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

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

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