www.coe.int/cybercrime

Data Protection and Cybercrime Division
Directorate General
Human Rights and Rule of Law
Strasbourg, France

Version 8 October 2012

## CyberCrime@EAP and CyberCrime@IPA

**Regional Cooperation against Cybercrime**

**Report on Activity 6.1**

# Criminal money flows on the Internet

**Intra-regional workshop**
**Kyiv, Ukraine, 27-29 February 2012**

**Project funded by the European Union and co-funded and implemented by the Council of Europe**

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

## Contents

For further information please contact:

Data Protection and Cybercrime Division
Directorate General Human Rights and Rule of Law
Council of Europe
Strasbourg, France
Tel: +33-3-8841-2103
Fax: +33-3-9021-5650
Email: cristina.schulman@coe.int
www.coe.int/cybercrime

# 1 Introduction

The workshop on Criminal Money Flows on the Internet was organised as an intra-regional activity of the joint EU/Council of Europe projects CyberCrime@IPA[1] and CyberCrime@EAP[2].

The CyberCrime@EAP project Cybercrime is one of four projects under the Eastern Partnership Facility of the European Union (EU) and the Council of Europe (CoE). The project has a duration of thirty months (1 March 2011 – 31 August 2013) and a budget of 724,040 Euro. It is implemented by the Council of Europe in the Eastern Partnership (EAP) countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine).

Expected result 2 is related to – among others – *financial investigations*:

> Financial investigations: awareness raised to confiscate proceeds from crime on the Internet among representatives of FIUs, asset recovery and financial investigation bodies, police and prosecution dealing with high-tech and economic crime and corruption, financial and supervisory authorities, banks and ISPs. Interagency and public-private cooperation in this area is strengthened as well as countermeasures and good practices are identified.

Under this result, the project supports awareness raising of the need for confiscating proceeds from crime on the internet, strengthens interagency and public-private cooperation against criminal money flows on the internet as well as identifies countermeasures (good practices) that could be implemented in the EAP countries.

The Cybercrime@IPA project started on 1 November 2010; its launching conference took place on 17-18 February 2011 in Istanbul, Turkey. Countries and areas participating in CyberCrime@IPA are Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, "the former Yugoslav Republic of Macedonia", Turkey and Kosovo3. The project has a duration of two years and a budget of Euro 2.78 million. The project is implemented by the Council of Europe. It comprises eight expected results.

Expected result 6 is related to financial investigations:

> Financial investigations: Capacities of financial investigators, Financial Intelligence Units (FIU), and/or relevant law enforcement units in charge of fighting against cyber criminals in following crime proceeds on the internet improved and their cooperation with the financial sector strengthened. (the first event in this respect was held in Belgrade on 17-18 March 2011)

Under this result, the project will support joint training courses carried out for cybercrime investigators, financial investigators and financial intelligence units, and help establish regional and domestic trusted fora for regular information exchange between public and private sector stakeholders.

It should also be noted that the Council of Europe (Moneyval and Global Project on Cybercrime) elaborated a typology study on Criminal money flows on the Internet: Methods, trends and multi-stakeholder counteraction. The study was adopted in the 38th Plenary

[1] Under the Instrument of Pre-Accession (IPA)

[2] Implemented under the Eastern Partnership - Council of Europe Facility (EAP).

[3] All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo. Kosovo was not represented in the workshop.

meeting of MONEYVAL, 5-9 March. Final amendments proposed during the workshop in Kyiv were reflected in the report subsequently adopted by MONEYVAL.

Furthermore, the European Union and the Council of Europe are currently implementing two joint projects in Serbia, namely, the Criminal Asset Recovery (CAR) project and the MOLI-Serbia project against money laundering.

The Intra-regional workshop in Kyiv, held on 27-29 February 2012, was the first project activity under Expected result 2 of the CyberCrime@EAP project and the second activity under Expected result 6 of the CyberCrime@IPA project.

The Regional workshop was aimed at the following:

- To raise awareness of the need to confiscate proceeds from crime on the Internet,
- To strengthen interagency and public-private cooperation against criminal money on the Internet,
- To identify countermeasures (good practices) that could be implemented in IPA countries and areas.

As a main result of this activity each delegation prepared its set of recommendations for measures that could be taken their respective country/area.

Participants of the meeting represented a wide spectrum of institutions involved in detecting, tracing, seizing and confiscating criminal money on the Internet from the countries/areas of both regions.

CyberCrime@EAP: Armenia, Azerbaijan, Belarus, Georgia, The Republic of Moldova and Ukraine:

- Financial intelligence units,
- Asset recovery and/or financial investigation bodies,
- High-tech crime units of the police, units dealing with economic crime and corruption,
- Prosecution services.

CyberCrime@IPA: Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, "the former Yugoslav Republic of Macedonia" and Turkey:

- Financial intelligence units,
- Asset recovery and/or financial investigation bodies,
- High-tech crime units of the police, units dealing with economic crime and corruption,
- Prosecution services.

Kosovo* was not represented at the Workshop.

The private sector was represented by PayPal and VISA Inc. (See the appended list of participants for further details.)

Three experts were invited to share their experience:

- from Belgium: Frederic van Leuw, Federal Magistraat
- from Ireland: David O'Reilly, Financial Cybercrime Analyst – free lance expert;
- from the Financial Action Task Force Secretariat: Timothy Goodrick, Policy Analyst.

# 2 Criminal money flows on the Internet: the issue

## 2.1 Cybercrime – Tools, infrastructure, threats, trends

The following sections outline, at a high level, some of the tools and infrastructure commonly used by attackers to perform cyber attacks to generate illicit proceeds on the internet. This is followed by a brief examination of emerging threats and trends.

### 2.1.1 Cybercrime tools

#### 2.1.1.1 Malware

Malware (malicious software) comes in many forms[4] and can be purchased on the black-market (underground economy), thus potential attackers do not need technical skills themselves. Some of the most common uses of malware are:

- To steal usernames, passwords and other account credentials;
- To present the user with pop-up advertisements. This is known as "adware";
- To cause the user's PC to become part of a botnet, as described above;
- To try to convince the user that they have a virus on their computer which they need to pay to have removed. This is known as "fake anti-virus";
- To capture and encrypt some of a user's content, which the user must then pay to regain access to. This is known as "ransomware".

#### 2.1.1.2 Botnets

A Botnet is a collection of computers that have been infected by malware. This enables criminals to access and remotely control the computers. The criminal issues instructions to the compromised computers via a Command and Control (C&C) infrastructure. The scale of botnets has increased substantially in recent years[5].

Botnets enable an attacker to perform tasks such as:

- Gathering credit card details and other credentials, such as online banking login details.
- Performing DDoS (Distributed Denial of Service) attacks[6].
- Recording a user's browsing activity and reporting it to the attacker via the command and control infrastructure[7].

[4] Malware is a generic term covering many different forms of malicious software including viruses, Trojan horses, worms, spyware, adware and rootkits.

[5] http://www.net-security.org/secworld.php?id=9648;
http://www.wired.com/beyond_the_beyond/2011/03/microsoft-versus-rustock-botnet/
Microsoft Security Intelligence Report, Volume 8, July through December 2009. Botnets such as "Rustock" were believed to be able to send up to 30 billion spam mails per day.

[6] This attack involves instructing all of the compromised computers in the botnet to send as much traffic as they possibly can towards (for example) a target website. The volume of traffic received by the target website could mean that it will become unavailable because it cannot service legitimate incoming requests.

[7] This technique is also used by attackers to gather intelligence about the detailed structure of a particular financial institution's online banking website. This information can then be used to craft a customized attack against this particular institution.

#### 2.1.1.3 Spam

Spam is the name given to unsolicited email and is still a major part of criminal activity online. Spam email is used to promote fake products and services (including counterfeit pharmaceuticals) and is also frequently used to compromise customer PCs with malware, either by attaching a malware directly to the email or by containing a link to a website that contains the malware.

### 2.1.2 Cybercrime infrastructure

#### 2.1.2.1 Proxies

Proxying is a technique of transmitting Internet traffic via a third party. Beside the legitimate uses[8], proxies can also facilitate criminals to conceal their identity online and can make difficult to trace the source of communication[9].

#### 2.1.2.2 Bulletproof hosting

Due to lack of cooperation, engagement between law enforcement and Internet infrastructure providers criminals have identified that it can be challenging for both national and international law enforcement agencies to have servers taken down when they are hosted in these jurisdictions. Registrars and registries in such countries often fail to exercise due diligence when domains are registered with incorrect information.

#### 2.1.2.3 Underground economy

There are many active communities of individuals offering goods and services for sale online[10] such as:

- Credit card details and other information used for identity theft;
- Offshore banking services and the creation of shell companies;
- "Expert services" such as malware development, recovery of data and anti-forensics and malware toolkits, fake anti-virus software;
- Spamming services;
- "Bullet proof" web hosting;

### 2.1.3 Threats and trends

Criminals find ways to exploit vulnerabilities of new technologies, platforms. The following section summarises some emerging or recent technologies and the types of attacks criminals have carried out against them.

#### 2.1.3.1 Social network platforms

Social networking websites have exploded in popularity in recent years[11]. With such a large user base, social networks present an obvious opportunity for criminals to spread malware, send spam, steal user identities, gather personal information, display fake anti-virus alerts and perform a variety of other schemes[12].

---

[8] http://www.squid-cache.org/

[9] https://www.torproject.org/

[10] Ghostnet is an example of such a forum http://www.guardian.co.uk/uk/2011/mar/02/ghostmarket-web-scam-teenagers

[11] In December 2011 Facebook reported 845 million active user accounts, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

[12] http://www.iseclab.org/papers/irani_dimva.pdf

#### 2.1.3.2 Cloud computing

Cloud computing involves the use of shared infrastructure to deliver services online. These cloud computing services present new challenges for the investigation of cybercrime.

For example, the fact that servers where illegal content is stored may be located in many different jurisdictions can present significant difficulties for law enforcement officers to gather data as part of an on-going investigation in their own jurisdiction[13].

#### 2.1.3.3 Threats against political or economic targets

Ideologically motivated cyber attacks against political or economic targets have become increasingly commonplace. This can include "hacktivism", terrorism, war and conflict by means of computer systems[14].

#### 2.1.3.4 Mobile devices

The ubiquity of mobile devices will also present new challenges for investigation of cybercrime, particularly as these devices become payment devices. Security vulnerabilities have already been identified that could be used for account take-over and other online banking attacks[15].

## 2.2 Offences generating proceeds on the Internet

In many jurisdictions, before a money laundering offence can have taken place a predicate offence which generated some illicit proceeds must have been committed. The following section describe some common online activities that could be considered predicate offences for money laundering.

The offence of identity theft can be defined in various ways[16] but can generally be thought of as consisting of three parts:

- Obtaining the identity. In the context of online attacks, this is achieved through techniques such as the different forms of phishing, keylogging (via malware infection), etc[17]
- Possession of the identity for sale or for use
- Use of the identity. In the online context, compromised identity credentials are often used to perform theft or fraud.

[13] http://www.eurodig.org/eurodig-2010/programme/workshops/workshop-1

[14] The "Anonymous" collective is an example of one of these groups (http://anonanalytics.com/)

[15] https://ub-madoc.bib.uni-mannheim.de/2998/1/dissertation_becher.pdf

[16] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=982076

[17] An example of an alert provided to customers by a mobile telephone operator can be found at: http://www.o2online.ie/o2/my-o2/phishing-alert/
http://www.fbi.gov/news/stories/2009/april/spearphishing_040109
http://us.norton.com/cybercrime/pharming.jsp
http://www.dataprotectioncenter.com/antivirus/symantec/phishers-on-a-live-chat/
http://blogs.rsa.com/rsafarl/chat-in-the-middle-phishing-attack-attempts-to-steal-consumers-data-via-bogus-live-chat-support/
http://community.eu.playstation.com/t5/Website-and-Forum-Help-Feedback/Forum-Phishing-Scam/td-p/14527737
http://www.businessweek.com/technology/content/jul2006/tc20060710_811021.htm
http://krebsonsecurity.com/2010/06/a-spike-in-phone-phishing-attacks/

Both ways of payment card fraud (card present - CP or card not present - CNP)[18] are popular ways to gather card details (gathering valid card data include counterfeit cards, lost/stolen cards and non-receipt of cards[19]).

Beside the phishing attacks (Section **Error! Reference source not found.**) banks may also be vulnerable to man-in-the-middle and man-in-the-browser style attacks[20], which are typically performed by installing malware on the customer's PC, then, when a customer logs into the legitimate online banking website the malware is installed on their computer hijacks their session and it injects additional payment instructions into the logged in banking session.

Confidence fraud schemes involve an attempt by an attacker to defraud by gaining a victim's confidence. Many such schemes[21] are enabled by the low cost of Internet communication (checks, money-orders and others). Investment fraud schemes tend to involve apparently legitimate bank transfers. West African groups rely on wire transfers with funds being collected by using forged identification[22]. Stock market manipulation[23] involves interference with the value of a stock market by manipulating the price of a traded entity. The Internet can be used to facilitate such manipulations.

Auction fraud involves an item being listed for sale over the Internet where the details of the item may be misrepresented or the item is never shipped to the winning bidder[24].

Multi-level marketing schemes, also known as pyramid schemes, involve the selling of goods and services through distributors who are promised a commission not only for their own sales but also for the sales of others that they recruited to join the scheme. Multi-level marketing schemes can involve actual products and services, but may also be based on fake products. Ponzi scheme[25] involves an investor making a financial investment or paying a fee to join the scheme. The apparent return on investment is paid from the investments or fees of other individuals who subsequently join. The scheme continues until the number of new investors tails off, at which point the scheme collapses.

The relatively anonymous nature of Internet communication is a significant enabler of distribution of child abuse materials. The most common techniques used are peer-to-peer networks and web servers with rapidly changing IP addresses[26].

---

[18] Fraud the Facts, June 2011. Published by UK payments and available from http://www.financialfraudaction.org.uk/Publications/.

[19] Fraud the Facts, June 2011. Published by UK payments and available from http://www.financialfraudaction.org.uk/Publications/.

[20] http://en.wikipedia.org/wiki/Man-in-the-browser

[21] http://www.fincen.gov/news_room/rp/reports/pdf/IMMFTAFinal.pdf

[22] http://www.consumerfraudreporting.org/nigerian.php

[23] http://www.sec.gov/answers/pumpdump.htm

[24] The US Internet Crime Complaint Center reports that in 2009, 19% of all complaints related to non-delivery or purchased goods. (http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf)

[25] http://www.sec.gov/answers/ponzi.htm

[26] A technique known as DNS fast-fluxing is used to rapidly change the IP address associated with a particular domain name. In Child Sexual Abuse Images – an analysis of websites by Cybertip.ca (November 2009) (http://www.cybertip.ca/pdfs/Cybertip_researchreport.pdf), on page 62 it is reported that over a 48-hour period, cybertip.ca observed one website cycle through 212 unique IP addresses, located in 16 different countries. The IP addresses are reported as changing approximately every three minutes.

The sale of counterfeit pharmaceutical involves medicinal products and devices, the identity or source of which are falsely represented[27],[28].

Violation of copy- and related rights can range from downloading of pirated music and unlicensed software to industrial espionage[29],[30].

Online extortion has many forms used by criminals to extort funds from victims over the Internet (e.g. threatening with DdoS attack, infection with ransomware.

## 2.3 Findings of typology studies

There have been two typology studies prepared recdently. As a result of the joint project by MONEYVAL and the Council of Europe's Global Project on Cybercrime entitled "Criminal Money Flows on the Internet: methods, trends and multi-stakeholder counteraction."[31] The Financial Action Task Force (FATF) typologies study entitled "Money Laundering Using New Payment Methods".[32]

The study prepared under the MONEYVAL/Global project on cybercrime framework examined reported money laundering typoligies such as

- Money remittance providers;
- Wire transfers and account take-overs;
- Cash withdrawals;
- Internet payment services;
- Money mules;
- International transfers;
- Digital/Electronic currency;
- Purchases through the Internet;
- Shell companies;
- Prepaid cards;
- Online gaming and trading platforms.

The FATF Money Laundering Using New Payment Methods report, involved the analysis of 33 case studies, which mainly involved prepaid cards or Internet payment systems. Three main typologies related to the misuse of new payment method (NPM) accounts for money laundering were identified and discussed:

- Third party funding (including straw men and nominees);
- Exploitation of the non-face-to-face nature of NPM accounts;
- Complicit NPM providers or their employees.

[27] http://www.eaasm.eu/Media_centre/News/February_2010

[28] http://www.pharmatimes.com/Article/10-02-16/One_in_five_Europeans_buying_fake_drugs_%E2%80%93_Pfizer_survey.aspx

[29] http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Global%20Impacts%20-%20Final.pdf

[30] http://portal.bsa.org/Internetreport2009/2009Internetpiracyreport.pdf

[31] http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2012)6_Reptyp_flows_en.pdf. Adopted by MONEYVAL at its 38th Plenary meeting (5-9 March 2012).

[32] http://www.fatf-gafi.org/dataoecd/4/56/46705859.pdf, published October 2010.

## 2.4 International standards and measures

### 2.4.1 CETS 185

The Budapest Convention is the first internatinonal legislative tool or the global framework of reference for cybercrime legislation. The treaty has served as a guideline for reforming legislations, training manuals, model laws and technical assistance. It specifies substantive law (offences against computers, computer systems as well as offences committed by means of computers), procedural law provisions but also general and specific provisions on cooperation.
The Convention is complemented by Protocol CETS 189 (of 2003) on xenophobia and racism committed by means of computer systems.

The Cybercrime Convention Committee (T-CY) has been established under Article 46 in order to allow the parties to the Convention to consult in view of facilitating the effective implementation of the Convention, to exchange information and to consider possible amendments or protocols to the Convention. The T-CY does not have a monitoring or evaluation function, but in November 2011 decided to start assessing implementation of the Budapest Convention by the Parties.

### 2.4.2 CETS 198

The 2005 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism ("The Warsaw Convention", CETS 198) updates and revises the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime ("The Strasbourg Convention", CETS 141).

The Convention covers, among other things procedural law and investigative provisions, criminalisation of laundering offences, preventive measures, the postponement of domestic suspicious transactions, international requests for information on bank accounts, on banking transactions, monitoring of banking transactions, establishment of financial intelligence units (FIUs) and co-operation between FIUs. The Convention provides for a monitoring mechanism, through a Conference of the Parties to ensure that its provisions are being effectively implemented.

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) is an independent monitoring body entrusted by the Committee of Ministers of the Council of Europe with the task of assessing compliance with the principal standards to counter money laundering and terrorist financing (AML/CFT) and the effectiveness of their implementation.

### 2.4.3 FATF Recommendations

The FATF Recommendations[33] set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. The FATF Recommendations set out the essential measures that countries should have in place to:

- Identify the risks, and develop policies and domestic coordination.
- Pursue money laundering, terrorist financing and the financing of proliferation.

[33] http://www.fatf-gafi.org/dataoecd/49/29/49684543.pdf, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, February 2012.

- Apply preventive measures for the financial sector and other designated sectors.
- Establish powers and responsibilities for the competent authorities (e.g. investigative, law enforcement and supervisory authorities) and other institutional measures.
- Enhance the transparency and availability of beneficial ownership information of legal persons and arrangements and
- Facilitate international cooperation.

# 3 Countermeasures

Several public and private sector organisations have adopted a range of measures in response to the increasing criminal money flows on the Internet. These measures may serve as good practice and could become elements of more systematic future approaches aimed at prevention of money laundering and terrorist financing and at the search, seizure and confiscation of proceeds from Crime on the Internet.

Public – private information sharing and analysis could overcome difficulties originating from limited data and knowledge of fraud and other types of cybercrime is a key obstacle to preventing and controlling cybercrime and criminal money flows on the Internet. Awareness that organised criminal structures may be behind what appears to be instances of minor fraud is limited.
Several example of good practice are included are available in the Tyopolgy Study on Criminal money flows on the Internet[34].

Public education and awareness are essential elements to prevent fraud and other forms of crime. There are an increasing number of public websites with

- General fraud prevention information[35]
- Educational materials and courses[36]
- Specific resources to prevent risks in a specific sector[37]
- Assistance to victims of fraud[38]

Regulatory and supervisory measures include risk management and due diligence as well as due diligence for registrars and registries[39].

Creation of a legal framework based on international standards (the Budpaest Convention, Warsaw Convetnion) assist countries to meet challenges of the investigation of cybercrime, money laundering, financing terrorism.

Specialised cybercrime/high-tech crim units are essential tools to investigate, prosecute and adjudicate cybercrime. In 2011, the EU Cyber Crime Task Force and the Council of Europe cooperated in the preparation of a good practice study on specialised cybercrime units[40].

---

[34] http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2012)6_Reptyp_flows_en.pdf.
[35] http://www.ic3.gov/preventiontips.aspx
[36]For example: http://www.polizei-nrw.de/koeln/Vorbeugung/kriminalitaet/Internet-und-datenkriminalitaet/
[37]For example, Resources for merchants to prevent payment card fraud http://www.visa.ca/en/merchant/fraud-prevention/index.jsp
[38] For example: http://www.actionfraud.org.uk/home
[39] Internet Corporation for Assigned Names and Numbers (www.icann.org)
[40] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf

Cooperation between authorities responsible for financial investigations and confiscation of proceeds, measures against money laundering and cybercrime is considered an important condition for success against criminal money on the Internet.

Public-Private Cooperation and Information Exchange is one of the measures delivering the greatest impact on the prevention and control of criminal money flows on the Internet. It addresses a key problem; the limited sharing and use of existing information between domestic financial institutions and between financial institutions and law enforcement. There have been several initiatives, fora established to facilitate cooperation between public authorities and industry[41].

Training on cybercrime, threats, trends, typologies, technology, international standards ofr the different stakeholders of investigating, prosecuting and adjudicating cyber offences is required is many countries. Certain organisational initiatives have been launched[42] to support law enforcement although concepts, guidelines have been elaborated to further increase the importance of training as well as to support national authorities with elaborating training strategies[43]. There are other, on-going initiatives of the Council of Europe supporting national authorities in the cooperation against cybercrime[44].

[41] The Irish Banking Federation – High-tech Crime Forum, Incident Management Working Group in Hungary, NCFTA in the United States http://www.ncfta.net/, Financial Services – Information Sharing and Analysis Centres (FS-ISAC) etc. for further information, please consult http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2012)6_Reptyp_flows_en.pdf

[42] ECTEG - http://www.ecteg.eu/; University College Dublin Centre for Cybercrime Investigations - http://cci.ucd.ie/;

[43] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Cyber%20IPA%20reports/2467_LEA_Training_Strategy_Fin1.pdf
file:///Transit_src/Internet/DGHL/Cooperation/EconomicCrime/Web/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09.pdf

[44] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Default_eeg_en.asp

# 4 Country/area reports

## 4.1 Summary of the current situation in both regions

A Cybercrime Situation Report was prepared under both the CyberCrime@EAP and CyberCrime@IPA projects on the basis of the information submitted by project teams from each country/area. This report provides information on the current capabilities of the 14 project countries/areas (6 countries of the EAP region and 8 countries of the IPA region) in terms of dealing with cybercrime, analyses their particular situation and sets out a number of recommendations for implementation at national or regional level.

According to the findings of these reports the following types of crime are encountered on the Internet in the project countries/areas:

- CyberCrime@EAP:

Computer fraud, electronic banking and electronic transfer fraud, credit card fraud (including counterfeiting of cards), identity thefts and phishing type frauds also.

- CyberCrime@IPA:

Computer fraud, "Nigerian" fraud, electronic banking and electronic transfer fraud, credit card fraud (including counterfeiting of cards), identity thefts, as well as phishing frauds, investment fraud, child pornography and illegal betting.

The main obstacles to the prevention and control of criminal money flows on the Internet identified in the Reports with respect to all countries/areas are:

- Insufficient technical capacity to determine cash flows, especially when anonymous services are used and where data is held in countries where international legal assistance is needed.
- The speed of transactions is not matched by the speed of legal procedures needed to trace them.
- Lacunae in the legislation aimed at the prevention of criminal money flows on the Internet; absence of simplified procedures to enable effective communication between institutions.
- Lack of equipment and trained staff.

Examples of cooperation identified in the Situation Report involve almost exclusively cooperation between public sector organisations. There is a lack of information regarding collaboration with industry sectors; however, this activity is seen as necessary by most involved in dealing with this type of criminal activity. It should be said that this is not exclusive to this region.

The Reports recommended enhancing the capability at regional and country/area level to combat illegal money flows on the Internet by adopting the relevant findings of the Council of Europe study "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction". The relevant public sector, law enforcement agencies and industry players should be involved in the development of practical solutions.

## 4.2 Situation in the project countries/areas of the CyberCrime@IPA project

### 4.2.1 Albania

#### 4.2.1.1 Current situation - summary

The main types of fraud affecting Albania include: online purchase of travel tickets using stolen credit card data, which have been successfully investigated, and unlicensed online gambling, which has been identified but not investigated.

This is a new area for the Albanian authorities that have identified the following shortcomings in their ability to effectively control and prevent these activities:

- The lack of experience on the part of judges, prosecutors, judicial police officers and financial experts in the investigation of these crimes,
- Although an improvement in the level of referrals is noted, the referral of suspicious activities on the Internet by those obliged to report remains low,
- The Albanian banks have little tradition, and as a result their personnel do not have the necessary professional level required for the detection and referral of suspicious activities in the area of money laundering through the Internet,
- The existence of an informal economy allowing for cash transactions and financial activities outside the banking system.

The Criminal Procedure Code includes provisions covering the following areas of relevance to the subject matter:

- Article 191/a - Obligation to produce data held on computer systems
- Article 208/a - Powers to order the seizure of computer data
- Article 299/a - Expedited preservation and maintenance of computer data including traffic data
- Article 299/b - Expedited preservation and partial disclosure of computer data
- Article 36 carries a range of provisions regarding confiscation of the proceeds of crime.
-

Financial investigations are the responsibility of the following bodies:

- The State Police (Directorate against Financial Crimes),
- Ministry of Finance (General Directorate for the Prevention of Money Laundering) (GDPML) – FIU (Unit for the Supervision of Gambling),
- General Prosecution Office,
- High Inspectorate for the Declaration of Assets,
- High State Audit,
- State Intelligence Service,
- General Directorate of Customs,
- General Tax Administration.

The following institutions are responsible for the search and seize of proceeds of crime on the Internet:

- Ministry of Finance (General Directorate for the Prevention of Money Laundering) (GDPML) – FIU (Unit for the Supervision of Gambling):

  - GDPML is the Albanian Financial Intelligence Unit. It is the central institution for collecting, verifying, evaluation, analysing and

disseminating information to law enforcement agencies on issues related to the prevention of money laundering and financing of terrorism.

- For the purpose of exercising its functions GDPML obtains information from the following legal entities: banks, exchange bureaus, insurance companies, notaries and lawyers, licensed accountants, real estate agencies, gambling games and casinos, non-banking institutions, construction companies, car trading companies, travel agencies, dealers in precious metals and stones, real estate evaluators, etc
- Cooperation with the banking system is carried out by means of communication with the Bank of Albania as Supervising Authority, and the Association of Albanian Banks as well through direct contacts with compliance officers in these institutions.
- GDPML cooperates with other institutions like the National Chamber of Notaries, The Institute of Licensed Accountants, the Albanian Association of Constructors, and the Association of Real Estate Evaluators.
- GDPML provides information to the supervisory bodies on these subjects on a regular basis regarding the findings of inspections, the applied administrative measures and the training needs.

▪ The State Police (Sector against Money Laundering):

- The unit is responsible for the fight against money laundering at the central level; whereas in the District Police Directorates, the responsible bodies are the Sections against Money Laundering, as part of the Sectors against Financial Crime.
- These structures receive information from the FIU (GDPML) about bank accounts and transactions, persons suspected of involvement in organised crime; they initiate the preliminary investigations.
- These structures organise the tracing activity of the police in order to discover and investigate money laundering offences. Information may be obtained from intelligence services, Interpol, and Europol referrals.
- They cooperate with other institutions, such as tax administration and tax investigation bodies. The State Police cooperates with the prosecution service and carries out investigations under its guidance. This happens not only in the cases delegated to it by the prosecution service, but also in the cases investigated upon its own initiative. Joint Investigative Units are another example of this cooperation.

▪ The State Police (Sector against Computer Crimes):

- The Sector against Computer Crimes is responsible for the prevention, discovery and investigation of computer-related crimes which include computer forgery, computer-related fraud, phishing, use of cloned credit cards, hacking and cracking, crimes related to electronic trading, electronic procurement, child pornography on the Internet, illegal interception of computer data, card skimming and any other crime that can be committed through the Internet, on the territory of the Republic of Albania.

Cooperation between the State Police and the Unit for the Supervision of Gambling is established for the identification and discovery of illegal gambling organised through the Internet, which is an activity that involves crime (tax evasion). There is also cooperation with the FIU in relation to suspicious transactions performed on the Internet.

Those involved in combating the illegal activity include the Electronic and Postal Communications Authority (the main authority monitoring implementation of the law on electronic communications in the country), non-governmental bodies representing ISPs and the National Agency for Society and Information. No examples of public-private cooperation were provided.

#### 4.2.1.2 Recommendations

At the Workshop, the participants have formulated the following recommendations for action to increase efficiency of tracing, seizing and confiscating criminal proceeds on the Internet:

- Legislative reform
  - To supplement the Criminal Code of Albania with a new article on identity and data theft.
  - To review MLA provisions so as to speed up these procedures (currently plagued by delays).
- Trainings
  - Based on memoranda of understanding several joint investigation units (JIUs) were established in several regions of Albania. Their work includes, among other, the investigation and identification of cybercriminals.
  - Presently there is a need for further targeted training on cybercrime. Better skills are required in detecting websites or cybercriminals. Training is needed for all parties involved in the process of detecting and investigating cybercrime.
- Identification and exchange of information
  - Rules should be strengthened concerning the exchange of information with ISPs: these must be obliged to use filters and equipment to detect and identify all sorts of IPs being used. They should have functional blacklists and exchange them with each other and with state investigation bodies.
  - Companies providing services through the Internet should have safer systems and websites, the so-called seal, indicating to the client/user that he/she is entering the real (legitimate) website.
- Public awareness and cybercrime
  - There should be a national strategy for raising the public awareness regarding the risks of misuse of private data. Since more and more people use the Internet for procuring different services, they should be more aware of the everyday risk of their personal data being stolen and possible misuse of their e-mail addresses.
  - A website for reporting cybercrime and submitting any other information concerning it should be established and made functional.
- Legal obligations for private entitites
  - Companies should report spam, phishing and any other similar activities targeting them to the competent authorities; this should be formulated

as a legal obligation to be followed by investigation from law enforcement bodies.

- Infected and illegal websites should be detected and closed.

- Strengthening technical infrastructure

  - The infrastructure for intercepting and bugging all communication through computer systems according to all legal obligations should be improved.
  - At present the infrastructure allows for interception of phone calls: this is being done by a centre attached to the General Prosecution Office and by ISPs.

## 4.2.2 Bosnia and Herzegovina

### 4.2.2.1 Current situation - summary

At the **State level** of Bosnia and Herzegovina (BiH), the State Investigation and Protection Agency (SIPA) is the institution responsible for financial investigations, within which the Financial and Intelligence Department is responsible for investigation of money laundering and financing terrorist activities operates. At the level of the Federation of BiH (FBiH), these activities fall within the scope of work of the Federation Police Administration – the Economic Crime, Corruption, Money Laundering and Computer Crime Department, the cantonal Ministries of Interior, the Federation Financial Police, the Tax Administration of FBiH.

At SIPA, within its Financial and Intelligence Department, there is a Task Force of the Institutions of BiH to prevent money laundering and financing terrorist activities, composed of representatives of the Ministry of Security of BiH, the Ministry of Justice of BiH, the Prosecutor's Office of BiH, the Intelligence and Security Agency of BiH, the Central Bank of BiH, the Ministry of Interior of the FBiH and Republika Srpska (RS), the Indirect Taxation Agency of BiH, the Agency for Security of BiH, the Tax Administrations of FBiH and RS and Brčko District, the Banking Agency of FBiH and RS, the Securities Commission of RS and FBiH. The aim of this Task Force is to improve the inter-agency approach to the issue of money laundering. When it comes to seizure and confiscation of proceeds from crimes committed by using of the Internet, they are regulated by the provisions of the Criminal Procedure Codes of FBiH and BiH, and are carried out in the same way as for other crimes.

In the **Federation of Bosnia and Herzegovina** the primary types of fraud and other offences using the Internet identified by the Federation are criminal offences of computer fraud related to unlawful use of credit cards and other non-cash payment cards for purchasing various goods on the Internet; the use of those cards for child pornography, for online betting etc.

Legal provisions covering the tracing, search, seizure and confiscation of proceeds of crime on the Internet are regulated by the Criminal Procedure Code of the Federation of BiH, the Law on Prevention of Money Laundering and Financing Terrorist Activities in BiH. The law enforcement agencies in Bosnia and Herzegovina in collaboration with prosecutor's offices and courts are responsible for these activities.

The public and private organisations involved in the prevention and detection of criminal money flows on the Internet are the above mentioned law enforcement agencies as well as all legal and physical persons that the Law on Prevention of Money Laundering and Financing Terrorist Activities of BiH identifies as responsible for notifying the Financial Intelligence Department on any suspicious transaction. This includes banks, post offices, investment companies and pension funds, stock exchanges, stock exchange agencies, insurance and reinsurance companies, casinos, gambling facilities and other organisers of games of fortune and special lotteries, exchange offices, pawn shops, lawyers, accountants, privatisation agencies, travel agencies, real property agencies etc.

The following considerations are proposed by the Federation to improve the effectiveness of investigating this type of crime:

- International cooperation through 24/7 contact points should be improved to achieve a faster data exchange.
- Legal provisions should be adopted in BiH to require the ISPs to keep data on the Internet traffic for a period of at least 6 months.
- Investigators should be trained at relevant specialist training courses.

Republika Srpska does not have any statistics regarding criminal activity involving illegal money flows on the Internet, and considers inadequate cooperation with the banks to be the main problem.

The legal provisions available to trace criminal money flows and to search, seize and confiscate crime proceeds are covered by the Law on Seizure of Proceeds from Crime which was adopted in February 2010 and entered into force on 1 July, 2010. This Law regulates the terms, procedures and bodies responsible for detection, seizure and management of proceeds obtained by any criminal offence. Under the this Law, the Ministry of Interior i.e. the Financial Investigation Department which was established in the middle of 2010, is responsible for financial investigations, together with the competent Prosecutor's Offices. The Financial Investigation Department with support of the High Tech Crime Department of the Ministry of Interior are responsible for the following of criminal money flows, as well as search, seizure and confiscation of proceeds from this type of crime. As appropriate, the Economic Crime Department and Public Security Centres (regional organisational units of the Ministry) can also become involved, depending on the requirements of the prosecutor who initiates and conducts an investigation.

No examples are given of interagency cooperation or the identification of bodies that are involved in the prevention or detection of this type of criminal activity. No examples of public-private cooperation or identification of obstacles encountered are given.

The experience of Brčko District on this subject matter consists of two investigations: one involving a victim report of fraud related to a vehicle purchase through the Internet, and the other – a victim of an attempted fraud through the "Spanish lottery". No further information on the subject was provided.

#### 4.2.2.2 Recommendations

Workshop participants formulated the following recommendations for action to be undertaken by BiH in order to increase efficiency of tracing, seizing and confiscating criminal proceeds on the Internet.

- The Directorate for Coordination of Police Bodies should initiate activities related to cybercrime and cybercrime-related financial investigations: organise meetings with representatives of police agencies, the SIPA Financial Intelligence Department (FID), Ministries of Interior of RS and of FBiH, Police of Brčko District, prosecutors from the entity prosecution offices, Brčko District Prosecutor's Office, Prosecutor's Office of BiH, representatives of the Banking Agency (both FBiH and RS) and the Communications Regulatory Agency (CRA) (all Internet providers are under its jurisdiction).
  The aim of these meeting should be to ensure a more efficient and active work on cybercrime cases as prescribed in the Criminal Codes of FBiH, RS, Brčko District and in the Copyright law (at the state level), i.e. the offences provided for in the Cybercrime Convention (the Budapest Convention), and more efficient financial investigations and confiscation of financial benefits obtained in connection with the commission thereof, pursuant to the Council of Europe's Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (the Warsaw Convention). The objective of these meetings would be to coordinate effectively all activities in cybercrime cases and financial investigations on the territory of Bosnia and Herzegovina, wherever necessary, as well as in cases with an international element.

- It is also necessary to strengthen specialised and professional training of police officers and prosecutors dealing with high-tech crime.

- It is necessary to establish an independent agency outside the police structure to replace the Financial Intelligence Department (FID) within SIPA, in accordance with the practice of neighbouring countries and the European practice, which would help achieve a better flow of information. The present is such that Financial Intelligence Department (FID) is collecting information from private sector and directing it to police agencies and prosecutor's offices, subsequently ensuring more efficient and more independent work of FID as well as more efficient control of the financial markets and faster information flow required by the police agencies and prosecutors.

- It is also necessary to speed up the adoption of appropriate legislation regarding the confiscation of proceeds of crime to ensure harmonization of legislation in this area on the entire territory of BiH.

- The Communications Regulatory Agency (CRA) should be encouraged to speed up activities on amending the laws governing the operation of Internet service providers (ISPs), as well as to strengthen control over ISPs in order to ensure data retention by ISPs for a fixed period of time (e.g. 6 months). Technical conditions within ISPs should be improved in order to accelerate the flow of information from the ISPs to police agencies and prosecutors when required.

- In addition, activities aimed at detecting and prosecuting cybercrime should take place simultaneously with financial investigations and involve all relevant agencies and private sector (banks, ISPs) to ensure more efficient prosecution of criminal offenses related to high-tech crime.

- The Draft Law on confiscation of illegally acquired assets and on the establishment of an agency managing such assets has been prepared; it is expected that the new Parliament will work on the adoption of this law in 2011.

It is necessary to note as additional information that in accordance with the FATF Recommendations and MONEYVAL Action Plan who seek greater independence for FID, especially in terms of voluntarily submitting information to BiH agencies dealing with the problem of money laundering and terrorist financing, the Working Group of Institutions of BiH prepared a New Draft Law on the prevention of money laundering and financing of terrorist activities and submitted it for adoption.

This Draft Law provides for the establishment of a Financial Intelligence Unit (FIU) under the Ministry of Security of BiH, which would not have police investigators in its staff but would employ civil servants who would collect, analyse and forward information, documentation and analysis to the relevant law enforcement agencies in Bosnia and Herzegovina dealing with issues of money laundering and terrorism financing. In its work the FIU would use information from all taxpayers in accordance with the provisions of Article 4 of the Law on Prevention of Money Laundering and Financing Terrorist Activities currently in force.

## 4.2.3 Croatia

### 4.2.3.1 Current situation - summary

During 2009 and 2010, the main types of fraud encountered on the Internet were frauds committed by inviting citizens to invest financial resources in various funds on the FOREX market; with false promises of high profits from such investments within short periods of time. In relation to this, in 2010 14 persons were brought to the Investigation Centre of the Zagreb County Court on the grounds of reasonable suspicion of committing several criminal offences pursuant to Article 224, Para 4 of the Criminal Code, the criminal offence of money laundering pursuant to Article 279 of the Criminal Code and for associating with others for the purpose of committing criminal offences pursuant to Article 333 of the Criminal Code. The offences resulted in loss of property caused to a high number of victims and the acquisition of illegal gains by the offenders amounting to millions.

No systematic control of criminal money flow on the Internet is possible; the control of financial transactions falls primarily within the competence of the Financial Inspectorate, Tax Administration and the Office for Money Laundering Prevention.

The Criminal Procedure Act covers the pursuit search, seizure and confiscation of crime proceeds from crime on the Internet. The surveillance and suspension of financial transactions requires the warrant of the County Court; however, the temporary surveillance and suspension of financial transactions can be implemented in line with the Money Laundering and Terrorist Financing Prevention Act, in the case of criminal offences of money laundering and terrorist financing. In such cases the Office for Money Laundering Prevention is authorized to issue an oral or written warrant to the party liable (bank, financial institution etc.) for temporary suspension of transactions during the period which may not exceed 72 hours, or a longer period upon the issue of warrant by a competent court.

In the Republic of Croatia financial investigations are carried out by the National Police Office for Suppression of Corruption and Organised Crime in coordination with the State Attorney's Office; however a warrant for financial investigation in the case of a suspected criminal offence may be issued by the State Attorney's Office to the various departments within the Ministry of Finance, namely to the Financial Inspectorate, Tax Administration, Customs Administration, Financial Police and Office for Money Laundering Prevention. Each of them within their competence have the capacity and the right to control the money flow of a particular natural or legal person, their revenues and expenditures, owned assets (real estate, securities, movable property etc.); the reports on results are submitted to the State Attorney's Office and the police. The above parties cooperate in all cases relating to the subject matter.

Other institutions involved in the prevention and control of criminal money flows include the Central Depository & Clearing Company which is a public company maintaining records of security owners, and the Croatian Agency for Supervision of Financial Services (HANFA) which is the supervisory body for security transactions.

Public-private cooperation in this area is mostly performed through official means: entities subject to the Money Laundering and Terrorist Financing Prevention Act (all natural and legal persons) are required to cooperate with the Office for Money Laundering Prevention by submitting a notification on suspicious transactions. Banks shall, as required by the court, submit confidential bank data in line with the Credit Institutions Act.

Areas for enhancing the capability for the prevention and detection of criminal money flows on the Internet are considered to include:

- Higher quality and more expedient exchange of data, which requires an enhanced cooperation between state agencies during financial investigations.

- Establishing a central register of open bank accounts which would include data on banks and numbers of accounts opened in the Republic of Croatia. This would accelerate the procedure for obtaining a warrant for the submission of data on account turnover for a particular person.

The obstacles to providing an effective response to this type of crime are identified as: the absence of EU-level legislation that would enable efficient collection of data on financial transactions abroad. This should include data on the ownership of companies, ownership of real estate, revenues and data collected on the property of criminal offenders. Provisions should be implemented to enable requests to be made by means of international legal assistance to freeze particular property of criminal offenders, where there is a suspicion that it has been acquired illegally.

#### 4.2.3.2 Recommendations

During the Workshop, the Croatian participants have formulated the following recommendations for action:

- To establish specialised units for cybercrime within larger police divisions and state attorney's offices.

- To establish a centralised body for closer cooperation between institutions responsible for detecting, reporting and processing cybercrime.

- To involve the academic community in the suppression of cybercrime (by commissioning specialised studies, using high-tech laboratories etc.)

- To provide for clear and exact rules regarding the procedure for reporting cybercrime and defining bank and business secrecy.

- To provide training for the judiciary on the use of electronic evidence.

- To strengthen public-private cooperation in raising awareness of the consequences of cybercrime.

## 4.2.4 Montenegro

### 4.2.4.1 Current situation - summary

The main types of fraud identified are identity theft, counterfeiting of credit cards and non-cash payment cards as well as phishing frauds. Lack of equipment and trained officers are identified as obstacles to dealing with this type of criminal activity. The Criminal Code and the Criminal Procedure Code define the criminal offences that are subject to financial investigation, and deal with the manner of conducting the investigations and seizure of property gained through criminal activity.

Financial investigations are the responsibility of the prosecution service and the police directorate acting under the orders of the prosecutor. The responsible organisation for tracing money flows including those on the Internet is the Administration for Prevention of Money Laundering and Financing Terrorism. This Administration has been established as an administrative body; its task is to follow the money flows and to inform the responsible state bodies of suspicious transactions. Montenegro has established neither a financial investigation unit, nor a high-tech crime unit in the Police Directorate or in the Prosecution Office. The activities for detecting criminal offences in this field are conducted by the Division for Fighting Organised Crime and Division for Preventing Commercial Crime in cooperation with the Special State Prosecutor.

Public and private sector organisations involved in the prevention and control of illegal money flows on the Internet include Customs Administration, Tax Administration, courts, commercial banks, insurance companies, the Bar and companies that organise games of chance. Examples of cooperation between organisations has been seen in cases where criminal money flows on the Internet were identified by a commercial bank and reported to the Police Directorate that undertook action in accordance with the Criminal Code. It is considered that the establishment of a National Criminal Intelligence Service would enable faster and easier exchange of operational data. This together with closer cooperation with Internet providers and sufficient training for staff would improve the capability to prevent and control illegal money flows on the Internet.

### 4.2.4.2 Recommendations

Having harmonised its Criminal Code with the Budapest Convention, Montenegro created the legislative oreconditions for fighting cyber-crime.

- Information on international best practices and guidelines, including those formulated by international organisations in the field, would need to be put at the disposal of the judicial and prosecution bodies to help them in processing cases where digital forensics are involved.

- A special division for fighting cybercrime was established within the National Police. There is also a Forensics Centre. However, the authorities involved in the fight against cybercrime do not have adequate professional human resources; they also lack special equipment for examining digital evidence.

- A computer emergency response team (CERT) should be established in Montenegro, composed of the representatives of the National Police, Prosecution Service, Ministry of Justice and Ministry for Information Society. This CERT will be in charge of responding to cybercrime cases as well as of preventive actions aimed at protecting computer systems of government institutions.

- Cybercrime often has an international dimension. Therefore legal experts, police, prosecution and courts need to exchange experience internationally in order to fight cybercrime and implement preventive measures efficiently. International and inter-agency cooperation between relevant bodies should be strengthened, and cooperation between public and private sectors improved, by signing agreements and by establishing joint teams.

## 4.2.5 Serbia

### 4.2.5.1 Current situation - summary

The types of fraud identified include computer fraud, Nigerian fraud, misuse of credit cards, fraud involving electronic banking and electronic transfers. No statistical information is available. The main obstacles to the prevention and control of criminal money flows on the Internet are the technical inability to identify cash flows, especially when anonymous services are used and where data is held in countries where international legal assistance is needed. It is recognised that the speed of the transactions is not matched by the speed of the legal procedures needed to trace the transactions.

In terms of the legal provisions available to trace criminal money flows and to search, seize and confiscate proceeds, the law on confiscation of property of criminal offenders has general provisions, and it is possible to conduct a financial investigation and confiscate assets regardless of how the crime was committed. If the offence was committed through the Internet, and it meets the requirements of these general provisions, a financial investigation will be conducted as well. These investigations will begin when the prosecutor gives an order for such investigation, and will be conducted by the financial investigation unit of the Ministry of Internal Affairs.

The institutions responsible for the subject matter are as follows:

- Ministry of Finance – Administration for the Prevention of Money Laundering.
- Ministry of Internal Affairs – Financial investigations conducted by the Financial Investigation Unit (FIU)
- Ministry of Justice – prosecution, court proceedings and seized property management.

These Ministries are institutionally responsible for monitoring the proceeds of criminal activity and for the detection, seizure and confiscation of the assets acquired through crime, regardless of whether the crime is in the field of cybercrime or not. The following specific activities are conducted:

- The Administration for the Prevention of Money Laundering collects and analyses data on suspicious transactions.
- The Financial Investigation Unit conducts investigations to identify and locate assets obtained through criminal activities.
- The Department for Organised Financial Crime leads pre-trial proceedings in order to identify the offenders of the crimes in the field of cybercrime, as well as other crimes that are carried out using computers and computer networks.

A practical example of cooperation in the subject area is a case of illegal betting on the Internet. Cooperation between the Department for Combating Cybercrime, the Administration for the Prevention of Money Laundering and management of betting under the Ministry of Finance and the special department for cybercrime of the High Prosecutor's Office in Belgrade, where it was discovered that a group of offenders were responsible for this criminal act. The offenders were identified and arrested. Property acquired by the criminal network was identified and subjected to a financial investigation. The property was suspended until the outcome of the criminal trial. This was an example of a successful collaboration between departments.

Serbia suggests that efficiency in this type of activity would be increased by the connection of databases of public and private sector in a single system.

#### 4.2.5.2 Recommendations

At the Workshop, participants formulated the following recommendations for action:

- To ensure a faster and easier exchange of data within the country by establishing an electronic network of the vital services in the fight against crime, with control of the right of access to databases.

- To cooperate more closely with ISPs – by signing memoranda of understanding with them.

- To strengthen training provided to all relevant public authorities (the police, the prosecution, the judiciary, the Administration for the Prevention of Money Laundering, the Financial Investigation Unit...), as well as to the financial sector, in relation to high-tech crime and money laundering; to provide basic and advanced levels of such training.

- To adopt more detailed regulations with regard to requests made by public authorities in connection with the investigation of high-tech crime (for example, in respect of data retention).

- To enhance the capacities of public authorities to effectively collect traffic and content data on communications which suggest cyber-laundering activities.

- To formulate at the international level proposals for regulating and speeding up the exchange of information between different states with the aim of suppressing illegal money flows.

- Establishing links between private and public sectors in the area of suppressing and preventing crime by way of joint training in conducting procedures.

## 4.2.6 "The former Yugoslav Republic of Macedonia"

### 4.2.6.1 Current situation - summary

The main types of fraud and crimes generating proceeds in "the former Yugoslav Republic of Macedonia" are: credit card abuse and Internet fraud (Nigerian fraud, buying expensive wares at low prices, fictitious introduction for fraud, fictitious lottery – spam messages). The experience of dealing with this type of crime is limited, and the lack of public awareness is considered to be a key issue.

The national authorities have implemented the all-crime approach regarding predicate offences for money laundering. Proceeds from crime committed on the Internet/through computer systems are considered to be objects of money laundering. All measures are prescribed in the Law on the Prevention of Money Laundering, Other Proceeds of Crime and Terrorist Financing (AML/CFT Law).

The Office for Money Laundering Prevention and Financing of Terrorism (OPMLFT) within the Ministry of Finance acts as FIU; it is competent to collect, process, analyse, keep and disseminate data to the competent authorities. OPMLFT conducts (financial) analysis when there is suspicion or there are grounds for suspicion that money laundering or terrorist financing has been committed or attempted. Following analysis, the OPMLFT prepares and submits a report to the competent state authorities (Ministry of Interior, Financial Police or Public Prosecutor Office). In cases where there is suspicion of other criminal acts besides money laundering and terrorist financing, the OPMLFT prepares and submits a written notification to the aforementioned state bodies.

OPMLFT has no experience of interagency cooperation in the prevention and control of fraud and proceeds-generating crime, nor in identifying criminal money flows of proceeds from crime on the Internet.

It is considered that all financial institutions obliged to undertake the AML/CFT measures should be involved in the prevention of criminal money flows on the Internet. For the purposes of AML/CFT prevention these obliged entities regularly cooperate with the OPMLFT.

In June 2009 the AML and Compliance Commission was established within the framework of the Banking Association within the Economic Chamber. Representatives of several banks sit on this Commission. Its tasks include:

- establishment of an efficient system for the application of regulations regarding banking operations,
- permanent monitoring of the application of regulations and supervisory standards,
- improving the functioning of banks and savings banks and cooperation with the institutions working in the area of harmonisation and prevention of money laundering and terrorist financing.

Representatives of the Commission meet with representatives of the OPMLFT on a regular basis (every month) to ensure a uniform and more efficient implementation of the AML/CFT measures.

#### 4.2.6.2 Recommendations

At the Workshop, participants from "the former Yugoslav Republic of Macedonia" put forward the following recommendations for action:

- To improve cooperation with the private sector and involve it in investigations at the stage of identification and location of suspicious transactions.
- To establish a legal basis for the obligation to submit reports and information concerning any kind of abuse and cybercrime.
- To strengthen the capacity of national institutions in identifying, detecting and suppressing criminal money flows on the Internet.
- To explore the ways of more efficient cooperation with international service providers (Yahoo, Google, Skype etc).
- To improve and develop the existing communication and cooperation between the relevant institutions at the international level.
- To undertake measures and activities in order to improve the security of data on the Internet and to raise the awareness of Internet users of the opportunities for a secure use of Internet services.

## 4.2.7 Turkey

### 4.2.7.1 Current situation - summary

The main types of crimes involving the Internet and crime proceeds are: payment and credit card fraud, Internet banking fraud and frauds committed by using advertisements. The main challenges to prevent and identify criminal money flows on the Internet are seen as: the tracing of the proceeds, especially if broken down in to small quantities. Cooperation from banks is seen as necessary for combating this type of activity.

The Banking Law of Turkey requires banks to report suspicious financial transactions to the Financial Crimes Investigation Board/Ministry of Finance (MASAK) – the FIU. Investigation of the details would then be conducted.

The general rules for investigation of crimes apply to financial investigations; therefore prosecutors are in charge of investigations, supported by law enforcement. If a suspicious transaction is identified during an investigation, MASAK will be requested to collect and analyse data relevant to the transaction and provide a report to the prosecution service.

No examples of interagency cooperation were provided; however, it is believed that the following organisations should be involved in investigations involving criminal money flows on the Internet: banks, ISP's, the Interbank Card Centre (BKM), the Credit Bureau of Turkey (KKM), the Ministry of Finance and MASAK. No examples of public-private cooperation were provided. No obstacles or recommendations for improved results were identified.

### 4.2.7.2 Recommendations

At the Workshop, participants formulated the following recommendations:

- To establish an Asset Recovery Centre under the Chief Prosecutor's Office.
- To add an Internet portal for cybercrime reporting by citizens, legal professionals and business to the Judicial Information System (UYAP).
- To link IT systems of the relevant bodies (high-tech crime units, law enforcement, FIU, ISPs) to accelerate communications.
- To step up cooperation and communication between the stakeholders in the fight against cybercrime such as ISPs, the Banking Regulation and Supervision Agency, MASAK, the Bank Association of Turkey and GSM operators by creating an interagency taskforce under the Prime Ministry.
- To prepare amendments for increasing cooperation and exchange of data between law enforcement and MASAK under the supervision of the prosecution.
- To establish a [collective] 24/7 Point of Contact consisting of representatives of the prosecution, law enforcement, ISPs and the Interbank Card Centre (BKM).
- To revise the relevant legislation in order to enhance the information flow between ISPs and MASAK.
- To establish a Cyber Consultative Forum including: ISPs, law enforcement bodies, MASAK, representatives of the banking sector, experts on cybercrime from private companies and universities, NGOs, IT professionals.

- To establish a public relations unit in order to raise the awareness of citizens with respect to cybercrime.

## 4.3 Situation in the project countries/areas of the CyberCrime@EAP project

### 4.3.1 Armenia

#### 4.3.1.1 Current situation - summary

The following offences are identified as the main types of fraud and other offences on the Internet that involve crime proceeds:

- Embezzlement of bank cards details;
- Embezzlement of funds from accounts linked to these cards;
- Use of e-purses to cash money;
- Internet fraud, in particular, sexual services, sale of various goods and services, etc.

Low supervision, low levels of awareness and identification of users are considered the main problems that are encountered by those with responsibility for the prevention and control of criminal money flows on the Internet. In order to enhance the level of public awareness the General Prosecutors' Office with support of the Presidential Administration started to prepare and broadcast commercials. Information was published on the website of the General Prosecutors' Office.

The cooperation with commercial banks and e-payment systems are good since this sector has interest to cooperate with law enforcement authorities.

Financial investigations are the responsibility of the Police of Armenia, State Security Service of Armenia, State Proceeds Committee of Armenia, and General Prosecutor's Office of Armenia. These authorities are responsible for asset seizure and confiscation of proceeds of crimes committed on the Internet.

#### 4.3.1.2 Recommendations

- In order to increase effectiveness of the fight against financial crimes committed on Internet and the cooperation between agencies and private sector to examine advanced practice of foreign countries and organize seminars for law enforcement agencies in the country;

- Organise public awareness campaigns to increase knowledge of society and private sector about new types of financial crimes and strengthen cooperation between them and LEA;

- Take appropriate measures to increase international cooperation with countries, which are not cooperating, in particular offshore countries

- Prepare amendments on current legislation in order to enhance cooperation between LEAs and ISPs

## 4.3.2 Azerbaijan

### 4.3.2.1 Current situation - summary

Different types of fraud ("419" fraud, credit card fraud, advance fee payment fraud) are frequent although money laundering through online gambling, e-payment services, e-gold are also identified as main methods for committing money laundering.

The following shortcomings are identified in their ability to effectively control and prevent these activities:

- insufficient staff;
- lack of trainings/training materials for law enforcement as well as contact points for public-private cooperation in ministries and financial service providers and ISPs;
- lack of inter-agency cooperation and written procedures to regulate information exchange;
- public – private cooperation:
  - opening commercial sites on the Internet is not clearly regulated;
  - no written procedures are available on information sharing and exchange;
  - unified databases maintained by stakeholders are not available;
  - awareness raising needs further improvement;

- proof of burden is on the LEAs;
- complexity of criminal money flows schemes;
- reporting networks are not or not well established and need further development;
- unified procedure for international cooperation is not available.

### 4.3.2.2 Recommendations

- To organise trainings for law enforcement authorities, public prosecutors and judges in order to ensure specialisation, overt and covert search and investigatory structures;

- To develop programs of joint training of employees of law enforcement bodies and representatives of a private sector;

- To organise direct physical access for law enforcement authorities to databases of financial service providers ensuring that privacy rights are not infringed;

- To develop national system of monitoring of suspicious transactions;

- To develop special software for the above mentioned purpose taking into consideration the safeguards and conditions. The development of the software should be prepared with the consent of all stakeholders;

- To unify national legislations in the field of AML/CFT with regard to the requirements of the international standards and procedures. It will create conditions for effective international cooperation in issues of rendering of mutual legal assistance;

- To use the already operating network of 24/7 contact points of the Budapest Convention of the Council of Europe or G8 High Tech Crime Subgroup;

- To create a permanent multi-agency working group including both public and private sector to enhance the efficiency in drafting amendments to improve national legislation

- To establish a national coordination board or working group to improve inter-agency cooperation

- To create the general database on crimes, criminals, methods and money-laundering schemes, black lists of accounts of physical persons and legal entities and other information for optimisation of work of participants of financial monitoring, the account, conducting statistics, research of tendencies

- Establishment of a trusted forum for LEAs and also a public forum for users, clients in order to raise awareness

- Develop government programmes for awareness raising, including opening hotlines (both in public and private institutions)

- Establish National Cybercrime Centre, which will assist not only on investigations of hi-tech crimes but criminal money flows on the Internet and would also serve as an analytical, research and methodological institution

## 4.3.3 Belarus

### 4.3.3.1 Current situation - summary

The following are the main types of fraud and other offences on the Internet that involve crime proceeds:

- Embezzlement through the use of computer devices (including use of bank card details and forged cards).
- Advertising and distribution of child pornography.

Major issues identified are: the on-line nature of the crimes, no borders for criminals; borders and serious limitations related to bank secrecy for LEA; multi-turn schemes to transfer money through shell companies in off-shores, where the information virtually cannot be received; bank accounts in the name of front persons or non-existent persons; bank employees being either negligent or directly involved in criminal arrangements.

If a financial investigation is connected to a crime under investigation at "K" Department, then it investigates such financial crimes. If it is considered that the financial investigation is a separate law enforcement activity, the investigation authority in charge thereof in Belarus is the Financial Investigation Department of the State Controlling Committee of Belarus.

Where necessary, resources of the economic crime unit, organized crime and corruption unit of the Ministry of Interior can be used as well as resources of the Financial Investigation Department and Financial Monitoring Department of the State Controlling Committee of Belarus.

Competencies of the state authorities of Belarus as to investigation of crimes are described in Article 182 of the Criminal Procedural Code of Belarus[45].

### 4.3.3.2 Recommendations

- Consider creation of an online platform for complaints from users on small-scale fraudulent transactions and analysing such information;
- Enhance interagency cooperation between specialized anti-cybercrime bodies and the Department for Financial Monitoring of the Republic of Belarus;
- Continue the implementation of the FATF Recommendations in the national legislation;
- Further promote and expand private-public partnership initiatives, using, inter alia, the positive experience of interaction between the law enforcement and the VISA Regional Office. Such PPP initiatives should cover both national (cooperation between the National Bank and commercial banks) and international (electronic payments systems) levels;
- Learn best practices from Georgian experience of electronic processing of criminal cases on cybercrimes;
- Continue work on accession of the Republic of Belarus to international legal instruments on countering cybercrimes, in particular the Budapest Convention.

[45] http://www.pravo.by/WEBNPA/text.asp?RN=hk9900295#&Article=182

## 4.3.4 Georgia

### 4.3.4.1 Current situation - summary

The main types of fraud involving crime proceeds are credit card fraud, phishing; in addition, there are cases of legalisation of illegal income involving Internet.

The main obstacles for prevention are the lack of awareness, as well as insufficient training of professionals. In terms of control of criminal money flows on the Internet difficulty of identification of depositors (offender) and finding the true origin of money involved. For instance, a crime may involve opening an account as a fictitious person and then transferring particular sums of money to or from this account. In some cases it is complicated to provide adequate evidence of depositor's identity for the court.

The Investigation Service of the Ministry of Finance of Georgia was established in 2009 by Law on Investigative Service of the Ministry of Finance. It constitutes a special investigative body, which according to the legislation of Georgia is responsible for prevention, suppression and investigation of crimes committed within financial and economic spheres. According to the Article 8 of the Law, the investigative service is entitled to conduct investigative-operative activities, carry out investigations, obtain necessary information and carry out other activities provided by the legislation of Georgia.

The Financial Monitoring Service of Georgia is an administrative type of FIU. Its activity is regulated under the Law of Georgia on Facilitation the Prevention of Illicit Income Legalization (adopted on June 6, 2003) and the Regulation of Financial Monitoring Service of Georgia – Legal Entity of Public Law (approved under the Ordinance 859 of the President of Georgia on November 26, 2009).

### 4.3.4.2 Recommendations

- Improve international cooperation;
- Establish an inter-agency task force to improve cooperation among relevant government agencies.

## 4.3.5 The Republic of Moldova

### 4.3.5.1 Current situation - summary

The main problems encountered in the prevention and control of criminal money flows on the Internet, are the use of servers located outside the Republic of Republic of Moldova and the lack of cooperation with the financial institutions in the field. The institute responsible for financial investigations is the Centre for Combating Economic Crime and Corruption.

Further improvement is required in the field of inter-agency cooperation in order to effectively follow criminal money and to search, seize and confiscate proceeds from crime on the internet / on computer systems.

There are legislative problems with regard to obtain data from telecommunication companies, namely there has to be an open investigation to ensure information exchange. In the course of the preparation of the cybercrime legislation the private sector (including ISPs, TSPS, financial institutions) were invited to discuss the draft legislation. Cooperation is not only initiated by LEAs but also by the private sector.

### 4.3.5.2 Recommendations

- Amend CPC and AML legislation in order to:
  - launch investigations without the burden to prove the predicate offence;
  - the offender is under the burden of proof regarding proceedings;
  - simplify the procedure to seize, confiscate property originating from criminal proceeds;
- Expand the reporting list of the AML legislation to include obligatory reporting of (suspicious transactions, offences) ISPs, TSPs;
- Finalise and adopt the law on electronic payment services and electronic money;
- Awareness raising among the private sector on IT tools, methods, trends of criminal money flows on the Internet;
- Establishment the National Cybercrime Investigation Centre**.**

## 4.3.6 Ukraine

### 4.3.6.1 Current situation - summary

The following crime types have been identified: GSM network fraud, Internet-auction fraud, payment card fraud and the use of compromised bank account details or accounts in electronic payment systems. Social networks and social engineering are used often as well.

One of the most frequent fraud activities in the Ukrainian segment of the Internet is international financial fraud, (financial pyramids). Many commercial entities pretend to provide financial services (trust management of financial assets) or to carry out investment activities through web resources and e-payment systems; they offer people the opportunity to give their money to these companies, purportedly, in order to invest it in business projects with unrealistic (economically unfeasible) interest rates; usually accounts of such companies are held off-shore. The major problem is to overcome the anonymity of such companies on the web, i.e. to establish the link between these web resources and individual companies and thus to prove the fact of rendering a service that should be licensed under the law of Ukraine.

The problem in prevention and control over criminal money flows in the Internet is that e-payment system operation (in Ukraine) is not regulated, thus making it harder to trace monies of Ukrainian citizens deposited and withdrawn from fraudsters' accounts, as well as to control their further movements between accounts of companies participating in a criminal arrangement. Control and registration of money flows to off-shore jurisdictions and back into Ukraine (legalization) is yet at a low level due to the lack of an efficient mechanism of cooperation with international AML bodies and insufficient laws of Ukraine (which do not reflect the today's pace of IT development).

### 4.3.6.2 Recommendations

- Implement the revised FATF Recommendations;
- Send questionnaire to the participants of the seminar on problems hindering search, seizure and confiscation of digital assets;
- Strengthen international cooper.ation in search, seizure and confiscation of proceeds of cybercrime;
- Create a website which would raise public awareness in cybercrime issues and would work as an Internet Crime Complaint Centre.

## 4.4 Follow up

- States to fill gaps in the legal framework aimed at preventing criminal money flows on the Internet.

- The project is to support and follow up on the recommendations made in the event with special regard to:

  - awareness raising programmes;
  - establishment of trusted fora;
  - development of e-crime reporting networks, hotlines;
  - support training needs of the project countries;
  - discuss LEA-ISP cooperation in regional seminars.

- Provide EAP countries with an Electronic Evidence Guide (to be developed under CyberCrime@IPA).

# 5 Appendices

## 5.1 Agenda

| **Monday, 27 February 2012** | |
|---|---|
| 8h30 | Registration of participants |
| **Plenary sessions** | |
| 9h00 | Session 1: Opening<br><br>• Oleksiy Feshchenko - First Deputy Head of the FIU of Ukraine<br>• Vladimir Ristovski - Representative of the Secretary General of the Council of Europe<br>• Alexander Seger - Council of Europe Secretariat |
| 9h30<br><br>*11h15-11h30*<br>*Coffee break* | Session 2: Cybercrime and crime proceeds on the Internet<br><br>▪ MONEYVAL/Global Project on Cybercrime Typology study (Council of Europe) (*Alexander Seger 25 minutes)*<br><br>▪ FATF typology studies *(Timothy Goodrick FATF Secretariat 25 minutes)*<br><br>▪ Case studies<br>– Belgium (*Frederic Van Leeuw 20 minutes)*<br>– Ukraine (*Radzhamy Dzhan 20 minutes)* |
| 11h30 | Session 3: Criminal money on the Internet – the relevance of international standards<br><br>▪ FATF recommendations (as revised February 2012) *(Timothy Goodrick FATF Secretariat 40 minutes)*<br>▪ Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198) (*Oleksiy Feshchenko 20 minutes*)<br>▪ Budapest Convention on Cybercrime (CETS 185) (*Alexander Seger 20 minutes)* |
| *13h00 – 14h30* | *Lunch break* |
| 14h30<br><br><br>*16h15-16h30*<br>*Coffee break* | Session 4: Countermeasures<br>▪ Short description of the range of countermeasures<br>▪ FOCUS - Public-private information sharing and analysis<br>– Irish Bankers Forum (*David O'Reilly 15 minutes)*<br>– Paypal (*Bertrand Lathoud Head of Information Risk Management, 15 minutes)*<br>– VISA CEMEA *(Larissa Makarova – Country Risk Manager, CIS Ukraine 15 minutes)*<br>– GUAM (*Oleh Klynchenko Program Coordinator, Political and Legal Issues, Secretariat of the Organization for Democracy and Economic Development, GUAM)*<br>– Financial sector/law enforcement working group Albania (*Elton Kerluku 15 minutes)*<br>– Other examples |
| | ▪ Panel discussion: Financial investigations and asset-recovery from Internet-related crime: what options? |

| | |
|---|---|
| | Panellists: two members of Albanian, Serbian and Ukrainian delegation (FIU and Police) |
| *18h00* | *End of day 1* |
| **Tuesday, 28 February 2012** | |
| **Working group session**<br><br>▪ Group 1: Eastern Partnership countries *Moderator: Gergo Nemeth, Larissa Makarova, David O'Reilly*<br>▪ Group 2: CyberCrime@IPA countries/areas *Moderator: Alexander Seger, Frederic Van Leeuw, Bertrand Lathoud* | |
| 9h00<br><br>*11h00 – 11h15*<br>*Coffee break*<br><br><br><br><br>*13h00 – 14h30*<br>*Lunch break*<br><br><br><br>*16h00 – 16h15*<br>*Coffee break* | Session 5: Measures taken and recommendations for action in project areas<br><br>Working groups to go through the following steps:<br><br>▪ Problem analysis: defining the problem of criminal money flows on the Internet in each project area<br><br>▪ Stakeholder analysis: identifying public and private sector institutions (to be) involved in measures against criminal money flows and their roles<br><br>▪ Countermeasures: based on presentations on day 1, identifying measures underway (good practices) or to be undertaken in project areas<br><br>a) inter-agency cooperation<br>b) public –private cooperation<br><br>▪ Other measures: how to organise public-private information sharing and analysis |
| *17h30* | *End of day 2* |
| **Wednesday, 29 February 2012** | |
| 9h00<br><br>*10h30 – 11h00*<br>*Coffee break* | Session 6: Delegations of each project area to finalise recommendations |
| 11h00 | Session 7: Presentation of proposals by each delegation and conclusions |
| 12h30 | Session 8: Conclusions |
| **13h00** | **End of the meeting and lunch** |

## 5.2 List of participants (Kyiv, February 2012)

## 5.3 The revised FATF Recommendations

*AML/CFT Policies and Coordination*

1. Assessing risks and applying a risk-based approach: Countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.

2. National cooperation and coordination: Countries should ensure that policy makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policy making and operational levels, have effective mechanisms in place which enable them to cooperate and, where appropriate, coordinate domestically with each other.

*Money Laundering and Confiscation*

3. Money laundering offence: Countries should criminalise money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.

4. Confiscation and provisional measures: Countries should adopt measures to enable their competent authorities to freeze of seize and confiscate property, proceeds from or instrumentalities used in or intended for use in money laundering or predicate offences, property that is the proceeds of or used in the financing of terrorism, terrorist acts or terrorist organisations or property of corresponding value.

*Terrorist Financing and Financing of Proliferation*

5. Terrorist financing offence: Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

6. Targeted financial sanctions related to terrorism and terrorist financing: Countries should implement targeted financial sanction regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing.

7. Targeted financial sanctions related to proliferation: Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

8. Non-profit organisations: Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable and countries should ensure that they cannot be misused.

*Preventive Measures*

9. Financial institution secrecy laws: Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

10. Customer due diligence: Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. Financial institutions should be required to undertake customer due diligence measures.

11. Record keeping: Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities.

12. Politically exposed persons: Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic politically exposed person or a person who has been entrusted with a prominent function by an international organisation. In such cases, additional due diligence should be carried out.

13. Correspondent banking: Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships to perform additional due diligence.

14. Money or value transfer services: Countries should take measures to ensure that natural or legal persons that provide money or value transfer services are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

15. New technologies: Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products.

16. Wire transfers: Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

17. Reliance on third parties: Countries may permit financial institutions to rely on third parties to perform certain elements of customer due diligence, but ultimate responsibility for customer due diligence remains with the financial institution.

18. Internal controls and foreign branches and subsidiaries: Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements.

19. Higher-risk countries: Financial institutions should be required to apply enhanced due diligence measures to relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF.

20. Reporting of suspicious transactions: If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

21. Tipping-off and confidentiality: Financial institutions, their directors, officers and employees should be (a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative,

regulatory or administrative provision if they report their suspicions in good faith to the FIE and (b) prohibited by law from disclosing the fact that a suspicious transaction report or related information is being filed with the FIU.

22. DNFBPs46: Customer due diligence: The customer due diligence and record keeping requirements laid out in other recommendations apply to designated non-financial businesses and professions.

23. DNFBPs: Other measures: Subject to some qualifications, the requirements of recommendations 18 to 21 apply to all designated non-financial businesses and professions.

*Transparency and Beneficial Ownership of Legal Persons and Arrangements*

24. Transparency and beneficial ownership of legal persons: Countries should take measures to prevent the misuse of legal persons for money laundering or terrorist financing.

25. Transparency and beneficial ownership of legal arrangements: Countries should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing.

*Powers and Responsibilities of Competent Authorities and Other Institutional Measures*

26. Regulation and supervision of financial institutions: Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations.

27. Powers of supervisors: Supervisors should have adequate powers to supervise and monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections.

28. Regulation and supervision of DNFBPs: Designated non-financial businesses and professions should be subject to regulatory and supervisory measures.

29. Financial intelligence units: Countries should establish a financial intelligence unit that serves as a national centre for the receipt and analysis of suspicious transaction reports and other information relevant to money laundering, associated predicate offences and terrorist financing and for dissemination of the results of that analysis.

30. Responsibilities of law enforcement and investigative authorities: Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies.

31. Powers of law enforcement and investigative authorities: When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions.

32. Cash couriers: Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system.

[46] Designated non-financial Businesses and Professions.

33. Statistics: Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of the AML/CFT systems.

34. Guidance and feedback: The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

35. Sanctions: Countries should ensure that there are a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons who fail to comply with AML/CFT requirements.

*International Cooperation*

36. International instruments: Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1998; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.
37. Mutual legal assistance: Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions and related proceedings.

38. Mutual legal assistance: freezing and confiscation: Countries should ensure they have the authority to take expeditious action in response to requests from foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of corresponding value.

39. Extradition: Countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay.

40. Other forms of international cooperation: Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing.

## 5.4 Findings of the Typoligy study on Criminal money flows on the Internet

While cybercrime appears to be a widespread and growing threat generating large amounts of criminal proceeds, the survey responses and information available reveal that data on related money laundering and evidence of successful law enforcement action are weak. Cyber-laundering continues to represent a challenge for law enforcement agencies. These findings are aimed at assisting policy makers and regulators to identify issues which could be addressed through legislation, supervision and effective rules and guidance for implementation. They are also aimed at financial intelligence units and law enforcement agencies, to contribute to a more efficient analysis, detection and investigation of possible money laundering cases related to cybercrime. They are furthermore to encourage public-private cooperation and measures by the private sector.

### 5.4.1 Cybercrime and criminal money flows

Cybercrime can be conceptualised as comprising (a) offences against computer systems and data, and (b) offences by means of computer systems and data – including computer-related fraud – as defined in the Budapest Convention on Cybercrime.

The underlying tools and infrastructure of cybercrime encompass malware, botnets, the criminal misuse of domains, an underground economy providing criminal goods and services, and in particular money mules that form an essential part in the movement of crime proceeds and in money laundering on the Internet. Social networks and cloud computing services offer new platforms for cybercrime and pose new challenges for law enforcement. Complex fraud operations and this infrastructure show the features of structured organised crime groups.

It would seem that obtaining economic benefits is the primary purpose of cybercrime, and that large amounts of criminal money circulate on the Internet. Fraud is the most often reported category of cybercrime by far. It includes, in particular, fraud committed with stolen identities (using phishing and other social engineering techniques for the theft of information), payment card fraud, online banking attacks and account take-over, mass-marketing fraud, auction and other types of confidence fraud, investment fraud as well as pyramid and other multi-level marketing schemes. In addition to fraud, commercial child abuse materials, counterfeit pharmaceuticals, offences related to intellectual property rights, online dating schemes, illegal online gambling, extortion and other physical world crimes proliferate on the Internet and generate proceeds that are moved and laundered.

In can be expected that as societies rely even further on global communication technologies and networks, all forms of crime – in particular crime for profit – will be increasingly transnational and involve such technologies and electronic evidence in one way or the other, and so will criminal money flows and money laundering on the Internet. Societies (public and private sector institutions) need to prepare for this.

### 5.4.2 Money laundering and cybercrime issues

As regards cybercrime and money laundering, the key findings can be summarized as follows:

- The financial impact of cybercrime and the size of related proceeds (which are laundered or re-invested in developing new capabilities for further developing tools

and techniques for cybercrime purposes) are not quantifiable, in the absence of reliable data and research.

- Cases show that proceeds from cybercrime are laundered through sophisticated schemes, involving both traditional (wire transfers, cash withdrawals, money remitting services) and new payment methods (e-currency, Internet payment services).

- As Internet payment services inevitably use at least one element from the traditional financial system (cash, banks, credit cards…), cybercrime and cyber laundering also affect the traditional financial system. However, criminals have found ways to move value or monetize stolen goods without having to use the financial system.

- Internet money services providers, together with the "traditional" banking system are used both for cyber fraud and money laundering. Money remitting services or Internet payment services providers have been targets and/or victims of cyber-attacks, but also, their services have been used for money laundering purposes. Some Internet based payment methods are more vulnerable to money laundering than others.

- Cybercriminals prefer to transfer values between persons in different countries by bits and bytes of information rather than in the form of banknotes. Cash smuggling is reportedly rarely (next to never) used or might have remained undetected by existing controls. Money mules appear to be mostly used for "breaking the chain" rather than for cross-border movement of cash.

- Evidence reveals that unlike "traditional" criminal groups that are quite "stable" and have a well determined organisational chart, cyber criminal groups appear to be extremely flexible. Ad hoc criminal groups and networks or short term alliances are put together regardless of the location or profile of the perpetrators. The services provided by the underground economy reduce the need for sophisticated technical know-how of criminals.

- The awareness of risks related to new payment systems and services and of related money laundering appears to be at a relatively low level in the majority of countries having responded to the survey.

- The most targeted services and sectors by financially motivated cyber-attacks appear to be payment services and financial institutions, and these are likely to continue being the focus, considering the increasing reliance by businesses and individuals on online systems in daily life.

- It appears that there is a clear risk of un-detected or low report rate of cybercrime offences in most countries having responded to the survey, which could be due either to a lack of awareness or to reputational considerations, and this has a direct impact on the absence of related financial investigations/ money laundering investigations.

- Lack of relevant substantive provisions criminalising adequately cybercrime offences47 may result in excluding certain proceeds-generating types of cybercrime from qualifying as predicate offences for money laundering.

[47] For a common minimum standard of relevant offences which a State should criminalise, see the Council of Europe Convention on Cybercrime (CETS. 185) at http://conventions.coe.int

- Though AML/CFT policies constitute an important element of policy approaches to tackling criminal money flows, national anti-money laundering policies may be disconnected from anti-cybercrime policies, thus compartmentalising national efforts to prevent and combat cyber-laundering.

- Investigation and prosecution of crimes involving money laundering and cybercrime are likely to be complex and lengthy. Considering the large number of potential accessories to such crimes, the difficulties in collating a multitude of "small" cases to reveal large-scale criminal networks, challenges in obtaining electronic evidence cross-border and considering that many institutions/agencies may have jurisdiction, there are many deterrents to financial investigations. This may in some countries privilege investigations focusing on cybercrime only while neglecting financial and money laundering aspects. This may explain the limited number of investigations of crime involving money laundering and cybercrime in responding countries.

- Proper rules and regulations in the AML/CFT field with regards to Internet-based payment systems are not always in place. Targeted legal provisions requiring all Internet based payment services providers to implement AML/CFT procedures in terms of KYC, CDD and reporting obligations, will decrease the ML risks associated to this particular industry.

- Not only lack of relevant legislation, but also different approaches in different jurisdictions seem to enable criminals to misuse Internet-based payment methods for money laundering purposes.

- Different sources (FATF, FINCEN, MONEYVAL, countries' responses to the survey) refer to different electronic or Internet based payment systems and methods, using different terminology (e-payment, Internet based payment services, e-currency, new payment methods etc…). Apparently there is no common and general understanding of the terms used and sometimes referrals to market leaders or well known providers is being necessary in order to clarify the actual payment service in question.

- In the case of police authorities and public prosecutor's office, specialisation of officials is possible and in some jurisdictions even implemented, however this seems to be the exception rather then the rule. In case of FIU experts, sometimes targeted training programmes are compulsory with regards to cybercrimes and cyber-laundering, including the mechanisms governing the Internet payment services.

### 5.4.3 Conclusion and direction for development

In terms of countermeasures, the study documents good practices already available and taken by public and private sector institutions. These elements should inspire action by other countries and institutions to protect their citizens and financial infrastructure. The following areas are considered as having the potential to enhance global action and contribute to overall efforts to prevent and combat money laundering in this context:

*Adequate research and measures* to prevent or mitigate ML/TF and cybercrime risks. There is a clear need to undertaken research covering money laundering and cybercrime, with due consideration of the nature and scale, offenders and accessories used, their modus operandi, the infrastructures and services targeted, the emerging technologies and related vulnerabilities and emerging threats. Filling gaps through future research would also enable to target relevant policies and measures to prevent or mitigate ML/TF/cybercrime to the risks identified. It would also result in an increased awareness of competent institutions' and

private sector's representatives on the cybercrime tools, technologies, and operations in order to identify those that are likely to be primarily targeted by criminals for ML/TF activities, and as such would result in strengthening detection capabilities to support action against both cybercrimes and money laundering. Risk management in the private sector needs to be expanded to capture Internet-related risks.

*AML/CFT and anti-cybercrime strategies.* Integration into AML/CFT national strategies of elements targeting money laundering related to cybercrime and Internet-based payment systems has also been indicated as a possible direction for reflection and action, in particular for those countries particularly affected. Many cybersecurity strategies consider the financial sector to be part of the critical information infrastructure that is to be protected against cyber attacks. However, they do not necessarily cover the issue of criminal money. For this reason, it has been proposed to make financial investigations and measures against money laundering financial part of cybercrime strategies.[48]

Adoption and implementation of comprehensive substantive legislation in this area and of relevant *international standards*. Also important in this context is the necessity to update the national legal framework so as to cover adequately cybercrime, money laundering and procedural law measures to allow for the preservation, search and seizure of electronic evidence as well as international co-operation,; in line with the Budapest Convention on Cybercrime (CETS 185) and the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198). In this context, specific attention should also be devoted to the implementation of the FATF revised recommendations which have a direct relevance in this context, and notably those related to the assessment of risks, those related to new technologies, money or value transfer, wire transfers, etc.[49]

Establishment of clear mechanisms and incentives for *public reporting* on fraud and other proceeds generating offences on the Internet, or on cybercrime in general, while taking into consideration the necessity to observe privacy and liability rules. Such reporting mechanisms allow to determine not only overall trends and threats, but to analyse criminal operations and patterns of money flows and money laundering, and finally to initiate measures by criminal justice authorities and financial intelligence units to investigate and ultimately prosecute such offences.

*Guidance and typologies*. Guidance for financial and non financial institutions which are subject under AML/CFT legislation to report when they suspect or have reasonable grounds to suspect that funds are proceeds of a criminal activity could include elements to clarify instances of cybercrimes which may give rise to a duty to report under national legislation (ie. advance fee fraud, computer hacking, cyber extortion, identity theft, sale of stolen or counterfeit goods via Internet, credit card fraud, cyber laundering, etc), specific guidance on risk indicators and recognition of suspicious behaviour, examples of cases, ML/TF techniques and typologies identified in the national jurisdiction, and any related information which may assist reporting institutions to comply with their AML/CFT obligations. Within a financial institution, techniques such as behaviour profiling, monitoring for mule account activity and "hotlists" of known or suspected accounts can help in the detection of criminal money flows.

*Setting up of specialised units* for cybercrime. In many countries, high-tech crime units and units for cyber-forensics, and in some specialised prosecution services have been created in

[48] See proposals made by the Council of Europe's Global Project on Cybercrime http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf

[49] See http://www.fatf-gafi.org.

recent years. The importance and workload of such units will increase significantly in the very near future and so will be their need for resources.

*Inter-agency cooperation*, notably through proactive parallel financial investigations when pursuing cybercrimes and associated money laundering. Cybercrime and criminal money flows touches upon the responsibility of a number of institutions. Interagency cooperation, in particular between authorities responsible for financial investigations, for high-tech crime and financial intelligence units, will be essential, particularly in the context of major proceeds generating offences. Financial intelligence units may have not only access to information and intelligence but also analysis capability that would bring an added value and usefully complement the information gaps in the context of investigations of ML associated with cybercrimes and criminal money flows. The capacity of the financial intelligence unit in this context, both in terms of sharing of information with other stakeholders or of co-operating may be subject to limitations, subject to the specificities of the domestic legislation, and should thus be reviewed, especially in jurisdictions particularly affected by these phenonema. In many jurisdictions, prosecutors may play a major role in coordinating different agencies in specific investigations.

Promoting *public-private cooperation and information exchange* on criminal money flows on the Internet. The study shows that this is probably the area where the biggest impact can be made. The creation of trusted fora for information and intelligence between the financial sector, criminal justice and anti-money laundering authorities should be given consideration

*Training* of criminal justice and anti-money laundering authorities in matters related to cybercrime and electronic evidence. Given the increasing relevance of cybercrime and electronic evidence for most types of crime, such training should be mainstreamed in law enforcement and judicial training curricula. The need for the training of judges is a key lesson already learned with regard to money laundering and the financing of terrorism. Specific training on criminal money flows for relevant stakeholders, including FIUs, should be organised in addition.