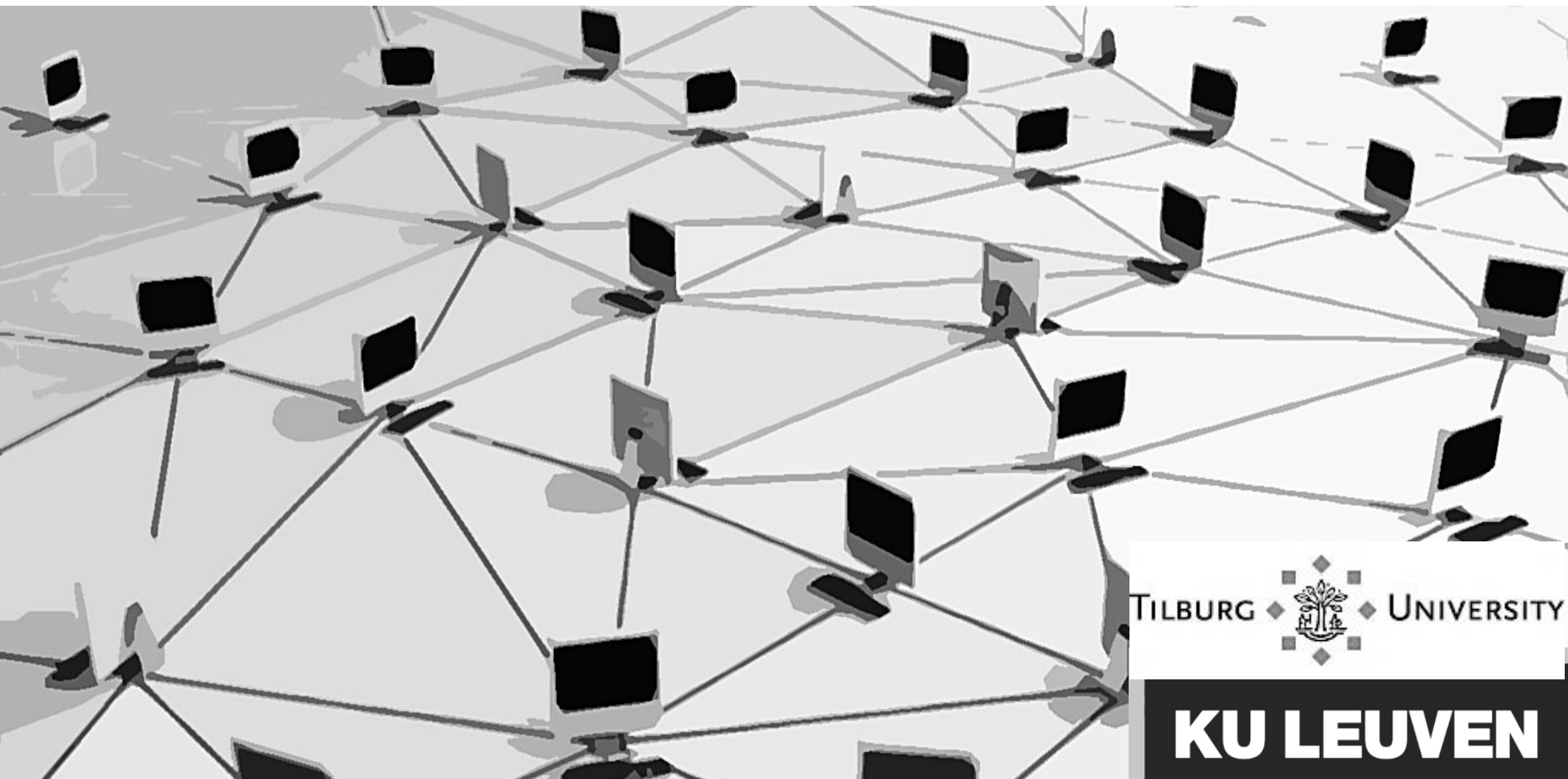


How to dismantle a botnet

the legal behind the scenes



Questions left unanswered

how, why, what



Apples & Oranges comparison



GameOver Zeus (2014, US)

Case 1



Key Agent

Intelligence gathering



US Law Enforcement

3 smart moves



Smart move 1

jurisdictional powers



KU LEUVEN

Smart move 1

jurisdictional powers

Subject matter (18 U.S.C. §1345 and 2521)
Personal jurisdiction (long arm statute)

Smart move 2

innovation

WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering

**EVGENIY MIKHAILOVICH
BOGACHEV**



Multimedia: Images

Aliases:

Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

Smart move 2

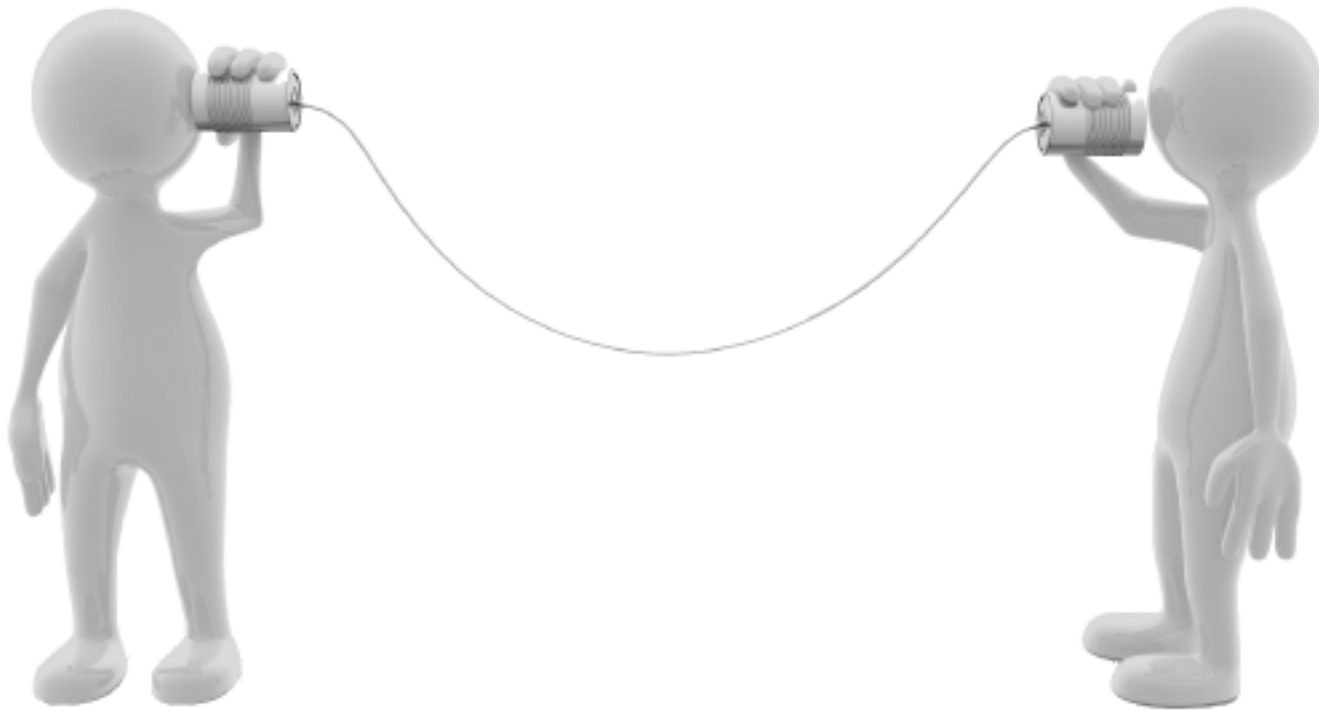
innovation

Notification of defendants (via email: Coreflood precedent)

Broad restraining order & preliminary injunction
(possible offence? highly intrusive, likelihood of damage)

Smart move 3

mutual assistance



Smart move 3

mutual assistance

Mutual Legal Assistance Treaties (MLAT) (with the UK and Luxembourg)

Coordinated international seizure of servers (Canada, France, Germany, Luxembourg, the Netherlands, Ukraine and the UK)

Bredolab (2010, NL)

Case 2



Legal issues was it okay?

[Nederlands](#) | [English](#)

POLITIE
Korps landelijke politiediensten
Dutch National Police Agency


[Home](#) • [Report Crime](#) • [Press Release](#) • [About Dutch Police](#)

Your computer is infected!

If this Browser has opened automatically then your computer has been infected with malware. Your computer has become part of a bot network.

This message has been sent to you by the High Tech Crime Team of the Dutch National Crime Squad and aims to notify all owners of infected computers.

Dutch National Crime Squad takes down infamous botnet
On October 25th 2010, the High Tech Crime Team of the Dutch National Crime Squad took down a very large botnet, containing at least 30 million infected computer systems worldwide since July 2009. These computers were infected with the malicious Bredolab trojan, through infected websites. Through these botnets, cybercriminals can spread large amounts of other viruses and create new botnets.
In close cooperation with a Dutch hosting provider, The Dutch Forensic Institute (NFI), the internet security company Fox-IT and GOVCERT, the computer emergency response team of the Dutch government, shut down 143 computer servers today.



More information:
For more information about removing Bredolab from your computer, visit:
<https://www.waarschuwingsdienst.nl/Risicos/Virusen-en-malware/Ontmanteling-Bredolab.html>

FOX-IT EXPERTS IN IT SECURITY | **GOV<E>CERT.NL** | **OPENBAAR** | **MINISTERIE VAN JUSTITIE EN VEILIGHEID** | **POLITIE**
Korps landelijke politiediensten
Dutch National Police Agency

Legal issues

was it okay?

Back-hack as an offence

Possible illegitimate use of art. 125j

Serious threat to privacy

Questions left unanswered

how, why, what



Lessons learned

the way ahead

law enforcement x intelligence

Common law x civil law

Innovation x due process of law

security x privacy

Thank you

k.k.esilva@uvt.nl

karine.esilva@law.kuleuven.be