criminal collaborations, as this is more complete than the global and fragmentary ideas of the situation before and/or without encryption. Moreover, when access is gained to encrypted data (the decryption phase), there is potentially a wealth of information, which could be beneficial for the investigation.

Main question: What is the role of encryption in criminal investigations? This study shows that encryption plays a prominent role in criminal investigations. This role works both ways. On the one hand, encryption plays an obstructing role for criminal investigations, but on the other hand it also plays a practical role in improving the investigations.

Overall, it can be concluded that it is, however, not easy to quantify the challenge. It cannot be determined how many cases are not solved or how much time is lost because of encryption. By the same token, it is also not possible to determine how many additional cases are solved or how much time is gained. Criminal investigation is too complex by the entirety of facts, coincidences, circumstances and trade-offs for that. This study provides a nuanced image of what the use of

encryption – consciously or unconsciously – means for criminal investigations. There are negative sides to the use of encryption, but positive aspects can also be identified.

When encryption is being examined, the process of encryption is not the only thing that needs to be considered. A holistic view is needed to get to the core of the 'problem' of encryption. This has been done by deliberately including decryption in the study as well. The nuanced effect of encryption on criminal investigations was also reflected in the responses we received through the various methods that we applied. Interviewees accepted that new phenomena have to be dealt with and acted upon in novel ways. The so-called 'cat-and-mouse' game that occurs between police and criminals is thus seen as an opportunity for the police organisation to develop further.

It is therefore important to (continue to) invest in developing knowledge and skills regarding detection and digital aspects of police work, such as encryption. It is also important to keep track of future (technological) developments and what they mean for the role of criminal investigations. These include quantum computing, which was mentioned by participants in this study, as well as developments that are already underway, such as 5G and in the field of AI (artificial intelligence).

To conclude. This study is about the role of encryption in criminal investigations. What we would like to convey here is the practical and often contradictory effects of encryption on criminal investigations, and the follow-up question of whether it should then be treated differently from the way it currently is.

After all, the police have always been dealing with crucial crime information stored in a memory to which they do not have direct access. We call that memory the human brain. Since the police cannot read that (they do not have a key) and the criminal may choose to remain silent, police have to think of all kinds of ways to bypass that security and/or get the key and/or trick someone into revealing the information. Now we have a computer that, like the criminal, says: you will not get in and I will not say anything. Then, as police, you must think of alternatives to deal with that. The police have always done that. So, what is really different now?

The tendency may be to compare the current situation – where encryption is thus a daily occurrence – with the situation where digital information was not yet encrypted. The question behind this is what standard is being followed. We can argue that compared to five, ten or fifteen years ago, the current conditions are more difficult for the police. We can also argue that by contrast, armed with decryption power, the police have gained extra access to information that is potentially much greater than before. Ultimately, digitalisation requires moving with and adapting to what comes our way. Therein lies the constant challenge.