Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE CONSEIL DE L'EUROPE
Implemented by the Council of Europe

CyberCrime@IPA and CyberCrime@EaP

Criminal money flows on the Internet
Common issues identified

International workshop, Kyiv, Ukraine, 27-29 February 2012

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

www.coe.int/cybercrime

1

Problem analysis

- Lack of information on criminal money flows and cybercrime/ -fraud trends – lack of reporting system
- No pro-active approach to follow criminal money on the internet (in particular if offender and victims in foreign jurisdictions)
- Limited data exchange between LEA (cybercrime units) and FIUs
- Limited skills/knowledge of financial crime issues by cybercrime investigators and on cybercrime by financial and money laundering experts
- Lack of central registers eg of bank accounts or legal persons
- Limited obligations of financial sector and ISPs to cooperate
- Problem of international cooperation and access to data abroad

Stakeholder analysis

FIUs do cooperate with multiple financial sector and LEA stakeholders. This is an opportunity!

Involve cybercrime units!

Countermeasures - Interagency cooperation

- Good practices of joint investigative teams or units available - Include cybercrime investigators
- Make more use of e-information exchange between institutions
- Make use of multi-agency groups for intelligence exchange, including cybercrime units (FATF R 30, 31)
- Set up specific, more limited groups for operational information exchange and cooperation in investigations (FATF R 30, 31)
- Make use of increased LEA/FIU information exchange to investigate criminal money on the Internet (money laundering and predicate offences) at domestic and international level (FATF R 40, Budapest Convention)

Countermeasures – Public-private cooperation

- Set up trusted fora for public-private intelligence exchange (consider interest of private sector)
- Protection of financial sector against cyberattacks
- Public-private cooperation on the laundering, search, seizure and confiscation of crime proceeds and asset recovery
- Establish clear obligations/rules/procedures for reporting and cooperation by private sector (financial sector, ISPs, mobile operators)
- Make use of LEA/ISP cooperation guidelines

Countermeasures – Reporting systems

- Expand existing crime reporting systems to include cybercrime
- Cybercrime reporting systems to include specific features to serve intelligence/analytical purposes and trigger investigations
- Use reporting systems also for prevention and public information

Countermeasures – International standards

Make use of international standards and good practices:

- Convention 198 on laundering, search, seizure and confiscation of proceeds from crim en and terrorist financing
- FATF 40 Recommendations as revised 15 February 2012
- Council of Europe Octopus Guidelines on Law Enforcement /service provider cooperation in the investigation of cybercrime
- MONEYVAL/Global Project on Cybercrime Typology study (March 2012)

Thank you

Alexander.seger@coe.int