

VIGILLO

consult

# Running botnets

..and getting away with it

ISD 2013

Cologne/Brühl

# Introduction

- Hein Dries- Ziekenheiner
  - Dutch Law (Masters, ICT and Telecom)
  - eLaw Leiden University
  - Dutch ISP association (RIP)
  - Post And Telecommunications Authority (OPTA now ACM)
  - Consultancy

# Today's subjects

- Dollar revenue (adware program)
- European law (a lot)
- Dutch law (a little)

# Dividing that 1/3

- Underground economy
- Case in point: Dollarrevenue



# Dividing that 2/3

- Dollarrevenue
  - Case



# Dividing that 3/3

- Analysis
  - What can be enforced under telecoms law?
  - Or the reverse: how can you get away with just about anything?



**VIGILLO**

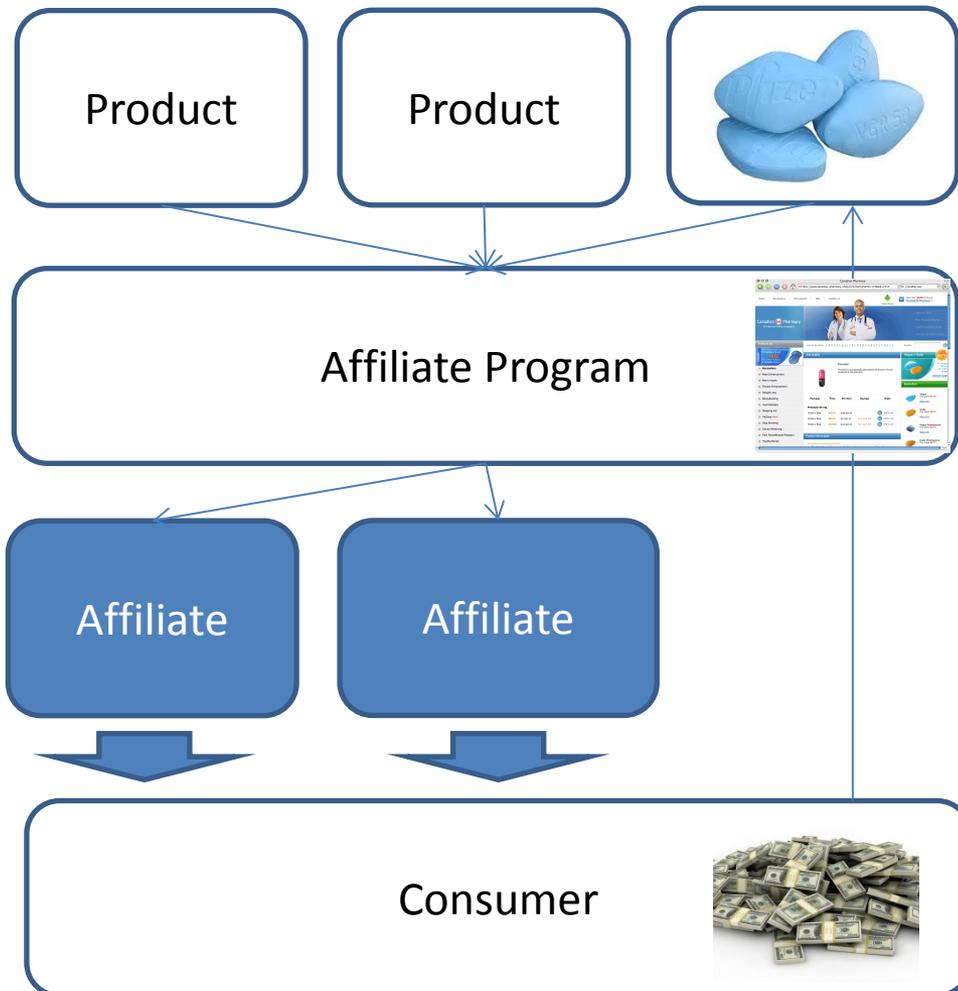
consult

Underground economy

# Division of labour

- Increasingly used
- Separation between
  - Product
  - Marketing (Affiliates)
  - Payment processing
  - Technical infrastructure
  - Botnet infrastructure

# Affiliate marketing



- Affiliates mislead spam or infect consumers
- Transaction: Pay-out
- Affiliates: “create traffic”
- Programs: “sells traffic”

**VIGILLO**  
consult

# Affiliate marketing

Canadian Pharmacy  
#1 Internet Online Drugstore

Special Offer  
Free Viagra samples  
4 pills for every order  
12 pills for order >\$300

Products list

Search by name: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Search:

Anti-Acidity

**Prevacid**  
Prevacid (Lansoprazole) decreases the amount of acid produced in the stomach.

Package	Price	Per item	Savings	Order
<b>Prevacid 30 mg</b>				
30 pills x 30mg	\$49.69	\$1.66 per pill		<a href="#">Add to cart</a>
60 pills x 30mg	\$84.29	\$1.4 per pill	Your save: \$15	<a href="#">Add to cart</a>
90 pills x 30mg	\$103.98	\$1.16 per pill	Your save: \$45	<a href="#">Add to cart</a>

Product Information

Viagra + Cialis **103<sup>08</sup>\$**  
10 x Viagra 100 mg  
10 x Cialis 20 mg  
[ORDER NOW](#)

**Bestsellers**

- Viagra Our price: **\$1.43** [More info](#)
- Cialis Our price: **\$2.37** [More info](#)
- Viagra Professional Our price: **\$3.73** [More info](#)
- Cialis Professional Our price: **\$4.17**

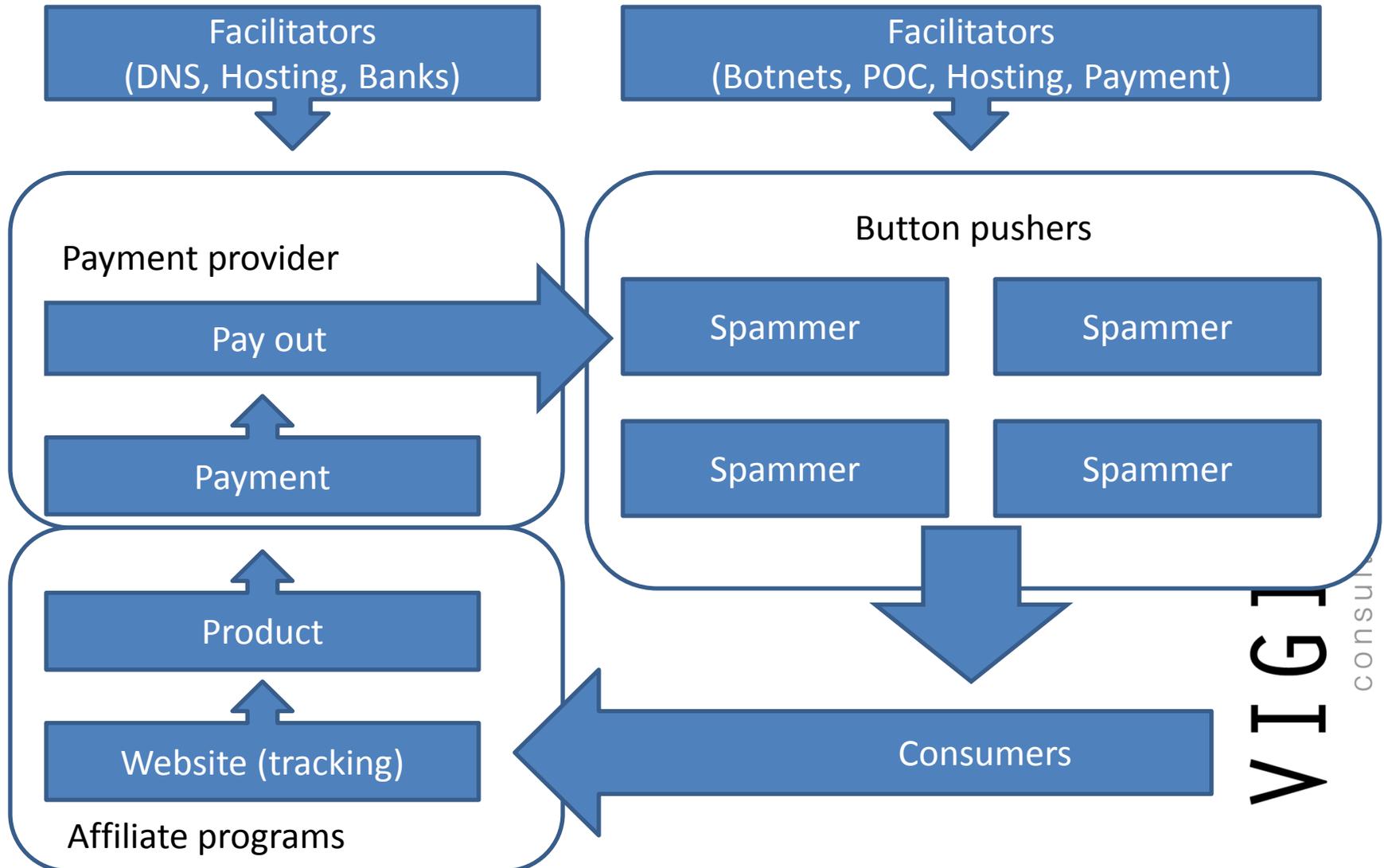
For Order more than \$300: 12 VIAGRA PILLS **FREE**  
For other Orders: 4 VIAGRA PILLS

**Bestsellers**

- Male Enhancement
- Men's Health
- Female Enhancement
- Weight Loss
- Body-Building
- Hypnotherapy
- Sleeping Aid
- Patches **New!**
- Stop Smoking
- Dental Whitening
- Pain Relief/Muscle Relaxant
- Healthy Bones

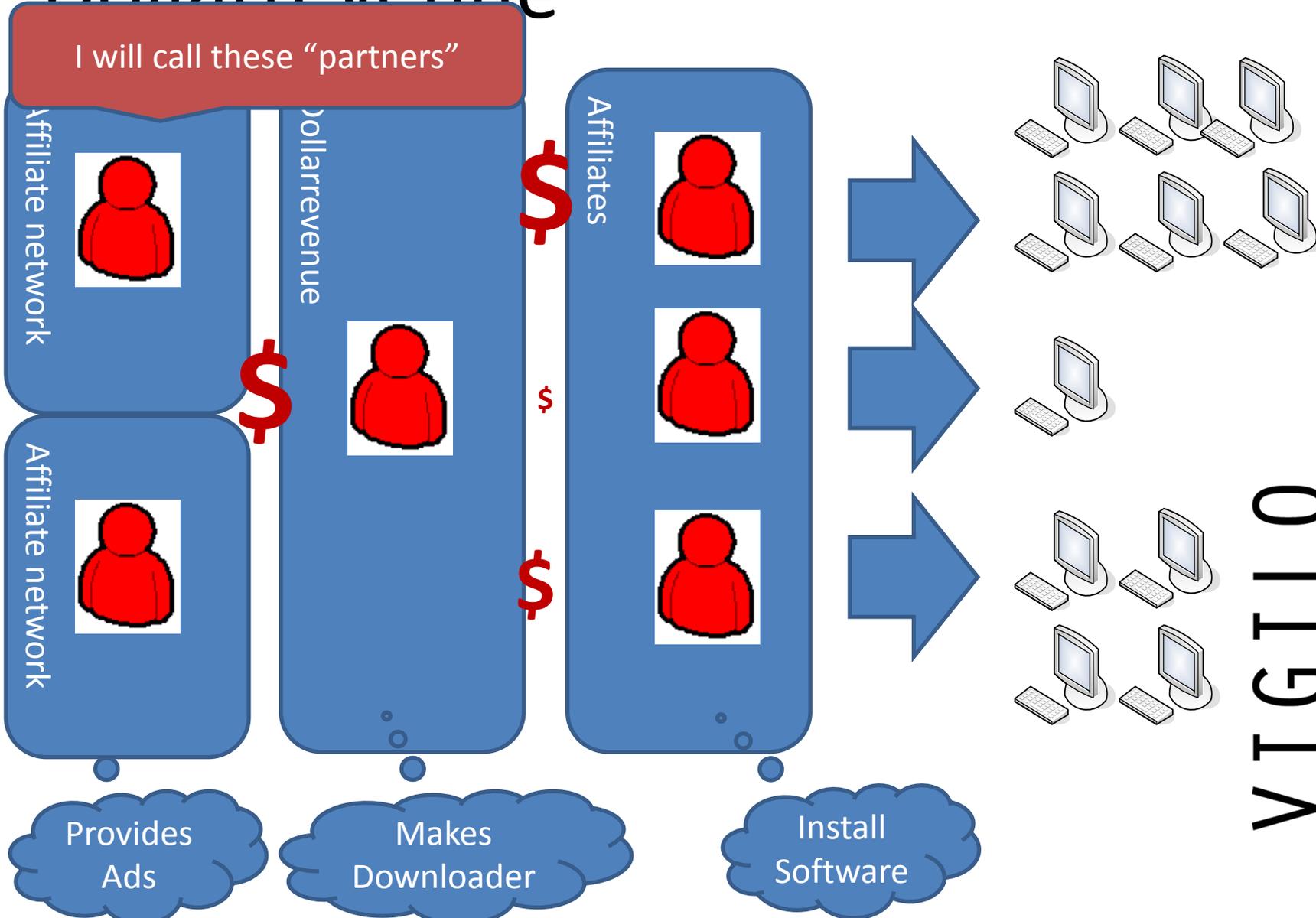
VIGILLO  
consult

# Diagram



VIGI  
consult

# Dollar revenue



**VIGILLO**  
consult

# Result: specialisation and facilitators

## DR Affiliate: Installation

- Herder: Botnet Operation
- Spam: lists
- Websites: SEO

## DR Suspects: DR Software

- Hosting
- Payments

**VIGILLO**  
consult

# International?

- Dollarrevenue:
  - 22M hosts
  - 1 to 2% NL
- Market:



DollarRevenue payouts:	
USA	\$ 0,30
Canada	\$ 0,20
United Kingdom	\$ 0,10
China	\$ 0,01
Other countries	\$ 0,02

# International!



VIGILLO  
consult

# Three points

- Division of labour
- Extensive facilitation and specialisation
  - Legal
  - Illegal
- Across International boundaries

# VIGILLO

consult

## Dollarrevenue

# The Law

- Administrative Decision on End User Rights and Universal service (4.1 BUDE):
  - Information on what is placed
  - A means to refuse the installation/placement
- Follows from EU telecoms package (ePrivacy directive 2002/58/EC)

# EU Law

- Aims to provide similar protection to ALL consumers in internal market
- “Harmonisation”
- Does not cover enforcement
  - National matter
  - Third pillar (law enforcement)

# Fine!

- ACM investigates
- November 2007
- Fines 2 individuals and 3 companies a total of € 1.000.000
- Two appeals stages

# Dollarrevenue & ACM agree:

Not disputed:

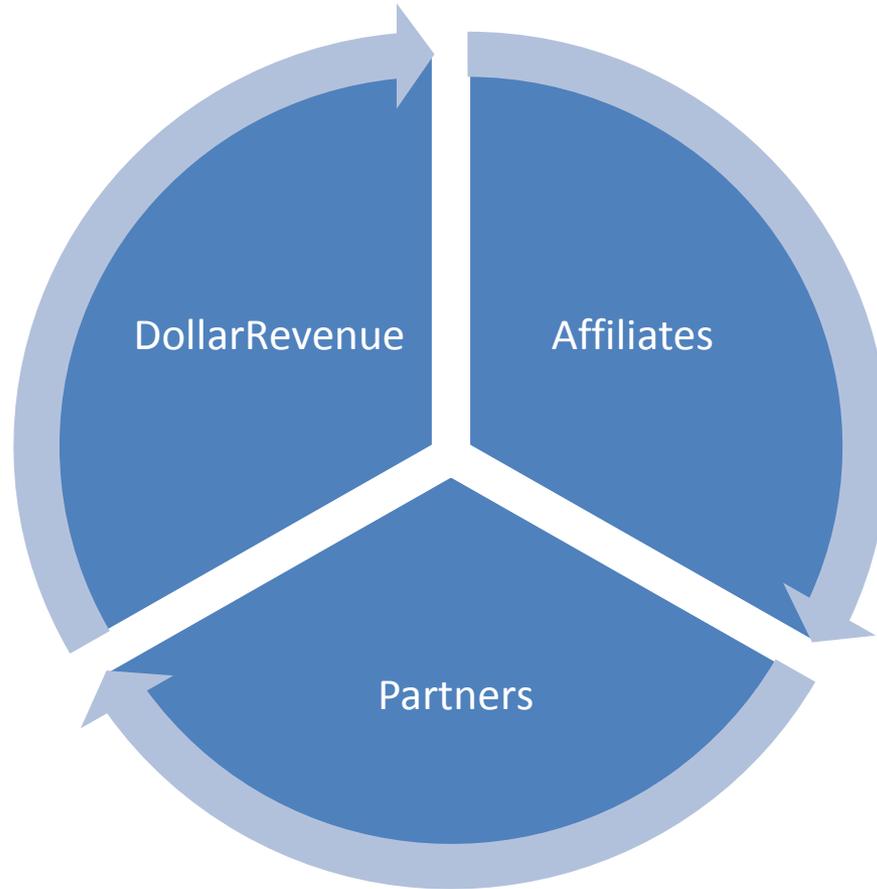
- “Software was placed”
- Staged downloader
  - DollarRevenue Controlled software “bundle”
  - Affiliates placed software using several methods
  - Most of these were illegal – mostly since information was lacking (EULA, ActiveX/Browser warnings are insufficient)

# But.... Who?

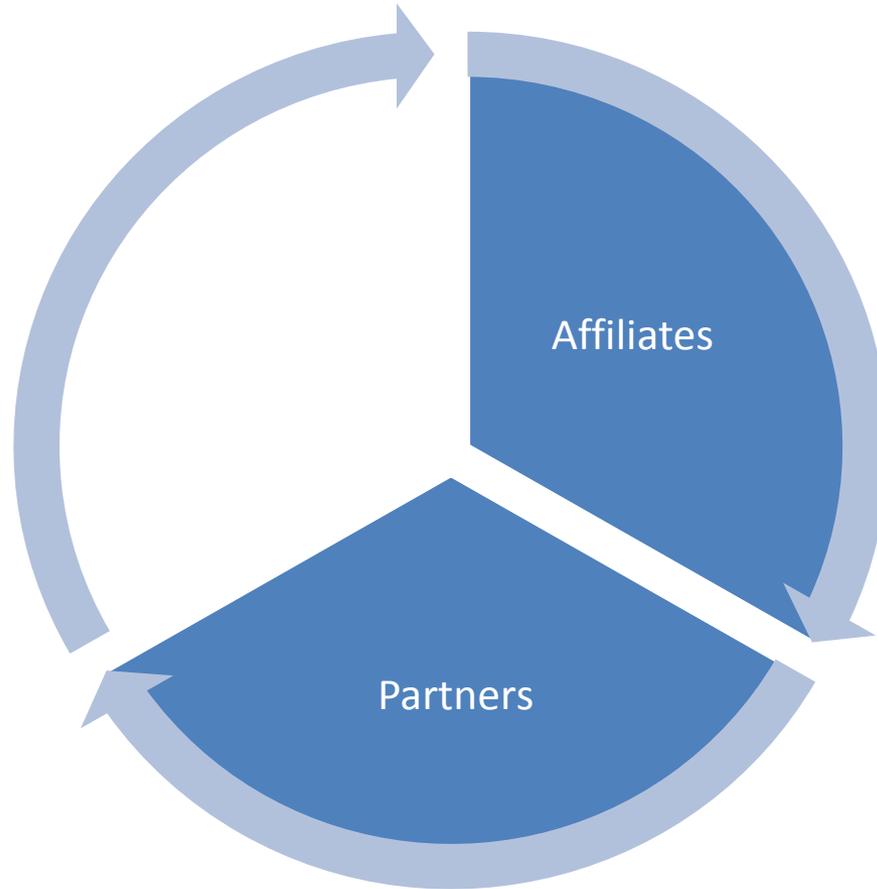


**VIGILLO**  
consult

# ACM/OPTA



# DollarRevenue



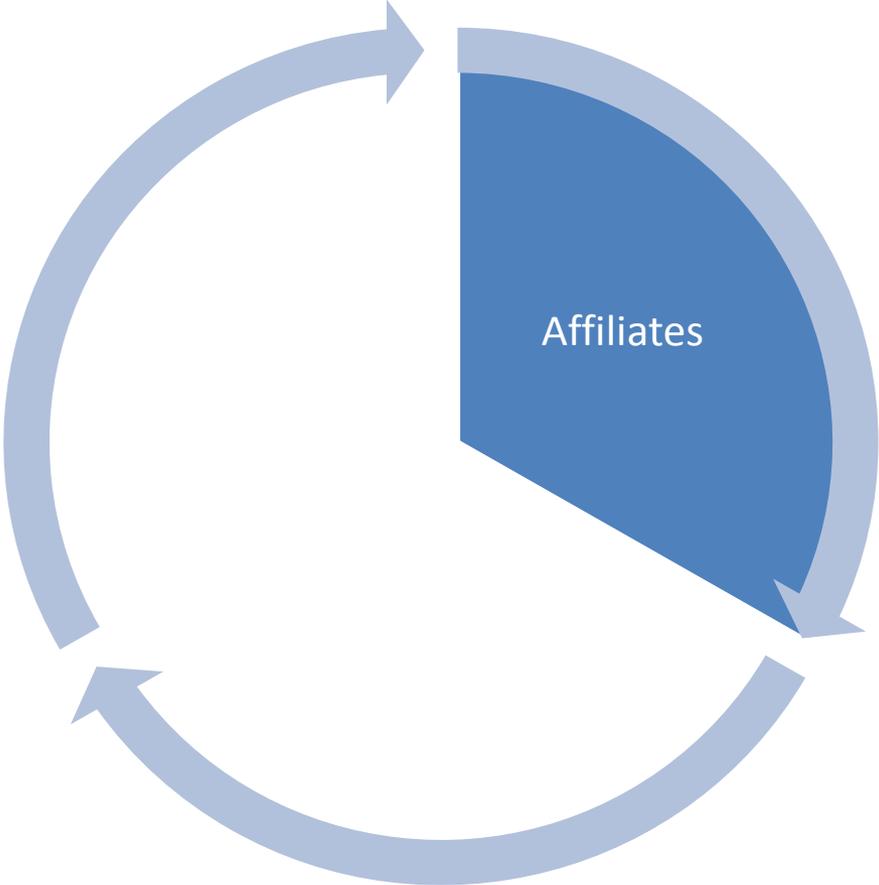
# What do you think?

- A: Affiliates
- B: Partners
- C: DollarRevenue
- D: All of the above



VIGILLO  
consult

# The Court

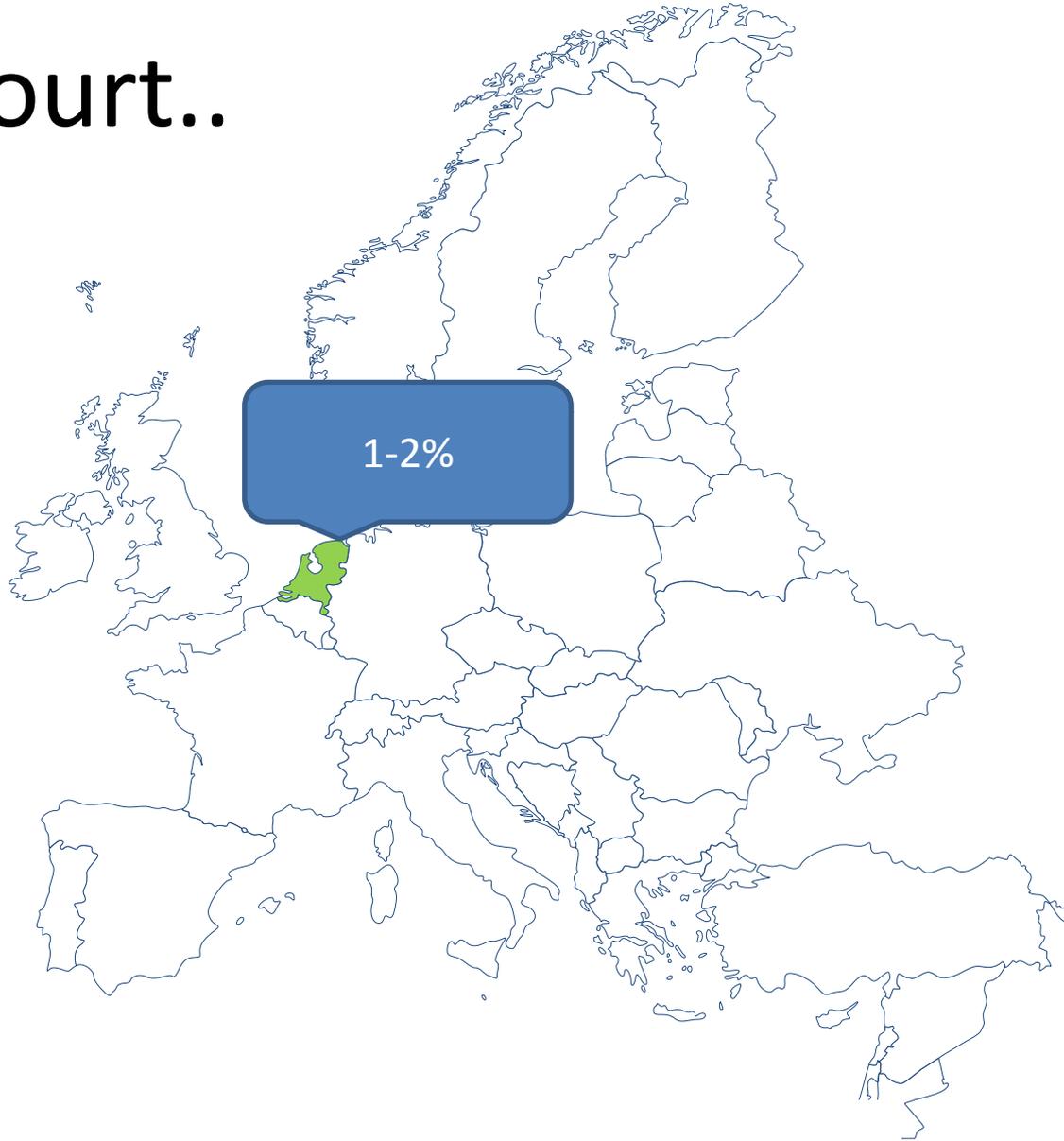


And then..



**VIGILLO**  
consult

# The court..



# VIGILLO

consult

## Analysis

How to...

# Gap analysis...



Autoriteit  
Consument & Markt

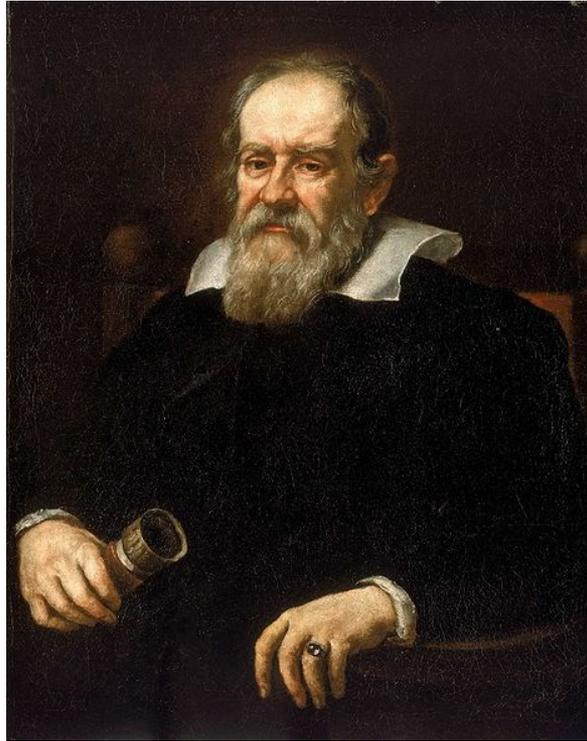


VIGILLO  
consult

# Gap analysis...

- Gap between security measures and criminal enforcement
  - Security: ISO 2700x, PCI DSS, COBIT etc...
  - Criminal enforcement: hacking, computer crime
- Difficulties in addressing facilitators to a crime?
  - Division of labor
  - Specialisation

# Gap analysis...



**VIGILLO**  
consult

# Issues?



**VIGILLO**  
consult

# Conclusion

How to... Set up a malware shop in the Netherlands:

- Find many affiliates!
- Make sure they are not from the EU..
- Install abroad (that is .. not in the Netherlands)
  
- AND: Don't piss off Dutch police..