

Cover Page



Universiteit Leiden



The handle <https://openaccess.leidenuniv.nl/handle/1887/44879> holds various files of this Leiden University dissertation

**Author:** Oerlemans, Jan-Jaap

**Title:** Investigating cybercrime

**Issue Date:** 2017-01-10

## Investigating Cybercrime



# Investigating Cybercrime

PROEFSCHRIFT

ter verkrijging van  
de graad van Doctor aan de Universiteit Leiden,  
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker  
volgens besluit van het College voor Promoties  
te verdedigen op dinsdag 10 januari 2017  
klokke 13.45 uur

*door*

**Jan-Jaap Oerlemans**

geboren te Barendrecht

in 1985

Promotor: prof. dr. H.J. van den Herik  
Copromotoren: mr. dr. F.P. Ölçer  
mr. dr. B.W. Schermer

Promotiecommissie: prof. dr. J.H. Crijns  
prof. dr. P.A.L. Ducheine (Universiteit van Amsterdam)  
prof. dr. G.P. van Duijvenvoorde  
prof. dr. S. van der Hof  
prof. dr. E.J. Koops (Tilburg University)  
prof. dr. H.G. van der Wilt (Universiteit van Amsterdam)



SIKS dissertation series no. 2017-01. The research reported in this thesis has been carried out under the auspices of SIKS, the Dutch Research School for Information and Knowledge Systems.

Lay-out: AlphaZet prepress, Waddinxveen  
Printwerk: Amsterdam University Press

ISBN 978-90-8555-109-6

© 2017 J.J. Oerlemans

*Behoudens de in of krachtens de Auteurswet van 1912 gestelde uitzonderingen mag niets uit deze uitgave worden veeelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.*

*Het reproprecht wordt niet uitgeoefend.*

*No part of this publication may be reproduced, stored in a retrieval system, made available or communicated to the public, in any form or by any means, without the prior permission in writing of the publisher, unless this is expressly permitted by law.*

## Preface

*Investigating Cybercrime* reflects my research journey into the topic of criminal investigations that involve cybercrimes. At the start of my PhD research in 2010, I had the ambition to examine the phenomenon of ‘high-tech crime’. I soon found out that criminal substantive law, i.e., the law that deals with criminalising certain behaviours, with regard to cybercrime was already up-to-date in the sense that Dutch law complies with international obligations in that regard. The real challenge with cybercrime lies in criminal procedural law and mutual legal assistance matters, so that became the focus of my research.

Criminal procedural law regulates, amongst other things, privacy-infringing investigative methods. Over time, I learned that much ambiguity exists concerning the regulations for using investigative methods in a digital context. The ambiguity on the applicable regulations hinders evidence-gathering activities and thereby also impedes the combatting cybercrime. Such ambiguity with respect to digital investigative methods is detrimental to the rule of law, since a key element of the rule of law is legal certainty. Individuals involved in criminal investigations should know the *scope* of the investigative powers and the *manner* in which they are applied by law enforcement authorities. Regulations for digital investigative methods are, however, often either non-existent or ambiguous. In part, this can be explained by the quick advancements in information and communication technology (ICT) that have not been taken in consideration in legislation.

In a broader perspective, it is also problematic to apply principles from mutual legal assistance to ‘the digital jungle’ of the Internet. In that ‘jungle’, law enforcement authorities of many different States use digital investigative methods across State borders, without physically leaving their own territory. The cross-border unilateral application of digital investigative methods can violate the territorial sovereignty of other States and can affect the rights and freedoms of individuals that live abroad. The cross-border unilateral application of digital investigative methods fundamentally affects the current fabric of international cooperation in criminal matters.

In this PhD thesis, I hope to provide more insight into the workings of cybercrime investigations and to contribute to the creation of a legitimate legal framework that regulates digital investigative methods. The manuscript was closed on 24 October 2016. Any changes in the law that have since occurred could not be included. Let us now start with addressing the fascinating questions that cybercrime and digital investigations provide. I wish you pleasant reading.

Jan-Jaap Oerlemans  
October 2016, Leiden



# Table of Contents

PREFACE	V
LIST OF ABBREVIATIONS	XIII
1 UPDATING THE LEGAL FRAMEWORK	1
1.1 Characterisation of the study	3
1.2 Problem statement and research questions	8
1.3 Restrictions of the research	11
1.3.1 Restriction to cybercrime investigations	11
1.3.2 Restriction to evidence-gathering activities by law enforcement officials	12
1.3.3 Restriction to art. 8 ECHR	13
1.4 Research methodology	14
1.4.1 Desk research	14
1.4.2 Comparative legal research	15
1.4.3 Fieldwork	16
1.4.4 Analysis	17
1.5 Structure of the thesis	17
2 DIGITAL INVESTIGATIVE METHODS	19
2.1 Cybercrime as the object of a criminal investigation	20
2.1.1 Target cybercrimes	21
2.1.2 Tool cybercrimes	24
2.2 Digital leads	27
2.2.1 Tracing back an IP address to a computer user	28
2.2.2 Online handles	30
2.3 The challenge of anonymity	37
2.3.1 Different internet access points	37
2.3.2 Anonymising services	38
2.3.3 Overcoming the challenges of anonymity	42
2.4 The challenges of encryption	44
2.4.1 Encryption in transit	45
2.4.2 Encryption in storage	49
2.4.3 Overcoming the challenges of encryption	52
2.5 The challenge of jurisdiction	56
2.5.1 Enforcement jurisdiction	56
2.5.2 Mutual legal assistance	59
2.5.3 Limits of mutual legal assistance	63
2.5.4 Overcoming the challenge of jurisdiction	64
2.6 Chapter conclusion	66



3	NORMATIVE REQUIREMENTS FOR INVESTIGATIVE METHODS	69
3.1	The scope of protection under art. 8 ECHR	70
3.2	Conditions to legitimise privacy interferences	73
3.2.1	A legitimate aim is available	74
3.2.2	In accordance with the law	74
3.2.3	Necessary in a democratic society	76
3.2.4	The scale of gravity for privacy interferences	77
3.3	Dynamic interpretation of the ECHR	80
3.3.1	Two examples of the dynamic interpretation of convention rights	81
3.3.2	Relevance for digital investigative methods	82
3.4	Chapter conclusion	83
4	THE RIGHT TO PRIVACY AND DIGITAL INVESTIGATIVE METHODS	85
4.1	Gathering publicly available online information	86
4.1.1	The right to privacy regarding similar investigative methods	86
4.1.2	The right to privacy and gathering publicly available online information	95
4.1.3	Desired quality of the law	100
4.2	Issuing data production orders to online service providers	102
4.2.1	Privacy and data production orders issued to telecom providers	103
4.2.2	Privacy and data production orders issued to online service providers	104
4.2.3	Desired quality of the law	113
4.3	Applying online undercover investigative methods	115
4.3.1	The right to privacy and undercover investigative methods	115
4.3.2	The right to privacy and online undercover investigative methods	118
4.3.3	Desired quality of the law	121
4.4	Performing hacking as an investigative method	124
4.4.1	The right to privacy and computer searches	124
4.4.2	The right to privacy and the use of covert listening devices	126
4.4.3	The right to privacy and hacking as an investigative method	127
4.4.4	Desired quality of the law	133
4.5	Chapter conclusion	135
5	GATHERING PUBLICLY AVAILABLE ONLINE INFORMATION	137
5.1	Accessibility	141
5.1.1	Manual gathering of publicly available online information	142
5.1.2	Automated gathering of publicly available online information	145

5.1.3	Observation of online behaviours of individuals	146
5.1.4	Section conclusion	148
5.2	Foreseeability	149
5.2.1	Manual gathering of publicly available online information	150
5.2.2	Automated gathering of publicly available online information	151
5.2.3	Observation of online behaviours of individuals	152
5.2.4	Section conclusion	155
5.3	Quality of the law	156
5.3.1	Manual gathering of publicly available online information	160
5.3.2	Automated gathering of publicly available online information	161
5.3.3	Observation of online behaviours of individuals	163
5.3.4	Section conclusion	164
5.4	Improving the legal framework	165
5.4.1	Manual gathering of publicly available online information	166
5.4.2	Automated gathering of publicly available online information	167
5.4.3	Observation of online behaviours of individuals	167
5.5	Chapter conclusion	168
5.5.1	Summary of conclusions	169
5.5.2	Recommendations	170
6	ISSUING DATA PRODUCTION ORDERS TO ONLINE SERVICE PROVIDERS	171
6.1	Accessibility	174
6.1.1	Subscriber data	175
6.1.2	Traffic data	178
6.1.3	Other data	181
6.1.4	Content data	183
6.1.5	Section conclusion	186
6.2	Foreseeability	186
6.2.1	Subscriber data	187
6.2.2	Traffic data	188
6.2.3	Other data	193
6.2.4	Content data	195
6.2.5	Section conclusion	197
6.3	Quality of the law	199
6.3.1	Subscriber data	200
6.3.2	Traffic data	201
6.3.3	Other data	203
6.3.4	Content data	203
6.3.5	Section conclusion	204

6.4	Improving the legal framework	204
6.4.1	General improvement to the legal framework	205
6.4.2	Subscriber data	205
6.4.3	Traffic data	206
6.4.4	Other data	207
6.4.5	Content data	207
6.5	Chapter conclusion	208
6.5.1	Summary of conclusions	209
6.5.2	Recommendations	209
7	<b>APPLYING UNDERCOVER INVESTIGATIVE METHODS ONLINE</b>	211
7.1	Accessibility	214
7.1.1	Online pseudo-purchases	214
7.1.2	Online undercover interactions with individuals	216
7.1.3	Online infiltration operations	218
7.1.4	Section conclusion	220
7.2	Foreseeability	221
7.2.1	Online pseudo-purchases	221
7.2.2	Online undercover interactions with individuals	224
7.2.3	Online infiltration operations	229
7.2.4	Section conclusion	235
7.3	Quality of the law	236
7.3.1	Online pseudo-purchases	238
7.3.2	Online undercover interactions with individuals	239
7.3.3	Online infiltration operations	241
7.3.4	Section conclusion	242
7.4	Improving the legal framework	243
7.4.1	Online pseudo-purchases	244
7.4.2	Online undercover interactions with individuals	245
7.4.3	Online infiltration operations	246
7.5	Chapter conclusion	246
7.5.1	Summary of conclusions	246
7.5.2	Recommendations	247
8	<b>PERFORMING HACKING AS AN INVESTIGATIVE METHOD</b>	249
8.1	Accessibility	252
8.1.1	Network searches	252
8.1.2	Remote searches	255
8.1.3	The use of policeware	261
8.1.4	Section conclusion	264
8.2	Foreseeability	264
8.2.1	Network searches	265
8.2.2	Remote searches	268
8.2.3	The use of policeware	271
8.2.4	Section conclusion	274

8.3	Quality of the law	275
8.3.1	Network searches	277
8.3.2	Remote searches	278
8.3.3	The use of policeware	278
8.3.4	Section conclusion	279
8.4	Improving the legal framework	280
8.4.1	Network searches	281
8.4.2	Remote searches	283
8.4.3	The use of policeware	285
8.5	Chapter conclusion	287
8.5.1	Summary of conclusions	287
8.5.2	Recommendations	289
9	CROSS-BORDER UNILATERAL INVESTIGATIONS	293
9.1	Consequences of cross-border unilateral investigations	294
9.1.1	Interferences with the territorial sovereignty of States	295
9.1.2	Dangers to legal certainty	297
9.1.3	Section conclusion	298
9.2	The gathering of publicly available online information	299
9.2.1	Interferences with territorial sovereignty	299
9.2.2	Dangers to legal certainty	301
9.2.3	Section conclusion	308
9.3	Data production orders	309
9.3.1	Interferences with territorial sovereignty	309
9.3.2	Dangers to legal certainty	316
9.3.3	Section conclusion	323
9.4	Online undercover investigations	324
9.4.1	Interferences with territorial sovereignty	324
9.4.2	Dangers to legal certainty	331
9.4.3	Section conclusion	337
9.5	Hacking as an investigative method	338
9.5.1	Interferences with territorial sovereignty	338
9.5.2	Dangers to legal certainty	344
9.5.3	Section conclusion	351
9.6	Restrictions for the identified investigative methods	352
9.6.1	Gathering publicly available online information	352
9.6.2	Data production orders	353
9.6.3	Online undercover investigative methods	354
9.6.4	Hacking as an investigative method	355
9.7	Chapter conclusion	356
10	THE WAY FORWARD	361
10.1	Challenges in investigating cybercrime	361
10.2	Updating the domestic legal framework	364
10.3	International legal framework	367
10.4	Chapter conclusion	369

---

11	CONCLUSION	371
11.1	Digital investigative methods	371
11.2	The right to privacy and digital investigative methods	372
11.3	Regulating digital investigative methods	374
11.4	Cross-border unilateral application of digital investigative methods	379
11.5	Answering the problem statement	380
11.6	Recommendations	382
11.6.1	Recommendations at the domestic level	382
11.6.2	Recommendations at the international level	383
11.7	Concluding remarks	383
	REFERENCES	385
	APPENDIX A	405
	SUMMARY	407
	SAMENVATTING (SUMMARY IN DUTCH)	413
	ACKNOWLEDGEMENTS	419
	CURRICULUM VITAE	421
	SIKS DISSERTATION SERIES (2009-2016)	423

## List of abbreviations

CFR	– Charter of Fundamental Rights of the European Union
CJEU	– Court of Justice of the European Union
DCCP	– Dutch Code of Criminal Procedure
DDoS	– Distributed Denial of Service
DEA	– Drug Enforcement Agency
DoJ	– Department of Justice
ECHR	– European Convention on Human Rights
ECPA	– Electronic Communications Privacy Act
ECtHR	– European Court of Human Rights
ENISA	– European Union Agency for Network and Information Security
EU	– European Union
FBI	– Federal Bureau of Investigation
GPS	– Global Positioning System
HR	– Hoge Raad (Eng: Supreme Court)
I2P	– Invisible Internet Project
ICE	– Immigration and Customs Enforcement
ICT	– Information and Communications Technology
IP	– Internet Protocol
IRC	– Internet Relay Chat
IRT	– Interregionaal Recherche Team (Eng: Interregional Detective Team)
ITU	– International Telecommunications Union
NIST	– National Institute of Standards and Technology
OSINT	– Open Source Intelligence
Par.	– Paragraph
PGP	– Pretty Good Privacy
PS	– Problem Statement
Rb.	– Rechtbank (Eng: Court)
RQ	– Research Question
SaaS	– Software as a Service
SCA	– Stored Communications Act
Stb.	– Staatsblad (Eng: Statute book)
Stcrt.	– Staatscourant (Eng: State Gazette)
TFEU	– Treaty on the Functioning of the European Union
Tor	– The Onion Router
Trb.	– Tractatenblad (Eng: Treaty Series)
UNODC	– United Nations Office on Drugs and Crime
U.S.	– United States
U.S.C.	– United States Code
U.S. CFR	– United States Code of Federal Regulations
VPN	– Virtual Private Network

