Summary

The investigation of cybercrime requires law enforcement officials to use novel investigative methods to gather evidence. However, the legal basis for using digital investigative methods in Dutch criminal procedural law is often unclear. This study aims to answer the question of how the Dutch legislature can adequately regulate digital investigative methods. To achieve that aim, the following three steps are taken: (1) the investigative methods that are commonly used in cybercrime investigations are identified, (2) the extent to which Dutch criminal procedural law can adequately accommodate these investigative methods is analysed, and (3) the extent is examined to which these digital investigations methods can be applied unilaterally, i.e., without permission from a State or a treaty basis, across State borders.

Chapter 1 introduces the study's topic and provides a characterisation of the study. It also presents the problem statement, restrictions to the scope of the research, and research methodology. The problem statement (PS) is as follows.

PS: *To what extent does Dutch criminal procedural law adequately regulate the investigative methods used in (cross-border unilateral) cybercrime investigations?*

The 'adequate regulation of investigative methods' is understood as legislation that provides law enforcement authorities with the instruments to gather evidence in cybercrime investigations and citizens with a minimum level of protection against an arbitrary application of governmental power. To determine the minimum requirements for the regulation of investigative methods, the right to privacy in art. 8 ECHR is examined in relation to the regulation of digital investigative methods.

This problem statement leads to the following five research questions.

RQ 1: *Which investigative methods are commonly used in cybercrime investigations?*

RQ 2: *Which normative requirements can be derived from art. 8 ECHR for the regulation of investigative methods?*

RQ 3: *Which quality of the law is desirable for the identified digital investigative methods?*

RQ 4: *How can the legal framework in Dutch criminal procedural law be improved to adequately regulate the identified investigative methods?*

RQ 5: *To what extent is it desirable and legitimate that the identified investigative methods are applied unilaterally across State borders?*

Chapter 2 answers RQ 1. The investigative methods are identified by examining which evidence-gathering activities take place in cybercrime investigations. These evidence-gathering activities are based on the digital leads of IP addresses and online handles. The investigative methods can also be applied unilaterally across State borders. However, these evidence-gathering activities are seldom straightforward, due to the three challenges of (1) anonymity, (2) encryption, and (3) the territorial limitation of enforcement jurisdiction in cybercrime investigations. By this principle, evidence-gathering activities by law enforcement authorities are restricted to the border of the investigating State, unless the activity is authorised by the other State involved or by a treaty basis. The study examines which investigative methods can be used to overcome the three challenges. The analysis shows that the following four digital investigative methods are commonly used in cybercrime investigations:

(1) gathering publicly available online information;
(2) issuing data production orders to online service providers;
(3) applying online undercover investigative methods; and
(4) performing hacking as an investigative method.

Chapter 3 answers RQ 2 by examining the relation between the right to privacy in art. 8 ECHR and the regulation of investigative methods. The examination shows that an important condition, namely that the privacy interference is '*in accordance with the law*', is particularly important for adequately regulating the investigative methods. The condition requires that the regulations for the investigative methods (1) are accessible, (2) are foreseeable, and (3) meet a certain quality of the law. In this study, these are considered to be the normative requirements for the regulation of investigative methods. The first normative requirement, accessibility, means that the law gives an adequate indication concerning the regulations for the use of investigative methods in a given case. The second normative requirement, foreseeability, implies that the legal framework for investigative methods prescribes with sufficient clarity the scope of the power conferred on the competent authorities and the manner in which the investigative method should be exercised. The third normative requirement, the quality of the law, means that regulations concerning investigative methods must be of sufficient quality. The ECtHR can specify the level of detail of the regulations and the minimum procedural safeguards for regulations concerning investigative methods that interfere with the right to privacy. The ECtHR requires more detailed law and procedural safeguards for regulating investigative methods, depending on the gravity of the privacy interference that takes place. This

mechanism is referred to as the 'scale of gravity for privacy interferences'. In this study, it has been important in determining the desired requirements for the regulation of the identified digital investigative methods. The scale of gravity also provides a tool for visualising the privacy interferences and for locating them within the Dutch legal framework. It contributes to the detection of misalignments between the quality of the law of current Dutch regulations and the desired quality of the law as it implied by art. 8 ECHR.

Chapter 4 answers RQ 3 by determining which specific requirements are desirable for the identified digital investigative methods. The chapter examines how the investigative methods interfere with the right to privacy and which quality of the law is desirable. The analysis shows that the application of investigative methods in a digital context often seriously interferes with an individuals' right to privacy. The reason is that it involves the analysis and storage of large amounts of personal data.

Chapters 5, 6, 7, and 8 answer RQ 4 with respect to each of the identified investigative methods. The three normative requirements are used to examine whether the Dutch legal framework is adequate for the investigative methods. The analysis shows that the Dutch legal framework is generally accessible. This can be attributed to the strong legality principle in Dutch law. The Dutch legality principle in criminal procedural law requires a legal basis for all privacy-interfering investigative methods. However, the *foreseeability* and the *quality of the law* of the Dutch legal framework for digital investigative methods often leave much to be desired.

It is important that the scope of the digital investigative methods and the manner in which they are applied are clear to the individuals involved, in order to avoid arbitrary interferences of law enforcement authorities in their private lives. Currently, a lack of foreseeability exists due to (1) the lack of indications about the scope of the investigative methods in statutory laws, (2) the often outdated examples in explanatory memoranda to legislation, and (3) the lack of case law regarding the application of the digital investigative methods. This shows an important and large task is ahead for the Dutch legislature and Public Prosecution Service. These entities should provide more clarity about the legal basis for digital investigative methods, their scope, as well as the manner in which they are applied.

In addition, the Dutch legal framework should meet the desired quality of the law. The desired quality of the law is in this study based on art. 8 ECHR. The analysis shows that the regulations that apply to the investigative methods were originally written for an application in an offline context. However, the application of investigative methods in an online context brings with different privacy interferences. The Dutch legal framework should take these changes into consideration. As a result of a more serious privacy interference, stronger procedural safeguards are suggested for regulations concerning the issuing of data production orders to online service providers, applying online undercover investigative methods, and perform-

ing hacking as an investigative method. The gathering of publicly available online information does not require detailed regulations with procedural safeguards in criminal procedural law. However, detailed regulations are suggested for the investigative method outside criminal procedural law.

Chapter 9 answers RQ 5. Mutual legal assistance treaties that facilitate the evidence-gathering activities of law enforcement authorities on foreign territory are written for a territorially partitioned legal world. The problem is that the Internet does not take these territorial borders into account and practically allows law enforcement officials to unilaterally gather evidence that is located on foreign territory. Despite the prohibition to gather evidence in this manner, the chapter aims to determine to what extent these cross-border unilateral digital evidence-gathering activities are acceptable. To achieve that aim, the negative consequences of this practice are further analysed. The analysis shows that the practices can (1) infringe on the territorial sovereignty of other States and (2) endanger the legal certainty of the individuals involved. The seriousness of the negative consequences are different for each investigative method. Therefore, in certain cases, the cross-border unilateral application of investigative methods could be acceptable to a certain extent. States should also recognise that digital evidence-gathering activities currently take place and should be prepared to regulate these activities insofar necessary. The study suggests which limitations for cross-border unilateral digital evidence-gathering activities are desirable and where additional regulations are necessary.

Chapter 10 evaluates the outcomes of the analyses regarding the domestic and international legal frameworks for digital investigative methods. The evaluation shows that updating the Dutch domestic legal framework to accommodate digital evidence-gathering activities is necessary, but in itself not sufficient. The international legal framework should also accommodate digital investigative methods. At present, States do not sufficiently recognise the urgency of amending the international legal framework and facilitating cross-border evidence-gathering activities by law enforcement officials in cybercrime investigations.

Chapter 11 answers the PS. The legal framework regulating digital investigative methods is in many respects outdated. The Dutch legislature is faced with the important task of updating criminal procedural law and adequately accommodating the identified digital investigative methods within the domestic legal framework. In the study, concrete suggestions are provided to improve the regulation of digital investigative methods based on the normative requirements derived from art. 8 ECHR. Due to the cross-border nature of both cybercrime and digital evidence-gathering activities, the international legal framework also requires an overhaul. States should first recognise that cross-border unilateral digital evidence-gathering activities are taking place. Amendments to mutual legal assistance treaties are

also needed to restrict and facilitate these cross-border evidence-gathering activities and protect both State sovereignty and the legal certainty of the individuals involved. Suggestions as to what these desirable restrictions may entail are provided for the Dutch legislature. The chapter is concluded with recommendations for the regulation of digital investigative methods on both the domestic level and the international level.