EuropaInstitut an der Universität Zürich

6. upc cablecom lecture

15. Oktober 2012

Tator Internet

Europäische / Internationale Bekämpfungsstrategien

Criminal money flows on the Internet

Alexander Seger

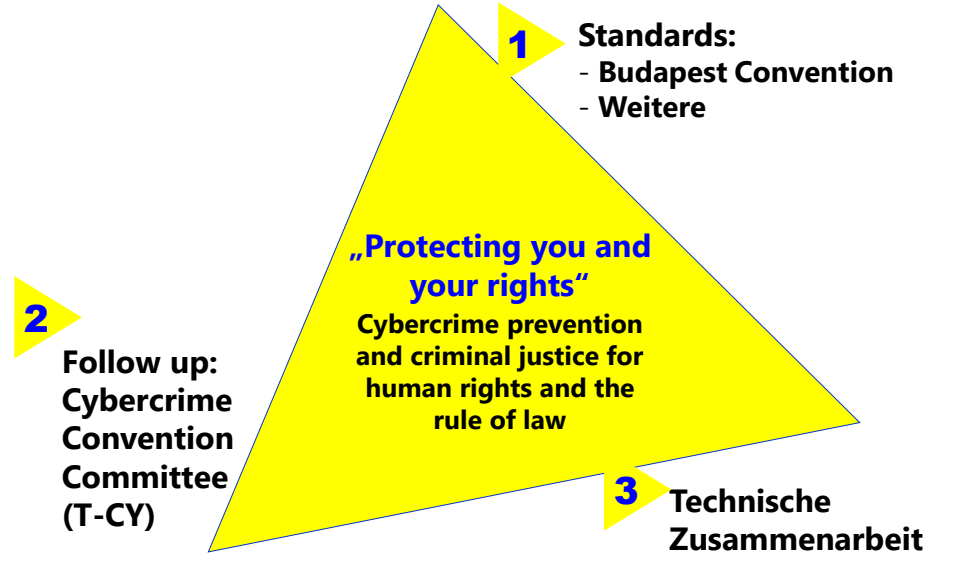
Europarat, Strasbourg

alexander.seger@coe.int www.coe.int/cybercrime

1

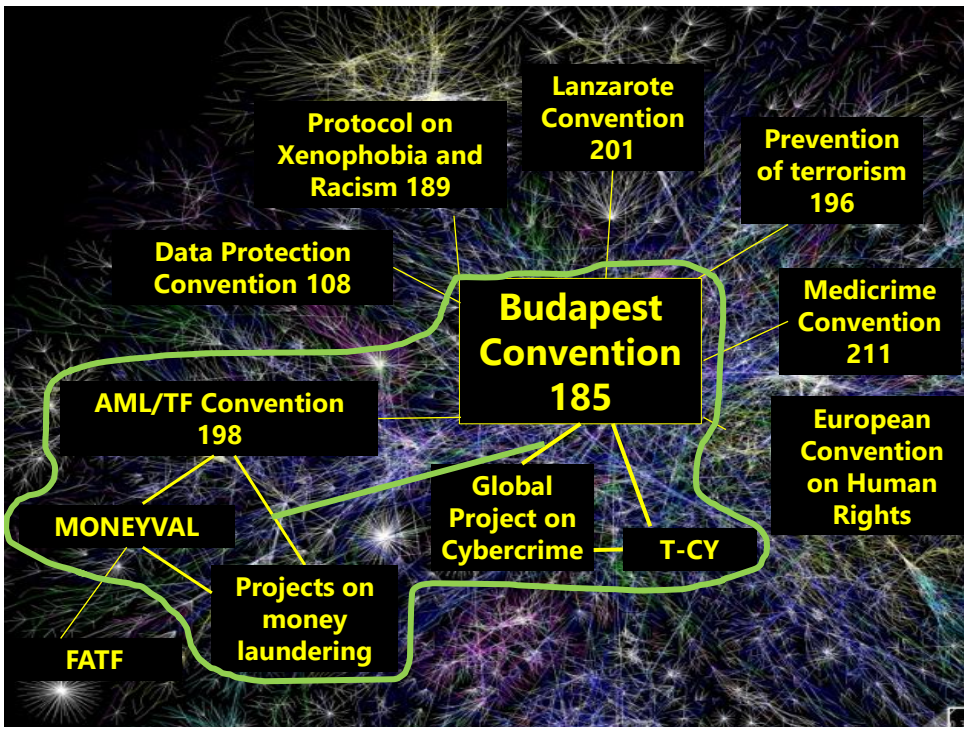
2

Cybercrime: Ansatz des Europarats



www.coe.int/cybercrime 3

3



4

MONEYVAL / Global Project on Cybercrime: Typology study

Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction

Start: Octopus Conference & MONEYVAL Plenary 2009
End: Adopted/published March 2012

Objectives of the study:

- to examine specific money laundering and terrorist financing risks and methods, trends and typologies
- to develop indicators to identify criminal money flows and money laundering on the Internet
- to identify possible solutions with regard to preventive measures, multi-stakeholder action, the seizure and confiscation of criminal money, and the investigation of money laundering and terrorist financing on the Internet and where possible, document good practices

5

5

Was ist Cybercrime?

Budapest Convention on Cybercrime:

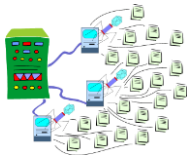
- Straftaten gegen Computer (Budapest Convention Artikel 2-6)
- Straftaten mit Hilfe von Computern (Budapest Convention Artikel 7-10), darunter Betrug
- Im Hinblick auf Strafverfolgung und internationale Zusammenarbeit: Elektronische Beweise im Zusammenhang mit jeder Straftat

6

6

Cybercrime tools, infrastucture, platforms

- Malware
  - Viruses, worms, trojans ►remove security applications, download additional malware, infect files, steal login and account credentials and other data
  - Web remains main vehicle for malware ►infections by visiting infected sites
  - Email threats ► spam as vector for malware and fraud
- Botnets
  - Main tool for cybercrime and
  - Main risk for cybersecurity (DDOS)
  - Organising for cybercrime



- Criminal domains ►anonymous and „bullet proof“ hosting of criminal domains
- Organising for cybercrime
  - Underground economy
  - Organised crime
  - Persistent threats against political or economic targets
  - Financing of terrorism
- Money mules
- Technology/context
  - Social networking platforms
  - Cloud computing

7

7

Cybercrime and predicate offences on the Internet

- Fraud
  - identify theft
  - man-in-the-middle-attacks
  - payment card fraud
  - account take over
  - mass-marketing fraud
  - pyramid schemes
  - confidence and action fraud
- Child abuse materials
- Counterfeit medicines
- IPR
- Extortion
- Many other forms of traditional crimes committed on the Internet

8

8

Typologies and case studies

1. Money remittance providers
2. Wire transfers and account take-over
3. Cash withdrawals
4. Internet payment services
5. Money mules
6. International transfers
7. Digital electronic currency
8. Purchase through the Internet
9. Shell companies
10. Prepaid cards
11. Online gaming and online trading platforms

Red flags and indicators for potential money laundering

- **Persons holding large number of accounts with the same Internet payment services provider**
- **Discrepancies between submitted customer identification and IP address**
- **Suspicious IP addresses, and suspicious usernames**
- **Log-ins or attempting log-ins from non trusted IP addresses or from user's ID previously identified as associated with suspicious activity**
- **Unusual conditions and complexity of the transaction: high frequency of money transfers in a short time, large and diverse source of funds, large and diverse payment methods for the beneficiaries**
- **Etc.**

Countermeasures – Stakeholders

Anti-money laundering system

- Financial sector institutions obliged to report
- Financial intelligence units (FIUs)
- Asset recovery/financial investigation agencies
- Prosecutors and judges
- Supervisors and regulators
- International monitoring bodies

Anti-cybercrime institutions

- Specialised prosecution services
- High-tech crime units
- Computer forensic laboratories
- 24/7 points of contact
- Prosecutors and judges

Financial sector (online)

- Payment cards industry
- Online banking services
- Online payment platforms
- Content providers
- Money transfer services

Internet service providers (ISPs)

- Telecommunication providers
- Internet access providers
- Hosting providers
- ICANN, registries and registrars

Institutions monitoring Internet activity

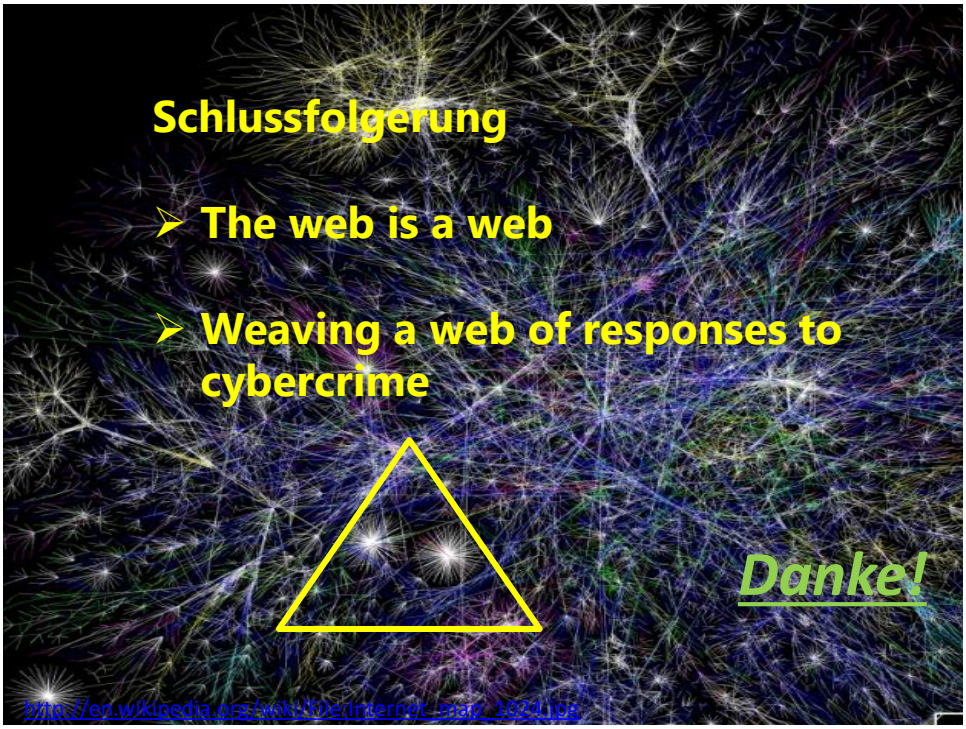
- CERT/CSIRT
- Industry, research institutions, associations or initiatives against cybercrime

11

Countermeasures – The way ahead

- Research and other measures to prevent/mitigate AML/TF and cybercrime risks
- AML/CTF and anti-cybercrime strategies
- Legislation (harmonised with Budapest Convention and Convention 198
- Reporting mechanisms
- Guidance and typologies for financial and non-financial institutions
- Specialised cybercrime units
- Inter-agency cooperation and parallel financial investigations when pursuing cybercrime and money laundering
- Public-private cooperation and information exchange on criminal money flows on the Internet
- Training of criminal justice and AML authorities in cybercrime and electronic evidence matters
- International cooperation between FIUs and Cybercrime Units

12


Schlussfolgerung
The web is a web
Weaving a web of responses to cybercrime
Danke!
http://en.wikipedia.org/wiki/File:Internet_map_1024.jpg

13