www.coe.int/moneyval
www.coe.int/cybercrime

Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction[1]

[1] Ref. MONEYVAL(2012)6, dated 9 March 2012, adopted by MONEYVAL at its 38th Plenary meeting (5-9 March 2012).

Table of contents

Executive Summary

1. This typology study is a successful outcome of a cooperative effort of MONEYVAL[2], the Council of Europe's Global Project on Cybercrime[3] as well as the joint project of the European Union and the Council of Europe against money laundering and the financing of terrorism in the Russian Federation (MOLI-RU 2). This report originates from a practitioners' desire to analyse the links between cybercrime and money laundering, the most frequently used methods and instruments for laundering criminal proceeds from cybercrime and through the Internet, as well as the risks and vulnerabilities posed by this type of money laundering.

2. This report differs slightly from other typologies reports previously elaborated by MONEYVAL, given that it was prepared using a wide-ranging source of data, gathered through a survey to which MONEYVAL, FATF and EAG member countries governmental experts as well as private sector institutions specialised in cybercrime matters. Hence, for the first time, it pooled resources and expertise from financial intelligence units, financial investigation services and high tech crime units and consulted key stakeholders from the private sector who contributed their experience to the project.

3. The report notes that though cybercrime appears to be widespread and generates large amounts of criminal proceeds, the data on related money laundering and evidence of successful law enforcement action is weak. In addition to contributing to raising awareness on current initiatives aimed at preventing and combating cybercrime and money laundering, as well as on proceeds generating offences on the Internet, the report considers the cyber-laundering risks and vulnerabilities and illustrates identified money laundering methods, techniques, mechanisms and instruments of criminal proceeds from cybercrime relying on a number of cases received from contributors, setting out typologies that were identified and specific indicators of potential money laundering activity within this context.

4. Unlike traditional money laundering schemes involving the use of the banking system, cyber-laundering involves sophisticated schemes and relies on various types of operations and financial services providers, ranging from bank transfers, cash withdrawals/deposits, the using of digital/ electronic currencies to money mules and money remittance providers. At the same time, the awareness of risks related to new payment systems and services and of related money laundering appears to be at a relatively low level. Hence, the detection and pursuit of the criminal money flows is much more challenging for law enforcement agencies. Furthermore, there is a clear risk of undetected or low report rate of cybercrime offences in most countries, which impacts on the absence of related financial investigations and money laundering investigations.

5. In its conclusion, the report sets out a number of findings as regards cybercrime and money laundering and of available countermeasures and good practices in some countries, which could inspire policy makers and regulators or become elements of more systematic future approaches and strategies that are aimed at the prevention of money laundering and the financing of terrorism, and at the search, seizure and confiscation of proceeds of crime on the Internet. A number of areas have been identified which are considered as having the potential to enhance global action and contribute to overall efforts to prevent and combat money laundering in this context.

[2] For further information, see www.coe.int/moneyval

[3] For further information, see www.coe.int/cybercrime

Abbreviations and Acronyms

ACH	Automated clearing house
AML/CFT	Anti-Money laundering and countering the financing of terrorism
APWG	Anti-Phishing Working Group
ATM	Automated teller machine
BKA	German Federal Criminal Police
BGP	Monitoring routing protocols
CERT	Computer Emergency Response Team
CDD	Customer due diligence
CNP	Card-not-present
CSIRT	Computer Security Incident Response Teams
DDOS	Distributed denial of services
ECCP	European Cybercrime Platform
ETS	European Treaty Series (since 1.01.2004, CETS – Council of Europe Treaty Series)
EU	European Union
FATF	Financial Action Task Force
FIU	Financial intelligence unit
FSRB	FATF style regional body
FT	Financing of terrorism
GAC	Governmental Advisory Committee
IC3	Internet crime complaint center
ICANN	Internet corporation for assigned names and numbers
ICT	Information and communications technologies
I-CROS	Internet Crime Reporting Online System
ID	Identification data
IPS	Internet payment services
ISP	Internet service providers
KYC	Know your customer
ML	Money laundering
MONEYVAL	Committee of Experts on the Evaluation of anti-money laundering measures and the financing of terrorism
PIN	Personal identification number
STR	Suspicious transaction report
SWIFT	Society for Worldwide Interbank Financial Telecommunication
T-CY	Council of Europe Cybercrime Convention Committee
VOIP	Voice over Internet protocol
USA	United States of America

1 INTRODUCTION

1.1 Objective of the study

1. Information and communication technologies (ICT) and in particular the Internet linking up computers worldwide offer unique opportunities to societies worldwide. The Internet allows an increasing number of people[1] and organisations to communicate, exchange information, to offer and make use of services, and to exercise their rights. At the same time, the reliance on ICT and the Internet makes societies vulnerable to threats such as cybercrime.

2. For the purposes of this study, cybercrime denotes:[2]

- offences against computer data and systems: this includes in particular the so-called "*c.i.a.-offences*" against the confidentiality, integrity and availability of data and systems;
- offences committed by means of computer data and systems: this includes offences such as fraud and child pornography or offences related to intellectual property rights that gain a different quality and impact if committed through computer systems.

3. The fact that any economic or serious crime may involve computer systems makes cybercrime a very broad and cross-cutting concept. In addition, cybercrime is highly transnational in nature. It is increasingly targeted at generating economic proceeds involving different types of fraud and economic and organised crime. While some are new types of crime, many are traditional types of crime that are now committed more effectively on the Internet. In addition, a digital underground economy is in place and growing, which involves organised crime, available IT experts, hackers, mules and other persons for hire, and is designed to provide the necessary tool and services to facilitate the commission of cybercrime or to ensure the disposal of crime proceeds. Organised crime groups do not necessarily need to develop their own expertise about the Internet, as such skills or services can be recruited to respond on a needs basis, creating a sort of transactional basis network connection between "small- time criminals" and organised crime, even located in different parts of the world. This suggests large amounts of criminal money flows on the Internet.

4. When money laundering is criminalised based on an all crimes approach, all proceeds-generating types of cybercrime would be considered as predicate offences for money laundering and the property that has been laundered taken out of or put into the "system" at any point considered as money laundering. Cybercrime is thus highly relevant for anti-money laundering and counter-terrorist financing efforts.

5. A wide range of stakeholders is involved in measures against such forms of crime not only from the public sector but in particular from the private sector. Although there are examples of multi-stakeholder action, efforts remain rather fragmented. Initiatives against fraud on the Internet are not necessarily linked to activities carried out by financial intelligence units or law enforcement authorities responsible for financial investigations.

[1] For Internet use statistics, see http://www.Internetworldstats.com/stats.htm. It is estimated that by March 2011, over 2 billion people used the Internet (representing a penetration rate of 30.2 % of the global population and a growth of 480.4% between 2000 and 2011).

[2] This "definition" is based on the Budapest Convention on Cybercrime (www.coe.int/cybercrime).

6. In short, on the one hand, much progress has been made since the late 1980s with regard to the creation of systems for the prevention and control of money laundering and more recently the financing of terrorism, and since the mid-1990s, in establishing financial investigations aimed at confiscating proceeds from crime as part of criminal investigations. Progress has also been made since 2001 in enacting cybercrime legislation, establishing high-tech crime units, improving capacities for the investigation, prosecution and adjudication of cybercrime as well as international co-operation, and more recently also in strengthening public-private co-operation. On the other hand, the anti-cybercrime and the financial investigation/anti-money laundering and counter terrorist financing "worlds" remain largely unconnected.

7. Better knowledge of methods used for laundering the proceeds from crime, including fraud and terrorist financing, on the Internet through exchange of information between relevant public and private sector stakeholders can only facilitate more effective financial investigations, the seizure and confiscation of crime proceeds and the prevention of such crimes through the Internet.

8. The objectives of this study are as follows:

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

1.2 Methodology

9. This study is the result of a cooperative effort of MONEYVAL[3], the Council of Europe's Global Project on Cybercrime[4] as well as the joint project of the European Union and the Council of Europe against money laundering and the financing of terrorism in the Russian Federation (MOLI-RU 2), following the adoption of the project proposal by the MONEYVAL Plenary in September 2009.

10. The study was prepared by a team comprising representatives of Rosfinmonitoring (Financial Intelligence Unit of the Russian Federation as co-leader of the study), the Ministry of Interior of the Russian Federation, the NOCPML (FIU) of Romania, the State Committee for Financial Monitoring (FIU) of Ukraine, the Federal Financial Supervisory Authority (BAFIN) of Germany, the World Bank, the MOLI-RU 2 project, the MONEYVAL Secretariat (co-leader) and the Global Project on Cybercrime (co-leader). Contributors throughout the project's lifetime included representatives of McAfee Labs, PayPal, Team Cymru and UK Payments. Two consultants, Adriana Holtslag-Alvarez (Netherlands) and Dave O'Reilly (Ireland), facilitated the preparation of the literature review, the questionnaire and the report outline, and contributed to the substance of the report.

11. In preparing this report, the team has made use of data and information gathered through a questionnaire which was circulated January 2010 to MONEYVAL and FATF members as well as law enforcement and private sector institutions specialised in cybercrime matters. In view of the joint typology meeting of MONEYVAL and the Eurasian Group (EAG) it was furthermore agreed to associate

[3] For further information, see www.coe.int/moneyval

[4] For further information, see www.coe.int/cybercrime

the Eurasian Group members[5] to the study and their responses to the questionnaire were received in June 2010. The team has thus received 22 responses [6] which enabled to gather valuable information.

12. The project team members have also held several working meetings during this project. A first preparatory meeting between ROSFINMONITORING and the Global Project on Cybercrime was held in Moscow in December 2009. Based on the literature review and the first set of replies received, a first draft report was discussed by the project team at the Council of Europe in Strasbourg in March 2010, which resulted in an agreed draft outline of issues to be covered in the report. An exchange of views was also held with several representatives of the private sector at that time. In June 2010, the preparation of the different sections of the report was distributed to members of the project team and by October 2010, the project team met again to review the draft report.

13. During the joint MONEYVAL/Eurasian Group meeting of experts on typologies of money laundering and terrorist financing (Moscow, 9-10 November 2010), a workshop was specifically dedicated to the themes of: criminal money flows on the Internet (based on the MONEYVAL typology exercise) and to the risks of misuse of E-money in money laundering and terrorist financing schemes (based on the EAG typology exercise). The participation of MONEYVAL and EAG members and public and private sector interventions and discussions fed additional information into the present study and assisted in validating the interim findings.

14. In addition, a wide range of publicly available related literature was made use of. The present study also took into account the findings of the FATF typology studies on money laundering and terrorist financing related to Internet payment systems of June 2008[7] and of October 2010[8]. While these studies focus on new payment methods, the present study provides a broader picture regarding links, risks and counter-measures related to cybercrime, criminal money flows and money laundering on the Internet.

15. Further consultations were held with members of the project team between December 2010 and December 2011 leading to the finalisation of the study.

---

[5] Eurasian Group (EAG) member States are: Belarus, China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Turkmenistan, Uzbekistan.

[6] Responses to the questionnaire and other contributions were received from : Albania (Albanian State Police, Sector for Criminal Assets and Sector against Cyber Crimes);Andorra (Police department, Ministry of the Interior); Belarus (Department for Financial Monitoring); Bulgaria (Financial Intelligence Directorate of State Agency for National Security); China (the People's Bank of China); Estonia (FIU); Germany (Bundeskriminalamt, FIU); Hungary (Hungarian Financial Supervisory Authority); Italy (Prosecutor's Office at Court of Law, Milan); Kyrgyzstan (State Financial Intelligence Service); Poland (Ministry of Finance); Romania (Prosecutor's office attached to the High Court of Cassation and Justice/Organized Crime and Terrorism Investigation Directorate); Russian Federation (project group including Rosfinmonitoring, Ministry of Interior, Federal anti-drugs Service, International Training Centre of Rosfinmonitoring); Slovenia (FIU); Tajikistan (National Bank of Tajikistan); "the former Yugoslav Republic of Macedonia" (Office for Prevention of Money Laundering and Financing Terrorism); Ukraine (FIU) , USA (US Department of the Treasury); Private Sector: McAfee Labs, France; Private Sector: Messaging Anti-Abuse Working Group (MAAWG); PayPal; University College Dublin, Centre for Cybercrime Investigation.

[7] Financial Action Task Force: Money Laundering & Terrorist Financing Vulnerabilities Of Commercial Websites And Internet Payment Systems (June 2008). http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf

[8] Financial Action Task Force: Money Laundering and Terrorist Financing through New Payment Methods (October 2010).http://www.fatf-gafi.org/dataoecd/4/56/46705859.pdf

2 OVERVIEW OF INITIATIVES AND ISSUES INVOLVED

2.1 Context

2.1.1 Measures against cybercrime

16. The Convention on Cybercrime was opened for signature in Budapest in November 2001. By January 2012, it had been ratified by thirty-two states (31 European countries and the USA) and signed by a further 15 countries (11 European as well as Canada, Japan and South Africa). This treaty, under Article 37, is open for accession by countries that are not member States of the Council of Europe and that did not participate in its preparation. So far, Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, the Philippines and Senegal have been invited to accede. In addition, a large number of countries have been using the Budapest Convention as a guideline for reforming their legislation. The treaty has served as a basis for guides on cybercrime, training manuals, model laws and technical assistance. The Budapest Convention thus is the global framework of reference for cybercrime legislation.

17. The Budapest Convention requires States:

- to criminalise attacks against computer data and systems (that is, illegal access, illegal interception, data interference, system interference and the misuse of devices[9]) as well as offences committed by means of a computer system (including computer-related forgery and fraud[10], child pornography[11], and infringements of copyright and related rights[12]);
- to put in place procedural law measures to enable its competent authorities to investigate cybercrime and secure volatile electronic evidence in an efficient manner (including expedited preservation of data, search and seizure of computer systems, interception of communication etc.) [13];
- to cooperate efficiently with other parties to the Convention through general (such as extradition, mutual legal assistance and others) and specific provisions (expedited preservation of data, access to stored computer data, interception of traffic and contents data, creation of 24/7 points of contact and others) on international co-operation.

18. The Convention is complemented by Protocol CETS 189 (of 2003) on xenophobia and racism committed by means of computer systems.

19. 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.

---

[9] See Articles 2-6 of the Budapest Convention on Cybercrime of the Council of Europe (CETS 185).

[10] Articles 7 and 8 of the Budapest Convention.

[11] Article 9 of the Budapest Convention. The term "child pornography" in the context of cybercrime is often considered too limiting. The offences provided for in the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) offer a broader approach.

[12] See Article 10 of the Budapest Convention.

[13] The procedural powers are not limited to the offences listed in articles 2 to 10. The Budapest Convention, in article 14 (2), stipulates that the procedural law powers and procedures are to apply to any criminal offences committed by means of a computer system and the collection of evidence in electronic form of a criminal offence.

20. In order to support countries in the implementation of the Budapest Convention, the Council of Europe, in 2006, launched the Global Project on Cybercrime which assists countries worldwide in the strengthening of their legislation, the training of law enforcement, prosecutors and judges, public-private co-operation, international co-operation as well as measures for the protection of personal data and the protection of children against sexual exploitation and abuse. The third phase of this project was launched in January 2012.[14] This phase also comprises activities related to criminal money flows on the Internet. The global project is complemented by country-specific and regional projects.

2.1.2 Measures aimed at money laundering and the financing of terrorism, and at the search, seizure and confiscation of proceeds from crime

21. As regards the international standards, 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). Both are open Conventions not limited to Council of Europe member States. CETS 141 has been ratified by all 47 Member States of the Council of Europe and Australia. Currently the Conventions are operating side by side.

22. The Warsaw Convention was opened for signature on 16 May 2005 and came into force on 1 May 2008. As at January 2012, 22 States had ratified it and 12 were signatories, including the European Union. It is anticipated that all 47 Council of Europe Member States would in due course become Parties to CETS 198, as has been the case with the 1990 Strasbourg Convention, which was widely ratified. The Convention covers, among other things, confiscation (article 3), investigative and provisional measures (article 4), freezing, seizure and confiscation (article 5), management of frozen or seized property (article 6) and investigate powers and techniques (article 7), the criminalisation of laundering offences (article 9), the establishment of financial intelligence units, financial intelligence units (FIUs) (article 12), preventive measures (article 13), the postponement of domestic suspicious transactions, international requests for information on bank accounts (article 17), on banking transactions (article 18), for monitoring of banking transactions (article 19), for the execution of provisional measures (articles 21 and 22) and for confiscation (articles 23 and 24) and co-operation between FIUs (article 46). The Convention provides for a monitoring mechanism, through a Conference of the Parties to ensure that its provisions are being effectively implemented.

23. The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) is the 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. MONEYVAL not only monitors compliance with standards of the CoE but also of the FATF and the European Union, through a system of mutual peer evaluations. 28 Council of Europe member States, Israel and the Holy See (including the Vatican City State) are subject to its evaluation procedures and processes.

24. The standard setting work (in particular Conventions CETS no. 141 and CETS no. 198) and monitoring activities by MONEYVAL are complemented by technical co-operation projects which assist countries in the implementation of agreed upon standards and follow up to MONEYVAL and FATF

[14] The Global Project on Cybercrime is funded by public as well as private sector contributions. For Phases 1 and 2, that is, between September 2006 and December 2011, the governments of Estonia, Japan, Monaco and Romania and from the private sector McAfee, Visa Europe and in particular Microsoft made voluntary contributions that complemented financing from the regular budget of the Council of Europe.

recommendations. Many of these are joint projects of the Council of Europe and the European Union and include, inter alia, the MOLI-RU projects on money laundering and the financing of terrorism in the Russian Federation.[15]

2.1.3 Key international standards

International standards related to cybercrime

Council of Europe

- Convention on Cybercrime (CETS 185 of 2001) – "The Budapest Convention"
- Additional Protocol on Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189)

International standards related to crime proceeds and money laundering

Council of Europe

- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (CETS 141 of 1990)
- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198 of 2005)

European Union

- Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and implementing measures to the directive
- Regulation (EC) no. 1781/2006 on information on the payer accompanying transfer of funds
- Regulation (EC) no. 1889/2005 on controls of cash entering or leaving the Community
- Directive 2007/64/EC of the European Parliament and the Council on payment services in the internal market

Financial Action Task Force

- The Forty Recommendations (as revised in February 2012)

United Nations

- International Convention for the Suppression of the Financing of Terrorism (1999) (Terrorist Financing Convention)
- United Nations Convention on Transnational Organised Crime (UNTOC) (2000)

[15] The first phase started in February 2003. MOLI-RU phase 2 project ended in December 2010. Similar projects have been implemented in Moldova, Serbia, "the former Yugoslav Republic of Macedonia", and Ukraine.

2.2 Cybercrime: threats, trends, tools and infrastructure

2.2.1 Types of cybercrime

25. Cybercrime can be divided into the following types of offences:

– Offences against the confidentiality, integrity and availability of computer data and systems (the so-called "CIA-offences"), including:
  - illegal access, for example, through "hacking", deception or other means;
  - the illegal interception of computer data;
  - data interference, including the damaging, deletion, deterioration, alteration or suppression of computer data;
  - system interference, including the serious hindering of the functioning of a computer system, for example, through denial of service attacks against critical infrastructure;
  - the misuse of devices, which refers, for example, to the production, sale or otherwise making available of programmes or other devices or tools to commit "CIA-offences".

– Offences committed by means of computer systems, including[16]:
  - computer-related forgery and fraud;
  - content-related offences, in particular child pornography and the sexual exploitation and abuse of children, racism and xenophobia, as well as soliciting, inciting, providing instructions and offering to commit crimes, ranging from murder, to rape, torture, sabotage and terrorism. This category also includes cyber-stalking, cyber-bullying, libel and dissemination of false information through the Internet, and Internet gambling;
  - offences related to infringement of copyright and related rights, such as the unauthorised reproduction and use of computer programmes, audio-/video and other forms of digital works, or of data bases and books.

26. This classification has proven useful for the development of criminal justice responses[17] as well as for analytical purposes. In reality, however, an offence is likely to consist of a combination of different types of criminal conduct as illustrated in the following example involving illegal access, illegal interception, data and system interference, as well as forgery and fraud.

Example: Cybercrime targeting online banking customers[18]

Between July and August 2010, some £675,000 was stolen from a bank in the United Kingdom and some 3,000 customer accounts were compromised by cybercriminals. The case, documented by M 86 Security, illustrates that cybercrime involves a professional business model whereby different members have specific roles, are managed from an administration panel to operate simultaneously, and where legitimate bank accounts of "money mules" are used to transfer funds from compromised accounts.

[16] This is a rather open category in that any offence could involve a computer system in one way or the other.

[17] They also correspond to the categories of offences to be criminalised under the Budapest Convention on Cybercrime (CETS 185) and the Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189).

[18] Source: M 86 Security (White Paper): Cybercriminals Target Online Banking Customers (August 2010) http://www.m86security.com/documents/pdfs/security_labs/cybercriminals_target_online_banking.pdf
Investigations in at least two other European countries have revealed similar patterns.
See for example Bundeskriminalamt (2010): FIU Jahresbericht 2009.
http://www.bka.de/profil/zentralstellen/geldwaesche/pdf/fiu_jahresbericht_2009.pdf

The attack involved the following steps:

- Criminals infect legitimate websites with malware, create fraudulent online advertisement websites and publish malicious advertisement among legitimate websites.
- A user accessing an infected site is redirected to a site from where an exploit kit (in this case "Eleonore Exploit Kit") is loaded on the user's computer. This allows the owner of the exploit kit to control what is loaded to the user's computer, and is used in this case, to install a trojan horse[19]. The malware is well-obfuscated, and only very few anti-virus systems were able to detect it.
- The computer of the user is now a "bot" ("robot" or "zombie") from where the trojan reports back to and receives instructions from the command and control server (in this case hosted in a country of Eastern Europe).
- The user accesses his personal bank account, upon which the trojan transfers login credentials, date of birth and security number to the command and control server.
- As the user accesses the transaction section of the banking site, the data of the transaction form is sent to the command and control servers instead of to the bank.
- The system of the command and control server analyses and decrypts the information and identifies an appropriate money mule bank account.
- The trojan receives instructions to send an updated transaction form to the bank to transfer money to the mule account.
- Confirmation from the bank that the money has been transferred is also sent by the trojan to the command and control server.

2.2.2 Cybercrime tools and infrastructure

27. Information on the cybercrime situation and trends, and on the underlying technology and infrastructure provided by research, industry and public sector reports can be summarised as follows:

2.2.2.1 Malware

28. Malicious software or malware[20] remains the main primary tool for committing cybercrime. Malware is reported to have evolved into a major industry in itself with a complex economic infrastructure and well-organised and well-funded criminal gangs.[21] Viruses, worms and trojans that remove security applications, download additional malware or infect files, or that steal login, account credentials and other data are considered the top malicious code samples.[22] Malware evolves rapidly.

[19] A Trojan horse is a computer programme that appears legitimate but actually has hidden functionality used to circumvent security measures and carry out attacks. A trojan horse may enter a user's computer by presenting itself as a compellingly attractive tool of some sort, which the user intentionally downloads and installs, unaware of its ulterior purpose. Trojans typically build in the functionality of keyloggers and other spyware and a range of other functions to disable system security (Source: OECD (2007): Malicious Software (Malware) – A security threat to the Internet Economy. http://www.oecd.org/dataoecd/53/34/40724457.pdf)

[20] "Malicious software, commonly known as "malware", is software inserted into an information system to cause harm to that system or other systems, or to subvert them for uses other than those intended by their owners" (Source: OECD (2007): Malicious Software (Malware) – A security threat to the Internet Economy. http://www.oecd.org/dataoecd/53/34/40724457.pdf).

[21] Sophos Security Threat Report 2010 (August 2010), page 28. http://www.sophos.com/security/topic/security-report-2010.html

[22] See for example: Symantec Intelligence Quarterly April – June 2011

For illustration, Symantec notes that it created more than 450,000 malicious new code signatures in the period April to June 2010 in order to capture new malware variations. An increasing number of PCs is infected with malware.[23]

29. The web remains the main vehicle for malware. According to Sophos, Internet users are lured to sites where they are infected by malware. Some of these are compromised legitimate sites from where users are re-directed to sites hosting malicious webpages. In the second half of 2009, most of these were hosted in the USA (37.4%) followed by Russia (12.8%) and China (11.2%, compared to 51.4% in 2007).[24] Symantec for the period April to June 2010, lists the USA as the top-ranked country for malicious activity (accounting for 21%), followed by India (6%), Germany (5%), China (5%) and Brazil (5%). The top web-based attack was related to malicious PDF activity (36%).[25] Microsoft reports for 2009 that in terms of malware and potentially unwanted software the USA with more than 15%, China (about 8%) and Brazil (about 6%) were most infected. China (+19.1%), Russia (+16.5%) and Brazil (+ 15.8%) showed the most important increases.[26]

30. In terms of e-mail threats, spam remains a major tool for fraud schemes and spreading malware. Microsoft reports that spam associated with advance-fee fraud and gambling increased significantly in the second half of 2009. The USA accounted for 27% of spam sent, followed by Korea (6.9%), China, (6.1%), Brazil (5.8%) and Russia (2.9%).

31. Most e-mail traffic consists of spam[27] and it seems that very few botnets are responsible for the vast majority of botnet spam sent.[28] In the period April to June 2010, Symantec observed 12.7 trillion spam messages, accounting for 89% of all email traffic observed.[29] SPAMHOUSE maintains that:

> "*80% of spam received by Internet users in North America and Europe can be traced via aliases, addresses, redirects, locations of servers, domains and dns setups, to a hard-core*

(http://www.symantec.com/business/threatreport/quarterly.jsp); Microsoft Security Intelligence Report, 2010 (http://www.microsoft.com/security/about/sir.aspx).

[23] In Germany, for example, it is estimated that in 2010, 43% of Internet users have experienced malware infections of their computers. http://www.bitkom.org/65019_65010.aspx
According to Symantec, globally 51% of computes have experienced malware.
http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf

[24] Sophos Security Threat Report 2010 (August 2010) (http://www.sophos.com/security/topic/security-report-2010.html).

[25] Symantec Intelligence Quarterly April – June 2010
http://www.symantec.com/business/theme.jsp?themeid=threatreport

[26] Based on computers cleaned with Microsoft anti-malware products) Microsoft Security Intelligence Report, Volume 8, July through December 2009 http://www.microsoft.com/security/about/sir.aspx

[27] Estimates range from 75% to more than 90% of all email sent worldwide. According to the Commtouch Internet Threats Trend Report Q1 2010, spam and phishing messages average 183 billion per day. (www.commtouch.com/download/1679)

[28] Microsoft Security Intelligence Report, Volume 8, July through December 2009. According to this report, in the second half of 2009, three botnets accounted for 78.8% of spam, that is, Rustock 39.7%, Bagle-cb 28.6% and Cutwail 10.4%. Botnets such as "Rustock" were believed to be able to send up to 30 billion spam mails per day. http://www.microsoft.com/security/about/sir.aspx. Thus, the closing down in November 2008 of MColo, a web hosting provider in San Francisco, that had hosted the then world's largest botnet "Srizbi", reportedly reduced global spam by more than 50%, temporarily. http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658_2.html?sid=ST2008111801165&s_pos=

[29] Symantec Intelligence Quarterly April – June 2010
http://www.symantec.com/business/theme.jsp?themeid=threatreport

group of around 100 known spam operations, almost all of whom are listed in the ROKSO database".[30]

2.2.2.2 Botnets[31]

32. Botnets continue to be considered the primary threat with regard to cybercrime and information security. They consist of groups of individual computers that are infected with a piece of malware which turns these infected computers into "robots" (bots) or "zombies"[32] that are controlled remotely and without the knowledge of the owners of the computers by the originators or masters of the botnet ("bot herders") from command and control servers. The malware may furthermore be able to scan for vulnerabilities and propagate itself to further systems.

33. In 2005, the authorities of the Netherlands uncovered a botnet operation involving 1.5 million infected computers ("bots")[33]. In December 2009, the Mariposa botnet was dismantled that consisted of up to 12 million infected computers.[34] The malware monitored activities on infected systems for passwords, bank credentials and credit cards.[35]

34. Through botnets large amounts of spam can be distributed or websites can be paralysed. They can thus also be used for distributed denial of service (DDOS) attacks in order to paralyse critical infrastructure. At the same time, it is rather difficult to trace attacks back to the originators.

35. The take-down of the Rustock botnet in 2011, following legal action by Microsoft and other partners, shows new legal and law enforcement avenues for measures by the private sector and through public private cooperation.[36] Combined with follow-the-money techniques, attribution to criminals or criminal organisations should be possible.[37]

2.2.2.3 Domains used for criminal purposes

36. A further building block of the cybercrime infrastructure is the use of domains for criminal purposes. These domains are then used for botnet and spamming operations as well as hosting child pornography and other illegal content and for offering underground goods and services.

37. The misuse of domains for criminal purposes is facilitated by several factors:

---

[30] "The Register of Known Spam Operations (ROKSO) database collates information and evidence on known professional spam operations that have been terminated by a minimum of 3 Internet Service Providers for spam offenses". http://www.spamhaus.org/rokso/

[31] See Microsoft Security Intelligence Report, Volume 9, January through June 2010 with a detailed analysis of botnets (http://www.microsoft.com/security/sir/)

[32] Commtouch reports that in the first quarter of 2010, some 305,000 zombie computers were newly activated per day. Brazil (14%), India (10%), Vietnam (8%), the Russian Federation (7%) and Ukraine (4%) produced most zombies. (www.commtouch.com/download/1679)

[33] http://www.v3.co.uk/vnunet/news/2144375/botnet-operation-ruled-million

[34] Suspected leaders were arrested in Spain in February 2010, and the suspected creator of the malware was arrested in Slovenia in July 2010.

[35] http://en.wikipedia.org/wiki/Mariposa_botnet

[36] http://www.wired.com/beyond_the_beyond/2011/03/microsoft-versus-rustock-botnet/
For the complaint brought forward by Microsoft see the link at
http://krebsonsecurity.com/2011/03/homegrown-rustock-botnet-fed-by-u-s-firms/

[37] http://krebsonsecurity.com/2011/03/microsoft-hunting-rustock-controllers/

- Some domain or web hosting services allow for "bullet proof hosting", that is, providers do not cooperate with law enforcement and are lenient towards the activities of their customers and the materials they upload or distribute.[38] Some of those offering bullet proof hosting are reportedly themselves criminal organisations.[39]
- In many countries, there appear to be legal obstacles to closing down domains. This seems to be particularly the case if the criminal activities target other countries that the one where the domain is hosted.
- Registrars and registries often fail to exercise due diligence when domains are registered. Internet resources, such as domain names are managed/coordinated respectively by the Internet Corporation for Assigned Names and Numbers (ICANN) and Regional Internet Registries (RIRs) and their registrars (e.g. Internet Service Providers). To obtain these resources, a registrant has to provide certain personal information to the WHOIS database. According to a recent report for ICANN, less than half of records were fully accurate (only 23% when using strict definition of accuracy).[40] Inaccuracies are also found in WHOIS of RIRs. This hampers law enforcement efforts to track those who use domains for criminal activities. The arrival of IPv6 is likely to aggravate further this situation, as large amounts of IP addresses will be distributed under the current registration procedures.[41]
- Even if criminal domains are terminated, criminals are able to transfer their operations elsewhere.

2.2.2.4 Underground economy

38. In recent years, an "underground economy" has emerged that provides a market for tools, goods and services to commit cybercrime and for the sale of stolen goods and information. It represents a "genuine economic environment" for producers, traders, service providers, 'fraudsters' and customers"[42], and allows criminals to organise themselves. According to Symantec,[43] credit card details were the most frequently advertised item on underground servers in the period April to June 2010 (28%) followed by bank accounts (24%).

---

[38] Many "bullet proof" domains are reportedly hosted in Eastern Europe and the Far East. For an example in Europe see the report by Spamhouse on the criminal 'Rock Phish' domains registered at Nic.at (http://www.spamhaus.org/organization/statement.lasso?ref=7)

[39] A notorious example is the Russian Business Network (http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html; http://www.bizeul.org/files/RBN_study.pdf).

[40] http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf

[41] The 2010 Octopus conference of the Council of Europe therefore recommended due diligence measures by ICANN, registrars and registries and accurate WHOIS information, and endorsement of the "Law Enforcement Recommended Amendments to ICANN's Registrar Accreditation Agreement (RAA) and Due Diligence Recommendations" in line with data protection standards (http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/cy-activity-Interface-2010/2079_IF10_messages_1s%20provisional%20_24%20Apr%2010.pdf). http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/Ws%202/LEA_ICANN_Recom_oct2009.pdf

[42] G Data Whitepaper 2009: Underground Economy (http://www.gdata-software.com/uploads/media/Whitepaper_Underground_Economy_8_2009_GB.pdf)

[43] Symantec Intelligence Quarterly April – June 2010 http://www.symantec.com/business/theme.jsp?themeid=threatreport. See also the list of goods and services available for sale on underground economy servers (Symantec Corporation, 2010) at http://www.symantec.com/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers

39. Underground platforms furthermore provide drop zones for stolen goods and means for "cashout", that is, for turning virtual money into real money.[44]

40. Goods and services include:

- Credit cards and other information for the commission of identity-related fraud.
- Offshore banking services and the creation of shell corporations.
- "Expert services" such as malware development, recovery of data and anti-forensics.
- Spamming services, that is, the delivery of spam against payment.
- "Bullet proof" web hosting.
- Online offering of malware and tools to facilitate or commit other crimes, such as malware toolkits and fake anti-virus software. Malware toolkits allow non-technically skilled people to create and deploy a malware that targets online banking services. These malware toolkits typically contain features like keyloggers, form grabbers and botnet "zombie" software.

2.2.2.5 Money mules

41. "Money mules" or "financial agents" are money couriers that form an essential part in the movement of proceeds from crime between the victim to the offender.[45] Mules may be or be not aware of the fact that they are part of a criminal operation. Their recruitment may take place by various means; potential mules may be contacted via spam or respond to apparently legitimate recruitment websites where "financial manager", "work at home" or similar positions in a fake company are advertised. Mules may sign formal contracts of employment and be required to deposit copies of passports and other ID information.

42. Their primary role is to open a bank account or make their own bank account available. Once they receive funds in their account they will receive instructions to transfer these funds to other accounts or abroad using wire transfer services, thereby facilitating money laundering, while keeping a commission.

43. It has been argued that "money mules" are the bottleneck of fraud-related cybercrime, and that not enough mules are available to exploit stolen credit card and other ID information.

2.2.3 New platforms for cybercrime

2.2.3.1 Social networking platforms

44. Social networking sites and the number of users expanded considerably in recent years[46], and are now also used for spreading malware, offer targets for other form of cybercrime and constitute security risks. According to Sophos,[47] social networks have become a viable and lucrative market for malware distribution with Web 2.0 botnets stealing data, displaying fake anti-virus alerts and generating income for criminals. The proportion of companies reporting spam and malware attacks via social networking increased by 70% in 2009. Employees logging on to social networking sites thus

[44] G Data Whitepaper 2009: Underground Economy, page 17-18 (http://www.gdata-software.com/uploads/media/Whitepaper_Underground_Economy_8_2009_GB.pdf).

[45] http://www.banksafeonline.org.uk/moneymule_explained.html

[46] Facebook alone claimed some 845 million active users in December 2011 (http://www.facebook.com/press/info.php?statistics).

[47] Sophos Security Threat Report 2010 (August 2010). http://www.sophos.com/security/topic/security-report-2010.html

pose serious security risks to the information systems of their companies or institutions by opening them up for spam, phishing, malware and data infiltration.

2.2.3.2 Cloud computing

45. Technological developments create further vulnerabilities to cybercrime. A much discussed trend is "cloud computing", that is the migration of data and services from specific computers to servers "somewhere" in the clouds. This entails tremendous opportunities but has also far reaching security implications. On the one hand, individual computers will become less attractive targets, but on the other hand "with more sensitive data being stored on the Internet [..]. there is the potential for more serious security breaches and for more information to be stolen more rapidly than ever before".[48]

46. The fact that much of the traffic and other data needed for criminal investigations will be stored on servers in foreign or unknown jurisdictions will render law enforcement very difficult, and in turn facilitate cybercrime.[49]

2.2.4 Organising for cybercrime

2.2.4.1 Organised crime

47. Economic crime has been the primary activity of organised crime groups for many years. The trend observed since 2004, namely, that criminals increasingly organise to exploit the opportunities of the Internet and other information technologies continues, the more institutions and individuals use such technologies for their economic activities.[50] Organising for cybercrime is furthermore facilitated by anonymity, depersonalisation and ease of communication, the possibilities of global outreach for co-operation between criminals for and targeting of victims, the disconnection between the location of the offender and the victims, and the opportunities for money laundering.

48. Complex fraud operations, the infrastructure of cybercrime (including botnets and the underground economy), the level of specialisation and division of roles show the features of structured organised criminal groups that act in concert to commit offences to obtain financial or other material benefit.[51]

---

[48] Sophos Security Threat Report 2010 (August 2010), page 34 (http://www.sophos.com/security/topic/security-report-2010.html). See also http://www.sonicwall.com/downloads/SB_Security_Trends_US.pdf

[49] http://www.eurodig.org/eurodig-2010/programme/workshops/workshop-1
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf
In order to address the question of transborder access by law enforcement and related jurisdiction issues, the Cybercrime Convention Committee in November 2011 decided to establish an ad-hoc group to identify solutions such as Protocol to the Budapest Convention or a soft-law instrument.

[50] http://www.coe.int/t/dghl/co-operation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf
http://www.coe.int/t/dghl/co-operation/economiccrime/organisedcrime/Report2005E.pdf

[51] As defined in article 2 of the United Nations Convention on Transnational Organised Crime.

2.2.4.2 Persistent threats against political or economic targets

49. Threats directed at political or economic targets without immediate economic gain,[52] such as espionage, "hacktivism", terrorism[53], war and conflict by means of computer systems are real concerns. [54]

50. However, intrusions and denial of service attacks such as those on Estonia in 2007[55], on Georgia in 2008[56], the USA and South Korea in July 2009[57], the Google intrusion in December 2009[58] or the intrusion into governmental, business and academic computer systems in India in 2009 illustrate the difficulty of differentiating between crime, espionage[59], terrorism and war as long as attacks cannot be clearly attributed.[60] Since these threats are not aimed at generating crime proceeds they are not dealt with further in the present study.[61]

---

[52] These have also been named "Advanced persistent threats" or APT. It seems this term was coined by Mandiant, a US Security firm (http://www.mandiant.com/services/advanced_persistent_threat/). For a brief definition see: http://www.damballa.com/knowledge/advanced-persistent-threats.php. Also: http://tominfosec.blogspot.com/2010/02/understanding-apt.html
For some examples see: http://www.businessweek.com/magazine/content/08_16/b4080032220668.htm

[53] The use of the Internet for terrorist purpose may include denial of service or other types of attack against critical infrastructure, the use of the Internet for incitement, recruitment and training for terrorism, or the use of information technologies for target identification, communication, financing and other logistical purposes. http://book.coe.int/EN/ficheouvrage.php?PAGEID=36&lang=EN&produit_aliasid=2221
http://www.mpicc.de/ww/en/pub/forschung/forschungsarbeit/strafrecht/cyberterrorismus.htm

[54] Recent examples include attacks against servers hosting WIKI LEAKS and in turn against sites of organisations that had stopped business relations with WIKI LEAKS.
http://www.csmonitor.com/Business/new-economy/2010/1208/WikiLeaks-cyberattacks-now-involve-Visa-Facebook-Twitter-MasterCard
http://www.theglobeandmail.com/news/technology/wikileaks-faces-cyber-attacks-loses-paypal-account-for-donations/article1825485/
http://news.cnet.com/8301-31921_3-20024935-281.html

[55] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

[56] http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

[57] http://www.guardian.co.uk/world/2009/jul/08/south-korea-cyber-attack
http://en.wikipedia.org/wiki/July_2009_cyber_attacks

[58] http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html

[59] http://www.pwc.com/en_US/us/it-risk-security/assets/e-espionage.pdf.
See also Shadows in the Cloud: Investigating Cyber Espionage 2.0 (April 2010) (http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0). This study documents a complex ecosystem of cyber espionage, including theft of classified and sensitive documents, a command and control infrastructure that made use of social media to compromise computers and then redirect to and control these computers from accounts on free hosting services and later on from command and control servers hosted in a country of East Asia.

[60] Charney, Scott (2009): Rethinking the Cyber Threat A Framework and Path Forward (Microsoft) (http://www.microsoft.com/downloads/details.aspx?FamilyID=062754cc-be0e-4bab-a181-077447f66877&displaylang=en). Also: http://garwarner.blogspot.com/2010/07/future-of-cyber-attack-attribution.html

[61] It may thus be useful to deploy the means provided by criminal law and make best possible use of instruments such as Budapest Convention on Cybercrime - and with regard to terrorism also the Convention for the Prevention of Terrorism of the Council of Europe (CETS no. 196) (http://www.conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG) - before escalating other means.

2.2.4.3 Financing of terrorism

51. Terrorist organisations require funding not necessarily for specific attacks but "to meet the broader operational costs of developing and maintaining a terrorist organisation and to create an enabling environment necessary to sustain their activities".[62]

52. Terrorists may raise funds through legitimate businesses or charitable entities or a variety of criminal activities that increasingly involve the Internet, such as the hacking of online bank accounts, fraud and theft committed with stolen credit card credentials and the laundering of proceeds through online gambling sites. Websites of charities are reported to be used to raise funds also for terrorist purposes, and online payment systems are vulnerable for misuse by terrorist organisations.[63]

2.3 Proceeds generating offences on the Internet

53. Obtaining financial or other economic benefits has been one motivation of cybercriminals from the very beginning.[64] However, there is general agreement that generating proceeds is now the primary purpose of cybercrime.

54. It is difficult to arrive at an estimate on criminal money flows on the Internet and consolidated studies appear not to available. Certain consideration may lead to the assumption that cybercrime is perhaps the most profitable field of crime:

- Societies are dependent on information and communication technology;
- Almost any crime can be committed more effectively and with less risk on the Internet;
- Some two billion people, most companies, in particular the financial sector, and public institutions of the world are connected to the Internet.[65] They are all potential victims of cybercrime;
- Cybercrime can be committed across boundaries. This reduces the risk of detection. The fact that victims are abroad limits the interest of law enforcement to investigate and prosecute. Inefficient international co-operation and weak legislation further reduces risks for criminals;
- Cybercrime, including fraud schemes, are increasingly automated and thus do not rely on the availability of criminal man power;
- The underground economy provides inexpensive and easy access to tools needed to commit cybercrime. More and more sophisticated attacks can be committed with less and less knowledge;
- Cybercrime usually does not require violence or coercion, and is thus less hindered by face-to-face, humane inhibitions.

55. Based on these considerations, it can be assumed that the economic damage resulting from cybercrime exceed that of any other type of organised and economic crime. However, economic damage does not equal criminal money on the Internet. Repair cost, lost productivity, revenue loss,

---

[62] Source: FATF (2008): Terrorist Financing (http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf)

[63] Jacobson, Michael 'Terrorist Financing and the Internet', Studies in Conflict & Terrorism, 33:4, 353 – 363. Available at: http://www.informaworld.com/smpp/section?content=a919769800&fulltext=713240928
Financial Action Task Force: Money Laundering & Terrorist Financing Vulnerabilities Of Commercial Websites And Internet Payment Systems (June 2008). http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf

[64] See "Der Spiegel" (Germany) of 22 January 1979. Earlier forms of cybercrime included "phone phreaking" in the early 1970s (Schmidt, Howard (2006): Patrolling Cyberspace, Larstan Publishing).

[65] For illustration: the value of shipments, sales or revenue of US e-commerce reached 3,7 trillion in 2008 (Source: http://www.census.gov/econ/estats/2008/2008reportfinal.pdf).

data loss, reputation effects, infrastructure, patch deployment and development, security measure, law enforcement and others may be more expensive for companies than the monetary damage cased by fraud and theft. [66]

56. The following data illustrates the amounts at stake and also points at the need for more comprehensive analysis and reporting:

- From the 146,663 complaints received and referred to law enforcement in 2009 by the US Internet Crime Complaint Center, 100,206 complaints involved monetary losses amounting to US$ 559.7 million.[67]
- Complaints compiled through the Consumer Sentinel Network US Federal Trade Commission[68] reached 1.3 million in 2009. The amounts paid and lost through fraud schemes exceeded US$ 1.7 billion in 2009.
- In Germany, the damage of Internet crime actually recorded by the Federal Criminal Police amounted to Euro 36.9 million in 2009.[69]
- In 2008, airlines are estimated to have had losses in revenue of US$ 1.4 billion due to fraudulent online bookings.[70]
- Lost revenue due to software piracy has been estimated at US$ 53 billion in 2008.[71]
- A survey covering 45 US companies, published in July 2010, indicates that each company experiences about one successful attack per week on average with median annual cost of US$ 3.8 million. External cost are primarily related to the theft of information (42%) and business disruption and lost productivity (22%), while 46% of internal cost are related to detection and recovery.[72]
- UK Payments estimated the total payment card fraud losses in 2009 at £440.3 million.[73] Of this, card-not-present (CNP) fraud accounted for £266.4m.

57. Not all computer related criminality gives rise to criminal proceeds. The following proceeds generating types of crime, and thus potentially predicate offences to money laundering, appear to be particularly prevalent.

2.3.1 Fraud

58. The main category of proceeds-generating crime on the Internet – as in the real world – is fraud, that is, the intentional deception causing loss of property to another person for economic gain.[74] In order to ensure that not only traditional fraud committed in the IT and online environment is

[66] For a typology of costs of security breaches see Van Eeten, Michel / Bauer, Johannes M. / Tabatabaie, Shirin (2009): Damages from Internet Security Incidents - A framework and toolkit for assessing the economic costs of security breaches. TU Delft (www.opta.nl/nl/download/publicatie/?id=3083)

[67] Internet Crime Complaint Center (2010): Internet Crime Report 2009 (http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).

[68] US Federal Trade Commission Consumer Sentinel Network data for 2009 http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf. These include also the IC3 data.

[69] According to the BKA this does not include the damage of phishing or botnets as these are not recorded under a unique code.

[70] http://forms.cybersource.com/forms/airlinefraudpr

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

[72] http://www.arcsight.com/press/release/arcsight-and-ponemon-institute-release-first-annual-cost-of-cyber-crime-stu/

[73] http://www.ukpayments.org.uk/resources_publications/key_facts_and_figures/card_fraud_facts_and_figures/

[74] For an A-Z of fraud schemes see http://www.actionfraud.org.uk/a-z_of_fraud

criminalised, but also fraud involving interference with computer data and systems, a specific provision on "computer-related fraud" was included in the Budapest Convention on Cybercrime.[75]

59. Replies to the questionnaire confirm fraud as the main category of cybercrime in the majority of respondent countries. For example[76]:

- Albania: Fraud with credit cards and fraud via the Internet are reported to be on the increase. Since June 2009, eight cases involving credit card fraud and 5 cases of fraud through the Internet have been identified, and 15 criminal proceedings have been initiated, of which
  - 13 cases are computer fraud, including 8 credit card fraud and 5 cases of fraud via the Internet;
  - 1 case of system interference;
  - 1 case of distribution of child pornography.

- Andorra: Most cybercrime appears to be related to credit cards (53 investigations in 2009), followed by fraud via Internet (12 investigations), libel (10 investigations) and child pornography (7 investigations).

- Estonia: recorded cybercrime increased from 71 cases (in 2005) to 501 (in 2009), of which 470 were computer-related fraud. Computer-related fraud accounts also for the vast majority of crimes prosecuted (353 out of 368 cases and 148 out of 159 persons prosecuted in 2009). In six convictions for money laundering in 2009, the Internet was found to be part of the offence.

- Germany: the general German Police Crime Statistics,[77] that reflect all offences recorded by the police, state 63,642 computer crimes for 2008.[78] The largest category with 23,689 cases was fraud using an unlawfully obtained debit card with PIN, followed by computer-related fraud, that is, fraud involving an interference with computer data and systems, with 17,006 cases. The third category was illegal interception or data espionage with 7,727 cases, followed by computer-related forgery (5,716 cases) and fraud related to unauthorised access to communication services (5,244 cases).

[75] "Article 8 – Computer-related fraud
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
a any input, alteration, deletion or suppression of computer data;
b any interference with the functioning of a computer system,
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. "
In some countries, fraud provisions traditionally require the deception of a person or of a human mind, and do not cover the deception of a computer system. In Germany, for example, a specific article (Section 263a StGB – Computer Fraud) was therefore introduced in line with article 8 of the Budapest Convention (see: Brunst, Philip/Sieber, Ulrich (2010): Cybercrime legislation. In: Basedow, J./Kischel, U./Sieber, U. (eds): German National Reports to the 18th International Congress of Comparative Law, Washington 2010, page 730-731.

[76] Source: replies to the questionnaire unless indicated otherwise.

[77] The unlawful (criminal) acts dealt with by the police, including attempts subject to punishment, are recorded in the Police Crime Statistics

[78] Similar to previous years: 62944 (2007), 59149 (2006), 62186 (2005), 66973 (2004).

In the specific situation report on Internet crime for 2009,[79] the German Federal Criminal Police Office (BKA), notes 50,254 crime crimes in the narrow sense, that is, excluding credit card fraud:

- 22,963 cases of computer-related fraud (an increase of 35% compared to 2008);
- 11,491 cases of illegal interception/data espionage (an increase of 48.7%);
- 7,205 cases of fraud related to unauthorised access to communication services (an increase of 37.4%);
- 6,319 cases of computer-related forgery (an increase of 10.6%);
- 2,276 cases of data interference/sabotage (an increase of 3.1%).

The damage recorded was Euro 36.9 million.[80]

– Italy: computer fraud was the main category of cybercrime with 1,753 cases investigated between April 2008 and April 2009 by the Milan prosecution office, followed by cases of illegal access (541 cases). In another 1,653 fraud cases computers played an important role (for example auction fraud).[81]

– Lithuania: almost all cybercrime cases were related to fraud (4,586 cases recorded in 2009), illegal use of means of payment (2,376) and production and unlawful possession of electronic means of payment (881).

– Poland: in 2008, 94 new money laundering cases sent by the financial intelligence unit to the public prosecution office involved the use of Internet (compared to 14 in 2007 and 31 in 2006).

– Russian Federation: the Ministry of Interior of Russia has intensified activities in this field. In 2008, the department "K" of the Ministry initiated over 5,500 criminal investigations of illegal activities in the information technology sector, an increase of 20% compared to 2007. In January 2009, the Department initiated between 50 and 100 criminal proceedings weekly.

– Slovakia: police statistics do not allow extracting of cases involving computer systems, unless they involve the misuse and destruction of records on information carriers (including misuse of login data for Internet banking). 23 such cases were noted in 2008, and 28 in 2009. In 2009, the financial intelligence unit noted 128 cases of unusual transactions related to phishing and involving money transfer via money service businesses.

– Slovenia:[82] 9 cases were investigated and prosecuted for larceny and breaking into computer systems. In two of the cases, two persons withdrawing cash were convicted for money laundering by negligence. One case is still under court investigation for money laundering by negligence and another case is still pending prosecution. The possible proceeds amounted to Euro 128,500, but the majority of these proceeds were blocked by the Office for the Prevention of Money Laundering or with court orders and in some cases, banks returned the proceeds to the original accounts. The actual economic loss thus did not exceed Euro 30,000. Nine cases were connected to breaking into information systems and two to building fake

[79] http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_2009.pdf

[80] According to the BKA this does not include the damage of phishing or botnets as these are not recorded under a unique code.

[81] The data were provided by the Milan Prosecution Office. Following Law no. 48 of 18 March 2008 (which ratified the Budapest Convention on Cybercrime) 29 prosecution offices at the level of courts of appeal districts handle cybercrime.

[82] Reportedly, the malware for the Mariposa botnet was designed by Slovenian offenders. http://www.networkworld.com/news/2010/072810-alleged-mariposa-botnet-hacker-arrested.html

Internet sites. So far, two cases connected to breaking into information systems ended with convictions for money laundering.

– Ukraine: an increasing number of cybercrime-related offences is recorded every year and forwarded to courts: from 311 cases (of which 226 sent to court) in 2002, to 615 (364) in 2005, 691 (597) in 2008 and 707 (584) in 2009. Of these, 31 cases were related to data and system interference and misuse of devices and were investigated and sent to court In 2009.

– USA:[83] The IC3 Internet Complaint Center of the USA in 2009 received 336,655 complaint submissions, of which 146,663 were referred to law enforcement.[84] Most of these referrals were complaints related to the non-delivery of goods and services (19.9%), identity theft (14.1%), debit/credit card fraud (10.4%) and auction fraud 10.3%). Complaints compiled through the Consumer Sentinel Network of the US Federal Trade Commission[85] reached 1.3 million in 2009, of which 54% were fraud, 21% identity theft and 25% other types of complaints. Schemes include:
  - Online dating scams perpetuated through email and dating websites by fraudsters that pose as young women and engage potential victims in personal communication before soliciting funds for travel from country of the offender to the country of the victim. Money transmitters are often used to move the funds. These result in millions of dollars in fraud loss to U.S. victims.
  - Online bank theft based on intrusion and account takeover of online financial accounts to launder millions of dollars through a US-based network of money transfer mules. Social engineering is often used (via the computer or telephonically) to obtain account access or elevate account access or gain valuable information such as executives' email addresses for targeted identity theft. Crimes may also involve phishing, redirection to fake websites, account takeover, etc.
  - Online gambling through the recruitment of US-based players and the exploitation of the International banking infrastructure (bank checks, wire transfers, money remittances) which involves the laundering of significant sums of money using websites and operating from offshore locations.
  - Manufacture and/or sale of false identification documents (driver licenses, passports, insurance cards, etc.).
  - Online services offering offshore banking services, the creation of shell corporations, web hosting, money laundering, spamming services, and others.
  - Distributed Denial of Service attacks (DDoS) which are launched for a variety of reasons, sometimes to knock competitors' websites off-line.
  - Made to order or "off the shelf" malicious software (malware) to include key loggers, form grabbers, botnets, etc. in support of identify crimes such as account takeovers
  - Sale of false anti-virus programmes, pirated software and counterfeit pharmaceuticals.
  - Credit card fraud and online financial fraud through the theft of personal identifiers and the exploitation of e-commerce merchants, express shipping businesses, banking institutions and online payment business platforms such as PayPal and Google Checkout. Two significant types of crimes that result are:
    - reshipping of stolen computers, high-tech accessories, fashion accessories, etc. through an extensive network of reshipper mules based in the U.S. to offshore criminal ringleaders;

[83] For a listing of cases, see http://www.justice.gov/criminal/cybercrime/cccases.html

[84] Internet Crime Complaint Center (2010): Internet Crime Report 2009 (http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).

[85] US Federal Trade Commission Consumer Sentinel Network data for 2009 http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf. These include also the IC3 data.

- laundering of illegal proceeds from the sale of non-existent merchandise such as software, videogames, etc. on auction platforms where the merchandise is subsequently ordered through an e-commerce merchant with stolen identity and financial information; illegal proceeds are laundered through a large number of online payment and financial institution accounts in the U.S. and subsequently sent via wire transfer to criminal ringleaders located offshore.

60. Another scheme may involve fiscal fraud, whereby cyber-criminals can make fraudulent claims for benefits by attaching official online systems, such as the self-assessment forms. [86]

61. Many types of fraud are thus committed on the Internet and it is difficult to arrive at a detailed classification. Recent reports suggest that the following phenomena are particularly prevalent.

2.3.1.1 Identity theft

A wide range of fraud involving the Internet and other information and communication technologies is related to identity theft in one way or the other, whether ID theft is defined as "fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person's consent" [87], "the misuse of the identity (name, date of birth, address, financial information or other personal details) of another person without knowledge or consent" or as "assuming the identity of another person by stealing personally identifiable information (PII) to commit fraud" or as "the theft or assumption of a pre-existing identity (or significant part of it), with or without consent, and regardless of whether the person is dead or alive".

62. Conceptually, ID theft can be separated into three distinct phases[88]:

1. The obtaining of identity information, for example, through physical theft, through search engines, insider attacks, attacks from the outside (illegal access to computer systems, trojans, key-loggers, spyware and other malware), or phishing and other social engineering techniques
2. The possession and disposal of ID information, which includes the sale of such information that now plays an important role in the e-underground economy where credit card information, bank account details, passwords or full identities are among the most offered goods
3. The use of ID information in order to commit fraud or other crimes, for example by assuming another person's identity to exploit bank accounts and credit cards, create a new account, take out loans and credit, order goods and services or disseminate malware.

---

[86] Man arrested for £1m online tax fraud, See http://www.theregister.co.uk/2009/09/04/pceu_hmrc/

[87] Definition proposed by Koops, Bert-Jaap/Leenes, Ronald (2006). http://www.fidis.net/fileadmin/fidis/publications/2006/DuD09_2006_553.pdf
The US Identity Theft and Assumption Deterrence Act (title 18, s. 1028(a)(7) U.S.C.), punishes a person who: "knowingly transfers or uses, without lawful authority, of a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."

[88] Alexander Seger (2007) in: Demosthenes Chryssikos, Nikos Passas, Christopher D. Ram (eds): The evolving challenge of identity-related crime: addressing fraud and the criminal misuse and falsification of identity (UN ISPAC), page 154. http://www.ispac-italy.org/pubs/ISPAC%20-%20Identity%20Theft.pdf
See also:
http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf

63. Phishing remains one of the main social engineering techniques used on the Internet to steal ID-related information for fraudulent use. Variations include "smishing" (mobile phone text messages to seek the disclosure of information), "spear phishing" (personalised bogus message targeted at a single individual), "pharming" (redirecting website traffic from a legitimate website to a counterfeit website to trick users into disclosing information) and "spoofing" (a person or programme is masquerading as somebody or something else to gain trust and make them enter their details into a counterfeit website). Financial institutions as well as online payment systems and auction platforms are the main targeted sectors.[89] From a money laundering perspective, one should report a phishing attack when the information obtained is used to transfer funds from an account to another.

64. The Anti-phishing Working Group noted some 126,700 phishing attacks in the period July to December 2009.[90] Two thirds of these attacks were the responsibility of the Avalanche phishing gang which used a technique and an infrastructure for mass-produced phishing sites targeting more than forty financial institutions, online services and job search providers to obtain identity information. This criminal enterprise, moreover, combined phishing with the distribution of malware to steal further information:

> "In addition, the criminals used the Avalanche infrastructure to distribute the notorious Zeus Trojan, a sophisticated piece of malware that the criminals incorporated into its phishing and spamming campaigns. Zeus is crimeware – malware designed specifically to automate identity theft and facilitate unauthorized transactions. Potential victims are sent phishing-like lures that purport to offer popular software upgrades, file sharing services, and downloadable forms from tax authorities (such as the Internal Revenue Service in the United States, and Her Majesty's Revenue & Customs service in the United Kingdom). If a recipient takes this bait and his or her computer is infected, the criminals can remotely access that machine, steal the personal information stored on it, and intercept passwords and online transactions. The criminals can even log into a victim's machine to perform online banking transactions using the victim's own account details. This is difficult for the banks to detect as fraud. This combination of phishing and malware, advertised by spam, became one of the most insidious combinations on the Internet."[91]

65. Identity theft-related fraud schemes thus include data interference to deceive computer systems.

66. There is no data available at global level on the scale of cyber identity theft, though information is emerging from some country national assessments[92]. Of the 146,664 complaints referred by the US Internet Crime Complaint Center to law enforcement in 2009, identity theft was the second most referred category (14.1%) after the non-delivery of goods (19.9%).[93] The Consumer Sentinel Network report of the US Federal Trade Commission lists identity theft as the main category of complaints reported in 2009 (21% or 278,078 of 721,418 complaints received). The most common forms of identity theft were credit card fraud (17%), government/benefits fraud (16%), phone or utilities fraud (15%), and employment fraud (13%).

---

[89] According to Avira, the most phished brand in January 2011 remained PayPal, followed by other entries (ie. Ebay, HSBC Bank, Chase Bank, etc)
http://techblog.avira.com/2011/03/12/phishing-spam-and-malware-statistics-for-february-2011/en/

[90] http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf

[91] http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf

[92] UNODC, The Globalization of Crime - A transnational organised crime threat assessment (2010) at
http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

[93] http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

67. Also, the German Criminal Police noted that in addition to phishing in relation to online banking (2,923 cases recorded in Germany in 2009), modi operandi include "carding", that is the use of fraudulently obtained credit/debit card information for fraud (53 cases), account takeover through the interception of access credentials (617 cases) and the misuse of access data to telecommunication systems (3,207 cases).[94]

68. Identity theft is in many cases closely related to fraud involving payment cards and account take-over.

2.3.1.2 Payment card fraud

69. Types of payment card fraud include:

- Card-not-present (CNP), that is, genuine card details are stolen and then used to make a purchase via the Internet, telephone or mail order. In the UK, CNP fraud accounts for more than half of losses through plastic card fraud (UK£ 266.4 million out of total losses of UK £440.3 million in 2009); most of it committed via the Internet.[95]
- Counterfeit cards fraud occurs when a fake card is created using compromised details from a magnetic stripe of a genuine card". In the UK, this type of fraud amounted to UK£ 80.9 million in 2009. [96]
- Lost or stolen cards that are used in shops not requiring PINs or to commit CNP fraud.
- Card ID theft includes the opening of an account in the name of somebody else with stolen or fake ID documents ("application fraud") or taking over the credit or debit card account of another person pretending to be the genuine cardholder ("account take over")
- Mail non-receipt fraud means that cards are stolen while in transit from the sending company to the genuine card holder.

70. Related criminal conduct includes:

- Skimming/cloning where individual card details are captured ("skimmed") and either sold or duplicate cards are produced ("cloned"). Skimming can take place in several locations including at ATM machines and at points of sale due to either technical compromise or staff collusion.
- Data breaches where personal identifying information (card numbers, names, addresses, etc.) is stolen in large volumes from e-commerce merchants, shipping businesses, banking institutions and other online payment platforms.
- Stolen card details are sold in batches with US$1,000 for 100 card numbers being a typical price.

---

[94] http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_2009.pdf

[95] See: Financial Fraud Action UK (2010): FRAUD THE FACTS 2010 - THE DEFINITIVE OVERVIEW OF PAYMENT INDUSTRY FRAUD AND MEASURES TO PREVENT IT (http://www.ukpayments.org.uk/files/fraud_the_facts_2010.pdf). An important share of the fraud on UK cards was committed abroad (UK£ 122.7 out of UK£440.3 million in 2009), primarily in the USA (UK£ 21.4 million). Overall losses are reported to have decreased by 28% compared to 2008. While this report notes a decrease of 19% in CNP fraud losses compared to 2008, VISA Europe reports a steady increase in CNP fraud, while other types of card-fraud are declining (Source: Meeting at the Council of Europe on 22 July 2010).

[96] Financial Fraud Action UK (2010) (http://www.ukpayments.org.uk/files/fraud_the_facts_2010.pdf). This type of fraud decreased by 77% since 2004.

- The stolen card details are often used online to purchase high tech accessories, computers, jewellery, fashion accessories etc. These items are then typically reshipped by mules operating in various countries to the criminals.
- Another process exploited to take advantage of stolen credit card details is to create a listing on an auction site for a high value item at a low price. The winner of the auction then pays the criminal for the item, which the criminal then purchases buys directly from the manufacturer using the stolen card details.
- Illegal proceeds generated through the use of stolen card details are laundered through a large number of online payment and financial institution accounts and subsequently sent via wire transfer to the criminals by mules.

2.3.1.3 Online banking attacks, misuse and account take-over

71. A wide variety of attacks and misuses of online banking facilities have been reported.

72. The most commonly reported attack vector is phishing. The general form of a phishing attack involves customers being tricked, through various means, into visiting a fake website, allegedly belonging to the bank. This can be done both via email and via the telephone. The customer then enters his or her online banking credentials into the fake website where they are recorded by criminals and subsequently used to take over the customer's account.

73. Most commonly, phishing attacks are untargeted and carried out by sending large volumes of spam mails. However highly targeted phishing attacks have been observed where individuals or small groups will be contacted. This is known as "spear phishing".

74. Another technique, known as pharming, also involves the redirection of the customer to a fake website. This process works by interfering with the process used by computers to determine the IP address for a particular website. The customer's PC or broadband router can be compromised and reconfigured to intercept requests for online banking websites, sending the customer to the fake website rather than the legitimate one.

75. Another technique is the use of banking Trojans, that is malware that captures the communication between the customer and the online bank ("man-in-the-middle-attacks"). The captured account details are transmitted to the criminals. Alternatively, additional instructions can be injected by the Trojan into the customer's logged in banking session. This will deceive the banking computer to issue authorisations since the injected instructions appear to be originating from a legitimately logged in customer.

76. Once the customer's account has been taken over, criminals exploit the compromised account in various ways:

- Money can be transferred out of the customer account which involves the setting up of a new beneficiary account, usually a mule account, and transferring funds from the compromised customer account into the mule account.
- Applications for credit/debit cards in the customer's name can be submitted, leading to cash withdrawals, or point of sale or Internet purchases from the compromised account.
- The compromised account can also be used as a mule account.

77. Finally, weaknesses in the online banking infrastructure can be exploited leading to compromised customer details.

2.3.1.4 Mass-marketing fraud

78. "Mass-marketing fraud" refers to "fraud schemes that use mass-communications media – including telephones, the Internet, mass mailings, television, radio, and even personal contact – to contact, solicit, and obtain money, funds, or other items of value from multiple victims in one or more jurisdictions".[97] It includes schemes such as advance-fee fraud[98] or "419 fraud"[99], lotteries[100], price-winning schemes and others.

79. Mass-marketing fraud may target large number of Internet users for relatively small amounts of money or specific victims or groups of victims for large amounts of money per victim. Losses are estimated to amount to several billion Euros.

80. Mass-marketing fraud is often committed by criminal enterprises with information technologies allowing them to operate and target victims globally. Resources used include legitimate business services (such as mailing houses), lead lists with contact information (for example from direct marketing companies), payment processors, communication tools, fraudulent identity and fraudulent financial instruments. Mass-marketing operations and identity theft are thus connected.

81. The International Mass-Marketing Fraud Working Group notes that money laundering is a critical component of various mass-marketing fraud schemes. Victims may be requested to make payments via cash-based methods (checks, money-orders and others), investment fraud schemes tend to involve apparently legitimate bank transfers, while West African groups rely on wire transfers with funds being collected by using forged identification. Payments are channelled through several jurisdictions to avoid tracking. The International Mass-Marketing Fraud Working Group furthermore sees an:

> "increasing exploitation of fraud victims to receive and launder victim funds, or to receive and disburse counterfeit financial instruments. A typical mass-marketing fraud scheme, for example, may recruit individuals to work in such varied capacities as collecting wire transfers, depositing checks or shipping counterfeit checks to other victims, accepting deliveries of merchandise purchased with stolen credit cards, forwarding funds and products overseas, and serving as business account agents for foreign companies."[101]

82. For the US Internet Crime Complaint Center, with 9.8%, advance-fee fraud was the third largest category of complaints received in 2009.[102]

83. In the UK, losses due to mass-marketing fraud were reported to amount to £ 3.5 billion in 2006, affecting an estimated 3.2 million adults.[103]

---

[97] According to the International Mass-Marketing Fraud Working Group (June 2010). http://www.fincen.gov/news_room/rp/reports/pdf/IMMFTAFinal.pdf

[98] For a description see: http://www.consumerfraudreporting.org/nigerian.php

[99] Article 419 of the Criminal Code of Nigeria criminalises such conduct. For more information see the Economic and Financial Fraud Commission of Nigeria (http://www.efccnigeria.org).

[100] For a description see: http://www.consumerfraudreporting.org/lotteries.php

[101] http://www.fincen.gov/news_room/rp/reports/pdf/IMMFTAFinal.pdf, page 22.

[102] http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

[103] UK Threat assessment of organised crime 2009/10, page 57 quoting a report of the Office of Fair Trading. http://www.soca.gov.uk/about-soca/library

84. Re-shipping fraud is a variation whereby individuals or small businesses are tricked into re-shipping goods to countries with weak legal systems. The goods are generally paid for with stolen or fake credit cards.[104]

2.3.1.5 Confidence fraud, including auction fraud105

85. Auction fraud is among the most reported offences on the Internet.[106] It involves either the misrepresentation of a product advertised for sale or the non-delivery of goods purchased once they have been paid. Often the payment is requested by cash wire transfer.

2.3.1.6 Investment fraud, including stock market manipulation

86. Stock market manipulation is a deliberate attempt to interfere with the free and fair operation of the market, creating artificial, false or misleading appearances with respect to the price of a traded entity. An example of the types of market manipulation carried out online is a "pump and dump" scheme. These schemes usually involve purchasing a large volume of low value stock and then conducting a spam or telemarketing campaign to encourage the purchase of that particular stock. When the people behind the scheme sell their shares and stop promoting the stock, the price drops rapidly and other investors are left with stock worth significantly less than they paid for it.

2.3.1.7 Pyramid and other multi-level marketing schemes107

87. Multi-level marketing plans are designed to sell goods and services through distributors who are promised a commission for own sales and the sales of others recruited to join the network. Such plans would involve actual products and services, but may also be based on fake products. For example, a pyramid (or Ponzi) scheme requires a financial investment or fee which is returned if additional people are enrolled in the scheme, and not necessarily through the sale of goods and services. The scheme collapses eventually once less people are recruited.

2.3.2 Other proceeds generating offences on the Internet

88. In addition to fraud and financial crime, many other types of crime can be committed and generate proceeds by means of the Internet in one way or the other.[108]

2.3.2.1 Child abuse materials

89. The Internet, including peer-to-peer file sharing networks, has changed the way child abuse materials are disseminated.[109] These materials are no longer accessible to a limited number of paedophiles only. The proliferation of child pornography and other materials appears to generate a

[104] For regional variations see http://en.wikipedia.org/wiki/Internet_fraud

[105] For a description see: http://www.consumerfraudreporting.org/auctionfraud.php

[106] The US Internet Crime Complaint Center lists "non-delivery" as the complaint category most often referred to law enforcement in 2009 (19.0% of all complaints referred (http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).

[107] For a description see: http://www.consumerfraudreporting.org/MLMscams.htm

[108] From drug trafficking, to extortion, trafficking in human beings, dealing in stolen goods (fencing) and many others.

[109] In the early 1990s, research suggested that laws against child pornography had actually been effective and that large scale distribution and commercial child abuse had become rather marginal (http://www.ipt-forensics.com/journal/volume4/j4_2_1.htm). The arrival of the Internet seems to have changee this.

growing demand and thus a growing sexual exploitation of children.[110] An increasing number of sites offering child abuse materials is commercial, that is, fees have be paid, often after a "free tour".

90. In a Canadian study[111] carried out in 2009, 800 commercial sites hosting child sexual abuse materials were analysed. 89.4% of the images showed children under 12 years. They were hosted at 1,091 unique IP addresses. More than 70% of these were hosted in the USA, followed by Canada (8.2%), the Russian Federation (3.7%), the United Kingdom (3.7%) and Germany (1.9%). In Poland, with 80% the largest share of commercial sites compared to non-commercial child sexual abuse websites was noted, followed by Belgium (75%), Singapore (61.5%), Turkey (57.1%) and Italy (54.5%). In the report for 2009, the UK Internet Watch Foundation[112] 48% of child abuse sites were hosted in North America and 44% in Europe, including the Russian Federation. The main top level domains used were **.com** (41%) and **.ru** (20%).

91. However, such data may be misleading:

> "Although it is not explicitly tracked, Cybertip.ca suspects that some websites hosting child sexual abuse images operate on fast flux networks. Fast flux domains use nameservers that supply IP addresses that change quickly and constantly. Typically these are IP addresses of compromised residential computers that are serving the content of the webpage or acting as a proxy to the content hosted at another location. This means that a geographic lookup conducted on a website may provide a different result depending on when it is conducted— even if the lookups occur 10 minutes apart."[113]

92. According to the Canadian study, with regard to paying for child abuse materials, 56.4% of the sites required traditional credit card payment and 33.3% relied on online payment systems. Some 24% accepted multiple methods for payment.

93. The Internet Watch Foundation in 2009 processed 38,173 reports, of which 8,844 sites were confirmed to be related to child sexual abuse. In 2009, 461 identifiable brands were being run as businesses to profit from the sexual abuse of children.[114]

94. Spam seems to be a major vector to attract clients to child abuse websites.

---

[110] To prevent such materials to feed demand, the Budapest Convention on Cybercrime thus in Article 9 under child pornography covers not only actual minors but also images of persons "appearing to be a minor" as well as "realistic images representing a minor engaged in sexually explicit conduct".

[111] Canadian Center for Child Protection 2009: Child Sexual Abuse Images – an analysis of websites by Cybertip.ca (November 2009) http://www.cybertip.ca/pdfs/Cybertip_researchreport.pdf

[112] http://www.iwf.org.uk/media/news.285.htm

[113] Canadian Center for Child Protection 2009: Child Sexual Abuse Images – an analysis of websites by Cybertip.ca (November 2009), Page 62 (http://www.cybertip.ca/pdfs/Cybertip_researchreport.pdf).
See also http://wikileaks.org/wiki/An_insight_into_child_porn for an account on the use of encrypted hidden content server and proxy servers to make traffic between customers and content servers anonymous and unidentifiable. In this way, the server never appears in Internet traffic. Furthermore, legitimate websites may be hacked to advertise child abuse materials or to redirect visitors to child abuse sites. See: http://www.iwf.org.uk/documents/20100511_iwf_2009_annual_and_charity_report.pdf

[114] http://www.iwf.org.uk/documents/20100511_iwf_2009_annual_and_charity_report.pdf

2.3.2.2 Sale of counterfeit pharmaceuticals[115]

95. Counterfeit pharmaceuticals involve medicinal products and medical devices that are falsely represented as regards identity or source. They are highly prevalent in developing countries, but the problem is increasingly global.[116] It would seem that counterfeits are primarily produced in Asia (due to the outsourcing of the production of genuine pharmaceuticals to this region). Counterfeits are often sold in commercial quantities through legitimate distribution chains.

96. The Internet has led to large increases in the sale and proliferation of counterfeit medicines globally. This is facilitated by high profits and opportunities, outsourcing, repackaging and distribution chains, low risks due to weak legislation and slow transborder enforcement, and the involvement of organised crime groups combined with the anonymity, ease of communication and global outreach offered by the Internet.

97. With regard to the Internet the main channels are:

- Internet pharmacies. Research shows that a large share of e-pharmacies sell substandard or counterfeit or unapproved medicines.[117] The money is paid by customers through online payment systems to banks abroad.[118]
- Spam or mass marketing fraud. Messages related to pharmaceuticals reportedly account for 81% of the 183 billion spam messages sent per day.[119] Pharmacy spam operations relying on botnets and bullet-proof hosting[120] and sending tens of millions of spam messages per day are listed among the worst spammers globally.[121] Spammers may send messages on behalf of a particular e-pharmacy or act as affiliate advertisers that receive a commission for each click on a spam message or for actual sales.[122]

2.3.2.3 Violation of copyrights and related rights

98. Information technologies and the Internet facilitate the digital reproduction and dissemination of materials that are protected by copyrights and related rights. Therefore, the Budapest Convention

---

[115] "A counterfeit medicine is one which is deliberately and fraudulently mislabelled with respect to identity and/or source. Counterfeiting can apply to both branded and generic products and counterfeit products may include products with the correct ingredients or with the wrong ingredients, without active ingredients, with insufficient active ingredients or with fake packaging."
(http://www.who.int/medicines/services/counterfeit/overview/en/)

[116] For example, a study in 2009 on the counterfeit market in 14 European countries indicates a value of Euro 10.5 billion per year. http://www.eaasm.eu/Media_centre/News/February_2010
http://www.pfizer.co.uk/sites/PfizerCoUK/Media/Pages/CrackingCounterfeitEurope.aspx
A recent case in the USA: http://news.hostexploit.com/cybercrime-news/4448-online-pharmacies-targeted-for-illegally-distributing-drugs.html

[117] http://v35.pixelcms.com/ams/assets/312296678531/455_EAASM_counterfeiting%20report_020608.pdf

[118] See Moneyval typology study on money laundering and counterfeiting (2008).
http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2008)22RRepTyp_counterfeiting.pdf

[119] According to the Commtouch Internet Threats Trend Report Q1 2010. (www.commtouch.com/download/1679)

[120] Reportedly hosted in Eastern Europe.

[121] "Canadian Pharmacy" was reported to be most voluminous spam operation in 2009. Many gray-market pharmaceutical sellers brand their sites as Canadian to take advantage of the many Americans' belief that medicine in Canada is cheaper than in the USA. In the UK, they may post as "United Pharmacy". See also GlavMed (http://spamtrackers.eu/wiki/index.php/Glavmed).

[122] GlavNed reportedly pays a commission of 30-40% of drugs sold.
http://www.networkworld.com/news/2009/071609-canadian-pharmacy-spam.html?hpg1=bn

(article 10) requires countries to criminalise such violations if they are carried out on a commercial scale. Infringements related to copyrights and related rights generate vast amounts of crime proceeds and are reported to be linked to organised criminal groups.

99. For example, with respect to software piracy on the Internet, the damage is has been estimated to amount to US$ 53 billion for 2008 in direct foregone revenues. This does not include the damage related to cybercrime risks created through unpatched pirate software and the correlation between malware and software piracy, or revenues lost to legal support and distribution services.[123]

2.3.2.4 Online extortion

100. Different techniques are used to extort money from victims through the Internet or other technology. For example, the information system of a public or private sector institution is the threatened target or the threat is about the publication of private or harmful information about a person or institution.[124] With regard to businesses, including financial institutions, extortion schemes tend to involve threat of disruption of networks and websites through denial of service attacks, the theft of information or reputational threats, including website defacement or publicity on security gaps in the IT system or the protection of customer information.[125] Online payment systems are often used in this context for the transfer of the extorted money. Such transactions involve money laundering, as the beneficiary will receive criminal property (ie. proceeds of extortion).

101. Some examples include anti-malware software whereby users are tricked into installing an application that loads a warning that the computer is infected and that users should install a new anti-virus programme[126] which is payable and offers no protection but may on the contrary contain malware or "Hitman scams" in which victims are threatened that they or family members or friends will be assassinated unless they comply with instructions to send money via money transfer businesses.[127] Reports stress that this phenomenon is on the rise, often involving organised crime networks. Unfortunately, this is one of the areas where under-reporting is prevalent and there are no reliable estimates of the scale of extortion.

2.4 Mapping cyber laundering risks and vulnerabilities

102. Due to the rapid growth and technological developments, the payment systems developed tremendously in terms of speed of transactions, number and types of service providers, payment methods, clearing options and even currencies. These new developments of the payment systems offer opportunities for money launderers and render more difficult the detection of potentially suspicious transactions. In addition, cyber criminals combine within for the same schemes both traditional and new payment methods, co-mingling them in multiple operations including cash, bank transfers, pre-paid cards, money remitters, e-currencies and other electronic payment systems.

103. Some payment methods and services can be exposed to a higher ML/FT risk than others, depending on the degree of anonymity of the transfers, the location of the service provider, the segmentation of the agents and sub-agents, the relationship with a credit or financial institution in a jurisdiction observing (or not) the international AML/CFT standards, the quality of supervision, the

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

[124] http://www.cas.sc.edu/socy/faculty/deflem/zInternetextort.html

[125] http://us.mcafee.com/en-us/local/html/identity_theft/NAVirtualCriminologyReport07.pdf

[126] http://www.usprwire.com/Detailed/Computers_Internet/Fake_antivirus_software_take_extortion_scams_to_the_21st_century_109371.shtml or See also Symantec Report on Rogue Security Software (2009) http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr_rogue_security

[127] IC3 Internet Crime Report 2009, page 11. (http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).

AML/CFT rules and regulations in place etc. Different products have different features and those features can lead to designing the risk profile.

104. The FATF, in its 2006 report on new payment methods, had listed four potential ML/FT risk factors in respect of Internet payment systems: anonymous accounts, anonymous funding and receipt of funds (ATM), high or non-existent account funding limit, offshore service providers which may not observe the laws in other jurisdiction. Related risk mitigants included adequate requirements and processes to identify the account holder, to maintain transaction records identifying the payer and recipient, to monitor the transactions and report suspicious activities, to limit funding options, implement account block and limit access to the service. [128]

105. As regards cybercrime and money laundering, the survey responses highlighted in particular the risks listed below.

2.4.1 Technological risks

106. The increased and wide access to fast and modern equipment and connections, and the near ubiquity of the Internet connectivity enhances the ability of the public to initiate a range of financial transactions in an easy and low cost manner. The technical infrastructure is no longer an obstacle for consumers' access to Internet as a valuable information source but equally as an environment for funds displacement from a person to another or from a jurisdiction to another. Also, the software products evolved, creating a friendly interface between the public and the on-line based financial services, so that specific knowledge and computer skills are no longer an obstacle.

107. The coverage of computer network and information technologies is creating an infrastructure for the cross border delivery of products, services and funds for legal and natural persons. The relative easiness with which one is able to carry out cybercrime acts and cyber-laundering is a potential threat.

108. On the other hand, the information technologies have potential applicability to law enforcement investigations and supervision activity, but also offer criminals an easy and low cost access to fast, efficient and increasingly anonymous payment systems. If both criminals and law enforcement authorities could benefit from Internet based payment systems, the knowledge and the ease in using those features could make the difference.

109. From countries' responses to the survey, it resulted that whilst Police and prosecutorial offices tend to have specialised divisions, other law enforcement authorities, financial intelligence units and supervisory authorities might lack sufficient expertise on the functioning mechanisms of such new payment systems. In the absence of proper supervision mechanisms, difficulties in co-operation with public Internet services providers (such as cyber cafés, campus networks) have also been encountered.

2.4.2 Anonymity

110. When initiating a relationship with an Internet based payment services provider, the direct contact between the customers and the operator is either non-existent or minimal. Those services conduct a non face-to face business and as a result, they rarely (if ever) know their customers. Users acquire Internet based financial services through computer terminals and the money inputs and outputs are performed through an intermediary who could be an distribution agent or a bank.

[128] FATF-GAFI - Money Laundering Using New Payment Methods, page 18, October 2006.

111. If the intermediary is a bank, the bank doesn't have any information on the actual transactions, but can only notice the balance (if any) in relation to the cumulative account of the provider.

112. On the other hand, the financial service provider doesn't know the actual identity of the client or the origin of the money, as they are allocated based on an identification code.

113. If the intermediary is an agent (such as retailers selling prepaid cards and cash vouchers), the funding is made in cash and the identity of the customer is even more concealed.

114. Therefore, money laundering risks could be mitigated by restricting funding methods to agents that can be reliable in terms of applying CDD measures, in accordance with the FATF standard.

115. A vulnerability of the Internet payment services providers resides in the fact that some of the operators permit opening of anonymous accounts and transfers between different service providers. Immediately after the opening of the account, the money can be sent anywhere in the world, without the use of the traditional banking system. Moreover a debit or credit card could be attached to the mentioned account.

116. In some cases prepaid cards are designed to afford the customer absolute anonymity while they can be easily be passed on to unknown third parties, who will become the beneficial owner.

117. Anonymous funding methods, along with week customer identification data might result in the lack of or insufficient trail for the transaction and origin and the funds in case of a criminal investigation and could hamper seriously an money laundering and financing of terrorism investigations. In such circumstances, the relevant international standards and related national requirements in terms of know your customer, CDD, and reporting obligations are not adequately implemented by financial intermediaries. Even if some KYC and CDD measures are put in place by a number of cyber-payment services providers, the effective implementation is impeded by the fact that most of the users are occasional clients or they have a short time relationship with the financial entity, unlike in the case of the banking system.

2.4.3 Licensing and supervision limitations

118. Numerous responding jurisdictions indicated that internet based payment service providers are insufficiently regulated and supervised with regards to AML/CFT obligations. Weak or non-existent regulatory controls in the operating environment is a key risk factor for both institutions and jurisdictions, coupled with non-existent or inadequate sanctioning regimes.

119. One of the difficulties in licensing and supervising those entities resides in the fact that often the jurisdiction of registration is different from the jurisdiction of operation. In some cases even the lack of specific legal provisions directed to such payment services suppliers could be an issue.

120. Sometimes, e-payment services providers manage to willingly avoid the legally required obligations by registering in a "lightly" regulated jurisdiction whereas the financial operations are carried out in other countries.

121. Another difficulty in performing a proper supervision of those service providers resides in their virtual profile. There is no corporal exchange office, no boutique, no point of sale. The role of on-side supervision examinations is critical in maintaining the integrity of the financial intermediaries, including the e-payment service providers. The issue is how to execute on-site inspections on a virtual commerce. Moreover, in the event of such inspections, new technological means should be available

for the supervision authority and specialized training should be delivered to the inspectors in order to achieve effective auditing of the record keeping, proper analysis of the internal procedures in place and other AML/CFT obligations.

122. Another issue related to supervision is the legal competence of the supervisory authority over the Internet payment services providers. One perspective is that the country where the servers are located should achieve licensing and supervision over the commercial entity providing financial services. But this optic raises the question of the level of compliance to with AML/CFT requirements of the respective jurisdiction. Another perspective is that the authorities in countries where the financial entity offers Internet services should be responsible for supervision.

123. Licensing is another challenging issue related to Internet based financial services, as the license is given by the state authority responsible in the jurisdiction where the services provider is registered, even if the provider "provides" in totally different countries. The issue becomes even more complicated due to the cross border nature of the various services delivered through the network. A common view should be put in place in this respect, whereby the question of licensing and supervision could be somehow well distributed/divided between the jurisdiction of registration and the jurisdiction of "delivery".

2.4.4 Geographical or jurisdictional risks

124. With the expansion of the Internet worldwide, the notion of distance has become increasingly irrelevant and the wider the geographical reach of the payment system (Internet based or not), the higher the ML/FT risks. Criminals know those vulnerabilities and find innovative solutions to benefit from them.

125. Cross border functionalities render a service quite attractive to launderers as it can also enables payment service providers to conduct their businesses from jurisdictions where they may not be subject to adequate AML/CFT regulation and supervision, and where they may be outside the reach of foreign law enforcement investigations.[129]

126. Still money moves from a jurisdiction to another and actual trends of money flows can be identified. The analysis of the answers provided by countries revealed that some countries are the departure point for criminal money flows, which might indicate that the victims of the cyber attacks are located in those regions. Those jurisdictions are usually located in the western part of Europe or North America.

127. Other countries appear to be "destinations" for criminal money flows, even though it cannot be determined at this point if this is the final destination of the money. Cash withdrawals combined with the use of money mules for the purpose of breaking the trail and dissimulating the trace of the money, impede the clear determination of the final destination of the money.

128. However, from the answers to the questionnaire, it is clear that some countries are used as "hubs" as money flows are constantly directed to those countries, but in the same time, money flows are generated from those countries to other destinations, some of them unusual for cybercriminal attacks.

129. A relation between the destination for the money flows and the origin of the cyber-criminals was indicated by the countries participating to the survey, which suggests that often cyber criminals

[129] FATF-GAFI - Money Laundering Using New Payment Methods, page. 28, October 2010

tend to sent the money to their families and friends located in their countries of origin. It was also indicated that cyber criminals tend to operate in neighbouring countries (as for their country of origin), but also in developed countries even if those are far from their country of origin.

2.4.5 Complexity of laundering schemes

130. Unlike traditional money laundering schemes involving the use of the banking system, cyber laundering relies on various types of operations and financial services providers, ranging from bank transfers, cash withdrawals/deposits, the using e-currencies to money mules and money remitting services. Therefore, the detection and pursuit of the criminal money flows is much more difficult for law enforcement agencies.

131. Often the chain is "broken" by cash operations performed traditionally by money mules followed sometimes by the use of a traditional payment service. If the respective payment service is integrated with the Internet payment service provider, then the money could immediately be exchanged into e-currency ant transferred almost anonymously to other country.

132. Such a sophisticated scheme might challenge a powerful but "traditional" AML/CFT data mining software, based on customer transactional behaviour if part of the money laundering chain is ran in a totally different financial environment.

133. Internet based payment methods could also separate the source of communication of the instructions related to the operation from the actual settlement of the money transfer. This will constitute an additional obstacle for law enforcement officials in the detection phase and when following the criminal funds.

2.4.6 Other risks

134. Specific features of the cyber-payment systems could be risk factors in certain circumstances. The relative easiness of incorporating such a cyber-financial system along with the low cost of business development could lead to questionable profile of the ownership. The speed associated to the operations including in cases of international transfers could facilitate laundering schemes. The low cost of such operations could allow low rates for laundering and could encourage possible criminals in search of legitimising illegal income. The easy conversion to real money and cash in a large range of jurisdictions might represent a vulnerability to money laundering.

3 TYPOLOGIES AND SELECTED CASE STUDIES

3.1 Criminal money flows on the Internet and money laundering methods, techniques, mechanisms and instruments

135. The Internet-based predicate offences described in the previous chapter generate proceeds of crime and often the Internet is the place where the laundering process begins. In this process, the proceeds move from the victim to the offender and from the offender to the other parties involved in the laundering scheme, before the offender is able to fully dispose of these proceeds.

136. The rise of cyber criminals and cyber-criminal organisations is a new challenge for law enforcement officials and other key players. In the ICT environment, new crimes develop or new forms of traditional crimes develop. The increase of the penetration level of the use of new technologies in the economic and social life of a given country is usually directly proportional with the increase of cyber related crimes. Adaptation of the law enforcements techniques to address new technological changes, along with strong knowledge on the cyber payments systems are critical to maintain the investigative capabilities in the new environment.

137. Cyber criminals use the Internet to launder the proceeds of criminal acts independently from ICT (money resulting from tax evasion could be laundered using digital currency) or of cybercrime. Cases received from responding countries indicate that cyber-criminal money, that is proceeds from cyber-predicate offences, is laundered using different techniques, ranging from the use of traditional methods such as the banking system or the money service providers to more complex internet enabled transfers, which often involve organised criminal networks. Most of the criminal proceeds derived from cybercrime are processed as follows:

- they are cashed out after multiple transactions, including with the involvement of money mules to transfer cash or cash equivalents between payment systems in the Internet, "exchangers", mobile payment systems or settlement accounts of credit institutions;
- they are used to purchase highly liquid goods, prepayment cards, etc. for further sale to receive money in cash;
- they may also be used to purchase through the Internet tickets, travel vouchers, home accessories, or other items in order either to keep these or to return or re-sell them and obtain the cash;
- tart of them is often reinvested in developing new capabilities in order to circumvent security technologies.

138. The section below illustrates the most frequently used methods and instruments for laundering criminal proceeds from cybercrime which were identified by countries responding to the survey and as such attempts to illustrate the current vulnerabilities in the global financial system to this type of money laundering. However these should not be considered as being an exhaustive list, as they reflect only the information received and analysed from available cases gathered by the survey at the time of receipt. It also includes several cases detected by responding financial intelligence units or law enforcement authorities' representatives, illustrating the methods used by criminals to move criminal money flows through Internet by means of electronic payment systems, often combined with traditional payment means.

3.1.1 Money remittance providers

139. The majority of the large "traditional" money transmission services, such as MoneyGram and Western Union, provide online services. Some informal value transfer networks and underground banking systems such as Hawala networks also have online presences. The survey replies indicate that the use of money remittance providers is the most common technique for laundering criminal money derived from cybercrime, as 10 out of 17 responding countries indicated it autonomously or part of a more sophisticated scheme.

140. As the overwhelming majority of wire transfers through money remittance providers is paid out in cash, this service enables criminals to introduce criminal proceeds into the financial system. Also, the sheer volume of legitimate cash transactions executed through money remitters provides an excellent camouflage for money laundering activity in the placement stage.

141. The money services have simpler client's identification obligation, and relies on casual business relation with their clients. Simpler procedures in sending-receiving the money, make the money services being used by a wide range of people, from cyber launderers, mules or "financial agents" to less educated people, that find it more difficult to collaborate with an over-regulated financial institution. Often, the money services are just a part of a more complex scheme, where at least one cash operation is involved in order to brake the chain and lose the trace of money. Also, in money remitters schemes, at least one (aware or not) money mule is involved.

142. Money remittance providers offer inexpensive services, and appear sometimes to impose less rigorous AML compliance programs than traditional financial institutions. Usually, the money remittance providers have contracts with banks in order to offer safe and secure contact points with their clients. Often, they are just a part of a more complex scheme, where at least one cash operation is involved in order to break the chain and lose the trace of money, with the involvement of money mules.

143. Almost all responding countries indicated a typology with more or less similar to the following one:

- Fake job advertisements are sent via spam, applicants being recruited by telephone or by other non face-to-face procedures. Often the jobs are related to financial issues or advertise "work at home".
- Criminal proceeds from cybercrime are transferred into the bank account of the mule who is required to withdraw the amount in cash, and subsequently to send it to a specific beneficiary via money service providers, while keeping as payment for this service a commission. The transfers are usually of an amount lower than the reporting threshold, to avoid detection.
- Money remitters are used to move the cash to its final recipient.

144. Some of the identified cases where the services of money remittance providers have been extensively used have raised concerns about the possible collusion or infiltration by organised criminals of such businesses in order to organise and facilitate the channelling of proceeds. [130]

145. Case studies show that :

- money remittance services are used in money laundering schemes related to cybercrime.
- money remittance services are used in the laundering scheme often in relation to money mules.

[130] Money laundering through money remittance and currency exchange providers (MONEYVAL, 2010) at http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/RepTyp_MSBs_en.pdf

- money remittance services are one of the most regulated intermediaries involved in the cyber money laundering schemes and thus should have the capacity of providing valuable information to FIU and other law enforcements in deterring cyber-laundering.

Case study 1 : Credit card information theft and money laundering

Complaints were received from issuing credit card Company regarding fraudulent use of hundreds credit cards.

The common compromising point seemed to be a merchant's POS devices maintenance system.
The audit of the systems revealed the presence of a Keylogger. IP addresses, remote servers and email accounts have been followed and indicators of a perpetrator located in Romania and clones of compromised credit cards used in US were found.

In Romania intrusive measures, upon prosecutor's request have been issued by the judge. The data communication interception has shown that the perpetrator was collecting credit cards sensitive information by using a Keylogger and few collector email addresses. The Keylogger was a customized version of an application downloaded free from the Internet. The credit cards were selected and then sold 1000 USD per 100 pieces* to specific persons located in US. Email communication was found, as well as encrypted Messenger communication, ICQ and Skype.

The Romanian seller gave instructions for the money to be sent on different names in Romania and Bulgaria using Western Union services. As instructed the sender name should have been fakes, for avoiding a direct tracking. Other instructions were for the accomplices in US to send the money to a web money company which was instructed to execute the exchange and then to redirect the results to Western Union services in Bulgaria.

During the execution of the house search warrants there have been found computers used by the Romanian perpetrators, Western Union documentation, and cash. 120,000 USD has been seized

The computer search identified the Keylogger used, data bases with credit card information.
The Romanian perpetrators have been charged for illegal access to a computer system, illegal interception of a computer communication, fraudulent operation with credit cards and money laundering, all in a continuous aggravated form.

Source: Romania

Case study 2: STR report led to cybercriminals' arrest

The FIU received two STRs from a commercial bank concerning several cash withdrawals in small amounts (EUR 500 – 1,000 or equivalent) performed by a natural person A from his bank account. The operations were preceded by bank transfers, justified as "gifts" or "allowance", ordered by four individuals from a foreign jurisdiction.
The bank account held by individual A was monitored for a while, but the bank has not identified other types of transactions.
In the analysis process, the FIU requested information about the payers located in the foreign jurisdiction in question and was notified that one of orders was known to have links with people involved in a criminal group specialized in committing computer crimes. The criminal group's leader was an individual, known by the Police as "Samir". This man along with other co-authors and accomplices were wanted and as a result of extensive actions, carried by a joint task force, eight persons involved in computer crime were arrested.

Facts found in respect of arrested persons:
"Samir" has resided in Italy for a while, where in collaboration with an Italian citizen he had initiated, in legal conditions, a unit of fast money transfer. Once obtaining the licence for his company, he received also the username and password necessary for monitoring the transfer operations (MTCN transfers overview). By these means, he obtained data and information such as: name of the payers, their identification data, the amount of the money transferred, the location of the departure and the destination of the money. This information was used for forging IDs, and significant amounts of money were withdrawn from unit destinations.
In addition to the above mentioned, they cloned the operating system, after installing the license and certificate (based on digital signature), the resulting image being installed on two laptops which kept the same configuration (number, model, technical characteristics). The laptops were sold for 100,000 euro each, as they give the opportunity to the buyers to have access to the same data and information on the persons performing money transfers, as the legitimate licence holders. The case was submitted to the Court.

Source: Romania

Case study 3: Banking transfers, front persons and money mules for money laundering purposes

In phishing/pharming typical cases analysed by the FIU, in the early stages the offender fraudulently obtains the access to the victims' bank accounts using Internet banking services.
For concealing their identity, they contact different people offering money for using their personal accounts for performing transactions.
In many cases, the front persons open a new personal account intended for this purpose and when an external transfer is being made, they declare the funds as their own.
The funds are then transferred further to other accounts or withdrawn in cash. These intermediaries often make use of transfers of the funds via money transfer services.

Source: Slovakia

3.1.2 Wire transfers /take over or opening of bank accounts

146. Even if the new technologies such as the on-line payment platforms or digital currencies gain more and more ground in the day to day economic and social environment, cyber criminals and cyber-launderers are still dependent on the banking and financial system.

147. Wire transfers are a fast and efficient instrument for money launderers and are used most commonly at the beginning of the laundering process, as often the cybercrime itself consists in extracting money from victims' bank accounts using fraudulent techniques. Following this stage, the money is quickly transferred into the recruited mules' accounts and from there they are withdrawn in cash and/or forwarded to other destinations. If sent to other jurisdictions, transfers that are made are often of small amounts, below the reporting threshold, to avoid having to justify their origin.

148. Cases were reported where a number of transactions were made to conceal the illegal origin of the funds. In some cases, it was determined that perpetrators used several on-line banking accounts. Sometimes, the cyber-launderers execute hundreds of meaningless transactions across various bank accounts, followed by a limited number of cash withdrawals. In such cases, it is believed that all the on-line banking transactions have been carried by one mastermind in the background of the operation, while the cash withdrawals are entrusted to low profile members.

149. In other cases, bank accounts have been taken over by an attacker can be used as a "mule" account, most of the times, this being done without the knowledge of the account holder.

150. Case studies show that :

- most of the times, the banking system is the target of cybercriminals, and it is also used in money laundering process.
- cyber criminals are still depending on the banking system so strengthening the AML culture in relation to cyber attacks and cyber laundering features, could lead to limiting the phenomenon.
- The wire transfers are used in combination with other techniques.

Case study 4: Phishing and money laundering using bank accounts

A criminal group gathered user data and passwords by using keylogger type viruses. Botnets were widely used. Using the stolen data, money was extracted from victim's bank accounts. Subsequently, the money followed a series of bank transfers and at the end of the chain the criminals performed cash withdrawals. In some cases the stolen assets were converted into e-currency and back.

Source: Estonia

Case study 5: Embezzlement on bank accounts

Two nonresident companies (Invest1 and Invest2) transferred funds in small amounts (100 - 200 USD) from country "Z" to an account opened with "Bank U" by the non-resident "Y" with a purpose of payment "aid to relatives".
After the successful funds' transfer from accounts of companies Invest1 and Invest2, transfers of larger amounts of funds (200-300 thousands USD) were made. These funds were transferred to the same bank account, and when a sufficiently large amount was reached, the client "Y" tried to withdraw money in cash.

"Bank U" monitored these transactions and requested additional documents to client "Y" in order to clarify the purpose of the money transfers. The bank stopped the outgoing transactions on the account for 2 days. Also, "Bank U" reported the case to the FIU.

Based on the financial analysis performed, the FIU decided to prolong the withdrawal suspension period for 5 working days. During the analysis, it was established that the money was illegally transferred from accounts of Invest1 and Invest2 and that there was an unauthorized access to the accounts of these companies through their IP addresses (place of residence – country "Z"). It was identified that the non-resident "Y" has several passports. According to the correspondent bank information, the money transfers were illegal and the payer's bank asked for the return of the funds. During this period of time, an email was sent by unknown person "N" to "Bank U" with attached copies of contract with the purpose to confirm the legitimacy of the money transfers (contract of financial aids from companies Invest1 and Invest2 to citizen "Y"). After the analysis of the contract sent by "N", the name and surname (second name), as well as a nick-name of the email's sender were established. The IP address of email sender was identified. Also, through social networks, it was established that "N" is a friend of a "Bank U" employee, a CV was found etc. In addition, during the information exchange with counterparts, it was established that "N" was under suspicion on fraud operations.

Conducting further investigation, the FIU received information that computers of companies Invest1 and Invest2 were infected by a virus Trojan Spam Malware that contained harmful software. This virus was launched to receive an access to the companies' software and to control the online account of companies Invest1 and Invest2.

Source: Ukraine

Case study 6: Internet fraud and money laundering using front persons

The case illustrates cyber fraud followed by money laundering and involving an organised group which misused the Internet for committing criminal activities and opening bank accounts in several EU member States.

The criminal group created websites for Internet sales or made use of existing web pages (such as E-Bay), opened personal bank accounts in financial institutions within EU Member States requiring as services Internet banking, SMS notifications and issuance of debit card. The typical goods sold via Internet included electronics such as iPods, mobile phones, navigation systems, used cars, tractors or caravans. The suspicion arose from the low price and communication via email or the use of pre-paid SIM cards. They also sent fraudulent banking confirmations as well. The criminals asked for the payment to be made into an account opened in another EU country. These accounts were opened in those countries by front persons with low social status.

Once the payment was made, the money was withdrawn in cash by the front persons or immediately transferred to the account of another criminal group member. After few such transactions, the accounts were closed. The front persons used for opening those accounts were alternated.

Source: Slovakia

3.1.3 Cash withdrawals

151. The increased transparency associated with wire transfers and recently with money remitting services is a factor determining money launderers to consider cash a key element in moving assets and disguising their traces. Cash clearly remains a part of the cyber-laundering chain according to the countries' responses to the questionnaire, and it could be identified in all three stages of the money laundering process.

152. In some instances the proceeds from cybercrime (for example in the case of card-related fraud), is immediately withdrawn in cash from the ATM, in relatively small amounts. From this point the laundering process begins.

153. The same procedure is applied in the case of "phishing transfers" that are made to accumulating bank accounts hold by the financial agent. The financial agent withdraws the money – deducting his commission - in cash. He subsequently purchases anonymous credit vouchers of an Internet payment system at various issuing offices (like petrol stations, kiosks) in relatively small amounts (less than 500 €) (Germany).

154. Another identified typology mentions the cash withdrawals as part of the layering stage, as wire transfers are followed by cash withdrawals and the rest of the money laundering scheme continues in various ways, such as with the use of money remitters, currency exchange etc.

155. In other cases, the money is cashed out after multiple transactions, including those involving money mules, in order to transfer cash or cash equivalents between payment systems in the Internet, "exchangers", mobile payment systems or settlement accounts of credit institutions (Russian Federation).

156. However, apparently, for cybercriminals, cash has a number of shortcomings such as the necessity of direct contact between traders, the weight of large amounts in small notes or the need of physical movement of the notes by a carrier in exposing circumstances, such as the cross border transportation where police and custom checks could be performed. Another constraint is related to the distance between the participants in the transaction. But probably the most important downsize

that it cannot be stolen by cybercriminals in the form of banknotes. The cyber-attacks by "definition" are targeting more subtle forms of value, such as bank accounts, IPS accounts, e-currency etc… The cyber criminals are not pick-pockets, they do not steal paper money because they activate in a different line of business. However, they use cash to disguise the money trail. Cyber criminal cash is presented in relatively small amounts and is used in money laundering schemes in a way opposite to smurfing. The small amount of cash is withdrawn from bank accounts or sent via money remitting services, in order to be forwarded to "accumulating" accounts.

157. Case studies show that :

- Cash manipulation is a compulsory stage in a cyber-money laundering scheme;
- ATM are often used in cash withdrawals, to avoid personal contact with bank employees;
- The main target in cash interference in a money laundering scheme is concealing the trace of the funds.

Case study 7: International phishing attack using bank accounts and cash withdrawals

Using phishing attack or other type of stealing of credit card ID, the offender transfers small amounts of money from targeted accounts in favor of his personal account or account of a company controlled by him or on behalf of which he/she is empowered to perform financial transactions in another country. Subsequently the offender quickly withdrawals the money in cash using ATMs in a different jurisdiction from the one where the stolen money was transferred. He could make several other transactions in order to disrupt the identification of cash tracking.

Source: Bulgaria

Case study 8: Organised crime group specialised in fraud on money remitting services, phishing, fraudulent use of credit card information and forged credit cards

Police intelligence led to the identification of an organized criminal group in a large city, specialised in ATM manipulation and fraud. The intelligence was validated by additional information received from the FBI attaché, regarding electronic payment system fraudulent transfers.

Subsequently, a major bank and its clients became victims of a phishing attack, consisting in cash-out from ATMs in two major cities of the country. Additionally, police information and ad hoc police survey led to the detection of a fraudulent skimming device installed on ATMs in a third important city. Information gathered conducted to the conclusion that the perpetrators involved belonged to different criminal groups, but worked together in some instances.

The investigation determined that the criminal activity of the groups consisted in phishing (targets and instrument used were identified), fraud on money remitting services, fraudulent use of credit card information and forged credit cards, manufacture of skimming devices and their use for collecting personal identification data and passwords.

Source: Romania

3.1.4 Internet payment services

158. The expression 'internet payment services' (IPS) is generally used to describe Internet banking-style transfers (payment services that rely on a bank account, the Internet being only the channel used to give order for the money movement from the payer to the beneficiary) and other payment services provided by a non-bank institution operating exclusively on the Internet and that are indirectly associated with a bank account.

159. In case of IPS bank account related, the transfers are performed similarly to any bank operation, the only specific feature being related to the location of the bank customer in front of the computer and not in the bank's offices.

160. The non-bank IPS (such as Pay Pal) offer to their customers a range of services of fund transfers including cross border transfers, on line shopping, participation to on line auctions etc. Some non-bank IPS allow customers to hold accounts, in which case they may pool those customers funds into a single bank account, held in the name of the service provider. In that case, the bank holding the IPS' account may have no direct relationship with the service provider's individual customers, in which case identification or CDD measures in relation to the individual customers are not performed.

161. As the responses to the questionnaire revealed, the use of internet payment services in responding countries is on the increase, thus raising issues of an increased risk of misuse for ML/TF purposes and specific vulnerabilities rendering possible ML both in the context of the placement and layering stage. Often, the conversion related to the electronic payment systems is an important part of the layering stage. Such services allow customers to send or receive funds through a virtual account accessed via the Internet. Such services have sometimes a high degree of anonymity and are increasingly used to support person-to-person transfers.

162. Although IPS offer a cheap, anonymous and very quick method for international money transfers, they may not be subject to the same AML/CFT measures and supervision as the credit and financial institutions, which makes them vulnerable to money laundering risk. Even though IPS are offering financial services to their customers, not all suppliers are subject to AML/CFT regulation.

163. One "chartered" system of laundering money by using Internet payment platforms is that the money derived from various cyber-offences is wired to the bank account of the financial agent or money mule, followed by a cash withdrawal. Subsequently credit vouchers of an Internet payment system are purchased without the obligation of the seller to identify of the buyer. In this way, real money is converted to virtual money. The financial agent sends the voucher number by e-mail to the person giving instructions. Subsequently, the PIN can be used for Internet payments of goods and services, poker, casino and gambling websites on the Internet. Several vouchers for smaller amounts can be used jointly and combined. A conversion to other digital currencies by using various exchangers acting on the Internet is also possible. (Germany)

164. Sometimes the criminal funds are deposited into accounts of such entities, from which the money is used to buy products and services on Internet auctions. Although the payment services guarantees safety, the transactions cause a risk of fraud due to the impersonal nature of Internet commerce and the gap in regulatory treatment by jurisdiction. (Poland)

165. A recent development relation to IPS is that they become increasingly interconnected with different new and traditional payment services. Funds can now be moved to or from a variety of payment methods, ranging from cash, money remittance businesses, digital currency, wire transfers or credit cards. Furthermore, some IPS providers have started to issue prepaid cards to their customers, thus granting them access to cash withdrawals through the worldwide ATM networks.[131]

166. Depending on the legal requirements on the jurisdiction where the IPS is registered, they might be regulated as money services businesses and required to have AML/CFT compliance policies and regulations, maintain certain transactional records and report suspicious financial activity.

167. Case studies received show that :

[131] Money Laundering Using New Payment Methods – FATF Document, October 2010

- IPS accounts and transactions can be misused for fraud and money laundering purposes in a similar manner as the bank accounts
- Due to the link between bank accounts and IPS accounts, preventive measures taken by the banks could have positive effects on IPS
- The use of relatively small amounts is typical for fraud and money laundering using this technique

Case study 9: Identity theft and money laundering

A Pay Pal account was opened in a branch of a foreign bank. The account was debited with many transfers into accounts of a number of beneficiaries (according to order).

Modus operandi of the shady business consisted in changing middle (i.e. from 12th to 17th) digits of the account, checksums (check digits), names of beneficiaries and their addresses, while the last 9 digits and the bank code (digits from 3rd to 11th) remained the same. There were a few (max. 10) transfers, the value did not exceed 3000 PLN (equivalence of ca 1000 USD).

After a couple of days, the accumulated funds were wired into accounts of a few organizers or were withdrawn in cash.

As it was established, the funds originated from the American Pay Pal accounts belonging to different individuals. Having stolen their identity (identity theft), the criminals opened Pay Pal accounts on their behalf, then a motion to open a credit line was made on the behalf of victims. Material was sent to public prosecutor's office.

As a result, the bank implemented a system of automatic verification of the beneficiaries' accounts in case of incoming transfers, and this preventive measure forced offenders to change their modus operandi. The criminals started to open lots of Internet-access accounts in different banks (a record-holder opened 1 main and 261 auxiliary accounts). The accounts were credited with wire transfers coming from the Pay Pal account. Accumulated funds were transferred into accounts of few organizers from which were withdrawn in cash.

Follow-up material was sent to the Public prosecutor's office. 48 accounts belonging to one of the criminals were blocked. Police found out that the shady business was organized and controlled by a person who was a sort of specialist in banking and/or IT systems. The participants lived in the same district of the town and were well-known to the local police. As for the technical details, the identity theft crime was committed using botnet.

Source: Poland

Case study 10: Use of digital goods and defrauding their seller in a way that allows criminals to obtain directly legitimate funds

The victims: a set of Credit Cards holders, an e-payment company, and a VoIP Company

The scheme: Fraudsters own several companies that offer Premium Phone Numbers. They set a large number of relays around the world, mostly in poorly regulated countries, and they start calling these relays from zombie PCs', using VoIP accounts funded with fraudulent Credit Cards used through the e-payment system.

Comments: The calls generate actual revenue for the Premium Numbers' providers. These companies can legitimately assert that they have no ways to check that calls to their destinations are fraudulent or not. Moreover, if these calls come from all over the world, it is very difficult to find a commonality.

The e-payment system sees transactions with VoIP providers, but has no way to check if these are fraudulent or

not, beyond its usual anti-fraud checks. And the VoIP Company sees only the relays, but not the final destinations. If the relaying infrastructure is built prudently enough, there is almost no risk for the fraudsters to be uncovered.

And as a result, from an ML/TF perspective, we have the proceeds of a crime, the theft of Credit Cards details, which are transferred to the legitimate economy of a given country without having to go through the Financial System, and be exposed to its anti-money-laundering controls.

3.1.5 Money mules

168. Money mules are an essential element of a substantial number of criminal operations on the Internet as pointed out by most respondents to the questionnaire. According to the survey, the « mule » is an individual recruited through the Internet, who is requested to open a bank account whereby he/she will act as an intermediary for cash recovery of the dirty funds obtained by cyber-pirating (*phishing, keylogging, scam*). The mule would then transfer the remaining money to other accounts or abroad via wire transfer while keeping a commission. Mules receive in their bank accounts funds from, for example, a compromised online bank accounts and can either forward the funds to other accounts or withdraw the funds as cash and subsequently using another means such as a money transmission system or digital currency. The mule keeps a commission as part of the transaction.

169. Often, the mule and the victim whose bank account is to be defrauded, live in the same country. For each transaction, the mule receives a commission which was estimated as ranging from 5 to 10 percent of the total of the laundered amount (which will also allow the perpetrator to blur the links) and is required to transfer the remaining sum via a web-money service. However, several cases have shown that this percentage seems to have increased over the years, ranging from 30% to 50% in certain cases, probably due to the increased risk of being detected as a result of an increased efficiency of enforcement agents' action or possibly as raised by some persons, the difficulty of recruiting a sufficient number of mules on the market.

170. The mule is often described as a credulous individual who is deceived by the professional contacts with his "employer" and believes that he or she is working for a legitimate company. But this naïve image has now more and more been questioned by the police bodies and bank officials, as there have been numerous instances where it became apparent that the mule was fully aware of the illegal nature of his/her deeds.

171. There are several scenarios through which mule accounts can become involved in handling proceeds of crime. The account holder may be fully aware of the true nature of the funds and the true purpose of their actions or they may not. In cases where they are not, the mule has been contacted as a result of a legitimate recruitment website where roles such as "financial manager" or "work at home" positions are advertised. Spamming services are also used to advertise for potential money mules.

172. After recruiting the mules, the money is sent into their accounts with different orders. They can be instructed to transfer the money to an account abroad, to transfer the money to a tame account in the same bank during weekend, to take out the cash from an ATM – using the card usually for less than an hour, to move the criminal money forward using the remitting to it final destination.[132]

173. The number of mules increases directly proportional with the Internet fraud. If the "employer" will appreciate that the mule is not behaving as a "money laundering specialist", it will use him/her only few times so that the amounts gained will not be higher than 3.000 USD.

[132] Hungary.

174. However, some cases reported show also that money mules operations can involve a certain level of complexity as far as the structure is concerned, with several levels of mules and duties. Also, apart from "one-time" mules, which includes case cases where individuals believed to be involved in a work-at home scheme, there appears to be a growing class of professional mules that knowingly develop a lucrative business from such schemes.

175. Case studies and information received indicate that :

- money mule activities are often part of a wider and more complex money laundering scheme and can be a weak link in the cybercrime laundering process.
- their activities can be detected and be linked to identify transnational criminal operations as well as botnets and servers used for criminal purposes.
- the mule's activities have a series of typical features that make them vulnerable to identification by bank's staff, though transactions require close scrutiny as the amounts involved are quite small.
- money mules recruitment takes place in the majority of countries and is no longer primarily concerning less developed countries, this trend being explained as potentially resulting from various factors (i.e. consideration that a transaction from a person/money mule from a developed country would attract less attention in transaction scrutiny, global financial crisis, lack of sufficient number of money mules).
- international financial investigations combined with high-tech crime and cyber-forensic investigations appear to be the most effective way to achieve impact.

Case study 11: Automated Clearing House (ACH) fraud and money laundering using botnets and money mules

In March 2009, in the USA, apparently unrelated intrusions into two county school computers (the system of the country Treasurer and in a county college system) with a combined loss of more than US$ 790 were reported to the Internet Crime Complaint Center (IC3).

In one case, money was transferred to seven individuals who were confirmed to be money mules who had been recruited via seemingly reputable job hosting sites. Further IC3 analyses revealed that more than 200 complaints were linked to these mules.

Additional analyses by the National Cyber-Forensics Training Analysis (NCFTA) found that the Internet Protocol addresses from where the victims' computers were accessed were part of the Ligat botnet. This established a link between these cases as well as other intrusions in which the stolen credentials of victims were used to authorise ACH transfers. The analysis of IP addresses linked to the Ligat botnet revealed further connections to pharmaceutical spam operations to infect computers with malware, and to an underground carding forum and credit card dumps.

The following method was used in these ACH fraud cases:

- Targets were small businesses, schools, agencies of cities, counties and states
- Computers were infected with malware via spam sent via the Ligat botnet through which they became part of this botnet
- Stolen credentials were used to authorise ACH transfers
- The money was transferred to mule accounts
- The mules had been offered jobs by email after they had posted their CVs on reputable job posting sites
- Front-companies offered work-at-home employment
- ACH transfers were made to seven to nine mules with each transfer under US$ 10,000
- The mules then conducted wire transfers to two or three individuals with each transfer remaining under US$ 3,000. The transfers were sent repeatedly to several countries (ie. Czech Republic, Moldova, Russia, Tajikistan and Ukraine).
- Mules had access to an online "task management service"

- The "task manager" instructed the mules which wiring company to use, bank account to open, names and locations to transfer the money.

Source: Contribution by public sector

Case study 12: Home banking fraud and money laundering involving botnets, mules and VOIP

A bank offers online banking services to their customers, so that they can manage and make transfers from their homes via computers. Some customers had their account "hacked" and money was transferred from their account to accounts in other countries. The computers of the victims had been infected with malware which allowed the theft of account credential and other personal information (probably as part of a botnet). The international investigation conducted in the involved countries revealed a large and complex system of money mules spanning at least ten countries and large amounts of stolen money.

Mules were recruited via spam in different languages offering easy gain of money. Those who responded were contacted by telephone via Voice-over-Internet-Protocol (VOIP) which is difficult to intercept and for which bills had been paid with skimmed credit or stolen debit cards. The "first level" mules were asked to open a bank account. Within a few days they received money on this account. They were contacted again and instructed to withdraw the money and transfer it via money remittance providers to a given address in Eastern Europe jurisdictions. In Belgium, this breaking of the paper trail is considered money laundering.

The "second level" mules, in this case most of them located in Eastern European jurisdictions, withdraw the money and give it in cash to a third person, the "money collector". Neither the first nor the second level mules know any details about the origin of the money. The money collector is electronically informed about the amount to be received, the transaction code of the money remittance provider, and of the name and address of the first and second level mules. The money collector transfers the money to a fourth person, the e-banker, who converts it into Web money. In the case investigated, the money collector received US$ 150,000 within two months.

All these processes appear to be very well organised and automatically followed up, so it can be assumed that the organisation involves a central data manager or similar.

Comments:

- This case comprises computer data and system interference into computer systems, illegal interception, forgery and fraud, money laundering and organised crime.
- The fact that apparently unrelated minor cases of online transaction fraud were all related and part of a complex transnational criminal operation became only visible when several prosecutors and police authorities investigated their cases and made contacts with counterpart services abroad. Joint investigation teams (for example through Eurojust) in this context prooved very useful.
- In Belgium, contacts and information exchanges were established between the prosecution, police, financial intelligence unit, money remittance providers, banks and Europol. Information was gathered and analysed by a multi-disciplinary team of financial and high-tech crime investigators.
- Investigating money mules seems to be the most promising point of entry to uncover complex criminal operations.
- Following the money trail, that is, financial investigations, are as important as carrying out high-tech crime investigations and computer forensics, and the success appears to come when combining both.
- Even though VOIP is difficult to track, companies such as SKYPE may have details about a fixed telephone line or an address to which an invoice is sent and that is connected to a VOIP account.
- Furthermore, servers hosting criminal web sites should be investigated. In this particular case in Belgium, the server investigated hosted a site that directed criminals to other sites offering tools for "hacking" into the systems of specific banks and lists of potential money mules that had responded to spam.

Source: Belgium

3.1.6 International transfers

176. The international transfers could be analysed as a variety of bank transfers, but since the recent new payment methods development, in fact, international transfers can be performed using bank accounts but also e-currency, Internet payment services or traditional money remitting services as well. Regardless of the payment method, the international transfer of the funds have specific features and vulnerabilities regarding money laundering risks and this method was mentioned separately by the countries participating to the survey.

177. One key problem in relation to international transfers regards difficulties for law enforcement agencies in recovering the criminal assets when jurisdictional issues arise.

178. The international "shipment" of the money is usually a part of the layering stage, and follows after operations previously carried out, for example, the use of money mules.[133]

179. In terms of international transfers, it is often that several countries participate in international-scale arrangements. For this reason it is hardly possible to identify the criminal who "leads the game", who has invented the scheme and coordinates money transfers.[134]

180. It is also difficult to trace the money once it has been sent abroad. A particular vulnerability was noted in relation to some jurisdictions as regards the fraudulent payments with money subsequently transferred to accounts of companies residing in off-shore zones.[135]

Case study 13

The FIU conducted an investigation concerning a fraudulent scheme established by an unknown person who engaged in embezzlement of funds with illegal usage of computers. Further on, the embezzled funds were transferred in favour of a certain natural persons. Available funds on the account of Company X (Country W) were sent by unknown person who accessed to on-line bank account of the victim company via login and transferred unauthorized international transfers to accounts opened by natural persons with an Ukrainian bank.

A series of international payments were performed from Company's X bank accounts (Country W), in favour of a number of natural persons in Ukraine. The unauthorised transfers were performed by an unknown person who accessed the on line bank account of Company X via login. The total amount of the transactions was 577 000 USD.

The payer's bank in Country W revealed the unauthorized transfers and informed the Ukrainian bank. Funds in value of 284 000 USD were successfully returned. Furthermore, there were another two unauthorized transfers to 98 000 USD each from the account of Company Z, that were transferred in favour of these Ukrainian natural persons.

The FIU detected indicators of fraudulent financial transactions in the course of their financial analysis which was performed also using intelligence from international counterparts.

Source: Ukraine

[133] Hungary.

[134] Estonia.

[135] Slovakia.

3.1.7 Digital/electronic currency

181. Digital or electronic currencies refer to a value exchange system that operates electronically. Electronic currency is encrypted code representing the value attached to the certain "account", just as regular banknotes are a piece of paper carrying certain characteristics that transforms it in a symbol of value. Some say that electronic money is real money just as the paper bills are, but in fact they are not as "liquid" as the cash. Electronic currency can only be used in definite circumstances (e.g. need of available technical devices), whilst the cash can be used in any payment operation.

182. Global electronic money transfer services are accessible to people all over the world and make possible to move values from one country to another near instantaneously, sometimes without leaving a trace. Using electronic currency both natural and legal persons can send and receive electronic money in real time. Payments can be made 24 hours a day, 7 days a week, fast, anonymously, with low costs, without leaving the house.

183. There is a wide variety of digital money providers that purport to link their "currency" to various precious metals, and another category that does not explicitly link it to precious metals. Both categories of service providers seek legitimacy and customer trust through the Global Digital Currency Association, a trade association of digital currencies dealers and exchangers pressing for self-regulation. The GDCA provide a public ranking of its membership and offers arbitration procedures. "However the GDCA constitution makes no mention of AML policies and procedures or of adhering to international AML recommendations such as those promulgated by FATF"[136].

184. As stated above, the electronic currency and anonymous payment systems are divided in two categories: the "trust" type and the "precious metal" type. The first one relies on the trust between the seller and the buyer. There is no "exchange rate" for such a currency and it had no value to others but for the individuals and companies that use it. ([137]

185. The second has a guarantee in precious metals attached it is related to the gold value, in order to determine an exchange rate for the electronic currency, such as Egold and Pecunix. Once the conversion is made, the funds and the accounts are impossible to trace. Besides, some companies offer the possibility to link the electronic money account to a debit card that can be used in stores and ATMs identified in the Interac,[138] Cirrus, Maestro and Plus, such as GetEMoney.[139]

186. Cyber criminals and money launderers tend to use systems such as digital or electronic currency which afford varying degrees of anonymity depending upon the issuer, and typically afford them instant clearing and little or no chance of reversed charges. Some of the systems historically used by the criminal underground include, but are not limited to, e-Gold, WebMoney.ru, Liberty Dollar, Pecunix, Liberty Reserve, Fethard and E-Bullion.[140]

187. Similarly, commodity backed alternative currencies such as the liberty dollar are attractive for many of the same reasons. The easy conversion to various virtual currencies and accounts by so-called "exchangers" offers an effective opportunity to criminals to conceal illegal funds.[141]

---

[136] US Threat assessment – Department of Treasury, December 2005

[137] For example webmoney « WMZ », and UKASH http://www.ukash.com/fr/fr/home.aspx (entreprise londonienne)

[138] http://www.interac.ca/fr/about.php (Canada)

[139] http://www.getemoney.com/atmcard.aspx

[140] USA.

[141] Germany.

188. On the Internet sites and forums most frequently visited by cyber launderers are, e-gold, and Webmoney. In some jurisdictions, those businesses are not bound to AML/CFT legal obligations (submitting STRs, performing CDD or reporting operations above a certain threshold).

189. In some jurisdictions e-money payment services can be used anonymously. It should also be noted that e-money circulates outside banks and, as such, outside the bank supervision system. Banks serve as agents, letting the money in or out of the e-payment systems, and in certain cases – as "issuers"/emitters of e-money.[142]

190. There are instances where the AML/CFT legislation does not include e-payment systems providers into the list of entities that carry out operations with monetary and other assets and, as such, they are not subject to the above-mentioned relevant AML/CFT requirements. These gaps allow for the use of electronic money for legalization of proceeds from fraudulent transactions in the Internet (such as financial pyramids, personal data theft of Internet users owning bank cards or e-purses with the possibility to further use them for illegal financial transactions), illegal dissemination of no-license products in the Internet, stealing money from bank accounts (by breaking banks' software), stealing money from e-purses of customers of the Internet payment systems, illegal activities off-line (misappropriation of budget funds, illegal activities, etc.).

191. Organizers of e-payment system carry out virtually no control over their clients' activities who provide goods and services on-line. That provides for favorable conditions for illegal and shadow activities in the Internet.

Case study 14

The Ministry of the Interior received information from WM Transfer company that an unidentified user of their system violated the contract with the administrators of system and committed stealing of funds to the amount of $60 000 from the company's account, and opened in US payment system E-GOLD. The offender replenished the account of a credit card using the WM Transfer payment system service, and then cashed in the money.

Law enforcement agencies detained an individual who attempted to receive money of the amount of $14 000 in a bank, illegally using the passport and payment card of another person. The passport, sim-cards for mobile phone and bank payment card were confiscated. An IP address was identified, through which an illegal access to Internet and use of computer equipment were conducted. The equipment was used with a purpose to appropriate one's property (title marks of "exchange office" purse) involving fraud.

As a result of the investigation, the Ministry of Interior initiated a criminal case under Article 361, Chapter 2 of the Criminal Code. Two individuals were apprehended: a person of Caucasian region, who organized the withdrawal of money through the ATM network using counterfeit and lost passports of citizens of Ukraine; and another person, who was convicted for a term of 3,5 years for committing an analogical offense and was released due to the probation period. The criminal case with indictment was forwarded to court.

Source: Ukraine

3.1.8 Purchase through the Internet

192. The relationship between on-line payment services and on-line merchants is of a bilateral nature. The payment services are emerging globally in response to the market demand on on-line shopping offers. Returning the favour, the on line merchants are expanding as well, due to the easy

[142] Russian Federation.

and cheap access to the on line shopping settlements provided to the customers by on line payment services.

193. Individuals wanting to shop online or to participate in an online auction can use an existing bank account, credit card, wire transfer, money order, and even cash to fund an account with an online intermediary that will facilitate the payment. Some online payment services exist to facilitate transactions for online gambling and adult content sites that other money transmitters typically will not service.[143]

194. Using cyber money into the virtual market-place seems to be a logical aftermath for the perpetrators. Usually this technique is located at the end of the cyber laundering scheme, in the integration phase but occurs also at the layering stage, when the purchase is followed by a subsequent sale.

195. The on-line auction sites are a favourite tool for buying high value-goods (Russian Federation), or services flight tickets (Albania). A specific aspect to illegal purchases through the Internet is related to counterfeit pharmaceutical products and sales of high risk or illegal items - such as prescription drugs, firearms, suspect child pornography, multi-level marketing (pyramid or Ponzi schemes), escort services, tobacco sales, drug precursors, stolen credit cards and credit card information. Money transfers performed in relation to such transactions are particularly vulnerable to money laundering. Also, a particular risk for money laundering is associated with virtual gaming and payment made in relation to such services providers.

3.1.9 Shell companies

196. Cases also reveal the use of shell companies in this context. Shell companies offer large opportunities for cyber money launderers, and appear to be used primarily at the layering stage. Shell companies are enterprises without any business activity, assets and liability. But such an entity possesses a number of bank accounts often conveniently located in offshore jurisdictions. Their role is to offer a reason for the payment for the payer's bank, and to disguise the money trail.

197. Generally, the shell companies have only an address, a letterbox and a manager who is the nominee to deal with the company's many bank accounts. Shell companies could make use of both the traditional financial system and the Internet based payment services providers. If transactions are performed through the banking system, the difficulty in detection of the suspicious activity is, in fact, detecting the "shell" element in the company. If the transfers are made through the less regulated new payment services, the shell companies might proceed undetected.

198. Case studies show that :

- Shell companies can and have been used as vehicles for cybercrime schemes and money laundering.
- When shell companies are used in cybercrime and money laundering, the amounts transferred tend to be higher than usual.
- The use of shell companies is often related to offshore jurisdictions.

Case study 15: The use of a shell company for international transfer of fraudulent funds

The FIU received an STR based on the AML/CFT Act relating to fraud/fraudulent activity. 1.000.000 USD was credited into the bank account of an off-shore company holding a bank account in Hungary. The fund transfer came from a private bank account from another EU country.

[143] US Threat assessment – Department of Treasury, December 2005

Regarding this 1.000.000 USD transaction the Hungarian bank received a SWIFT messages from the sender bank in which the sender bank referred to fraudulent activity and asked the Hungarian bank to freeze the beneficiary's accounts and return the sum in question to the sender bank because of a suspected fraud. The beneficiary appeared to be a shell company.
After the money was received in the Hungarian bank account, a part of the amount was transferred immediately further on and the rest was withdrawn in cash by the representative of the off-shore company.
Criminal proceedings have begun in both countries, Hungarian law enforcement authorities froze the concerned bank accounts and AML actions are in place at the moment.

Source: Hungary

Case study 16: Fraud via POS terminals

A fraud and money laundering case was detected related to foreign natural persons who asked permanent residence for the purpose of business activities in the country and subsequently established a new company officially registered in the Company's Registry. The foreign citizens were registered as owners and statutory bodies of the company. The scope of business of the company was stated a wholesale of fashion goods. At the same time these persons opened bank accounts in the name of the company with domestic banks. The bank accounts were credited by deposits of high amounts of cash money.
The natural persons representing the company also requested the banks to provide them with mobile POS (point of sale) terminals for the purpose receiving regular incomes from the customers in their business activity.
These persons also opened a number of personal bank accounts with domestic banks and deposited cash in high amounts, asking the banks to issue payment cards related to these accounts.

As far as the system with POS terminals and pre-authorization operated as it was intended they made use of their personal payment cards via POS terminals. The company gave orders for realization of transactions based on pre-authorizations which had not been debited from the personal accounts but were processed. Immediately after expiration of pre-authorizations the funds were withdrawn in cash from the personal accounts by these persons. Then the funds were credited on accounts belonging to the company and immediately withdrawn in cash, deposited on new personal accounts and transferred abroad. The balance of personal accounts was minus indicating high debits.

Currently criminal prosecution is conducted for serious crime of fraud and money laundering. This case was special because of the in-depth preparation of the crime nd investment of own money, properly selected alleged scope of business, sophisticated modus operandi which required detailed knowledge of the bank system and timing for the ending of pre –authorization.

Source: Slovakia

3.1.10 Prepaid cards

199. Prepaid cards are relatively new in the world of consumer electronic payments and they begin as an electronic form of the paper-gift cards. A wide range of prepaid stored value cards are available for purchase with minimal or no identity checking. These cards can have funds transferred onto them and then be either sold or used. Aside from prepaid credit cards, this process can be performed with store cards and with "pay as you go" mobile phones.

200. The pre-paid cards bear in their memory the amount previously deposited to the company or agent that issued them. The so called gift-cards (closed system) allow the holder to buy goods and

services within a pre-determined commercial chain. They can be bought and used anonymously. These cards can be bought from auction sites (e-bay) at an under-valued price.

201. The open system pre-paid cards are issued by banks or other credit and financial institutions, and they can be used for acquisitions at all retailers where usual credit cards are accepted. They can be used for cash withdrawals and are linked to an on line payment account.

202. Prepaid cards can be used by criminals to move illicit money from a jurisdiction to another (layering stage) or to buy products and/or services for the criminal's benefit (integration stage). Prepaid cards have been introduced in a number of countries, but in most countries responding to the survey, their use appears to be less frequent compared with the US[144]. A Boston Consulting Group study forecasts that the US will account for 53% of the global prepaid cards, and supports data that found that Italy was the most advanced prepaid market in Europe, while UK market was described as "established", and markets as Germany and Austria were described as "embryonic". However, the use and spread of prepaid cards have grown in the recent years. According to the Basel Committee on Payment and Settlement Services the number of issued cards with an e-money function has grown from 107,6 million in 2004 to 275,28 million in 2008 in selected countries[145].

Case study 17: From phishing to conversion to digital currencies

Transaction numbers were initially "phished" by Trojans. The "phishing transfer" was made to a bank account held by a financial agent. The financial agent withdrew the money – deducting his commission - in cash. He subsequently purchased credit vouchers of an Internet payment system at various issuing offices, like petrol stations, kiosks, for a maximum amount of 500 €.The purchase was anonymous without identification of the buyer. In this way, real money was converted to virtual money. The financial agent sent the voucher number (which is called „ready- to-spend PIN code) by e-mail to the person giving instructions. The PIN code was used on the Internet for payment of goods and services, casino and gambling websites on the Internet. Several vouchers for smaller amounts could be used jointly and combined. A conversion to other digital currencies by using various exchangers acting on the Internet was possible. The law enforcement authorities were unable to trace the transaction channels.

Source: Germany

Case study 18: Data theft, money laundering and use of prepaid cards

Apart from mafia-style organisations that are operating within a determined area, a number of ad-hoc criminal groups join together as some opportunities arise. Some are operating for years, some just for a short period of time. The TJX company defrauded between 2005 and 2007 the stolen the credit cards numbers of 94 millions of north-American and British clients. In August 2008, 11 persons were arrested (3 US citizens, 1 Estonians, 2 Chinese, 1 Belarus and 3 Ukrainians [[146]]. Media reports indicated that they were part of an international pirates criminal organisation. Among them were those who broke into the wifi network and some top coordinators of the organisation. They were individuals that constantly met on carding forums created after the "CarderPlanet" model, welcoming members from all over the world.

Apart from the information related to credit cards, the sellers proposed false documents (passports), travellers' cheques and even false study licences. In 2009 another incident on 130 millions stolen banking data was revealed.

[144] FATF-GAFI - Money Laundering Using New Payment Methods, October 2010

[145] Belgium, France, Germany, Italy, Japan, Netherlands, Singapore and Switzerland.

[146] Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers: http://www.usdoj.gov/criminal/cybercrime/gonzalezIndict.pdf

The authors of this attack were the same individuals involved in the TJX case.

In order to develop a fraudulent scheme such as in the TJX case, criminal groups specialised in use of false credit cards are required. These criminal groups join together or are dismantles whenever necessary.

In March 2007, Florida Police investigated one of the criminal group member and made several arrests. The scheme was based on the use on pre-paid cards (gift cards) used in electronic and jewels stores for high value acquisitions. The pre-paid cards were bought with counterfeit credit cards supplied by another member of the gang. This technique allowed them to launder more than 225.000 USD. [147]

The trade with stolen banking data is high profit rate. Then users take supplementary risks, but the profits are also high. For the last ones, two methods are at hand: buying from the Internet from sites that require only the billing or the delivery address, or using counterfeit cards in countries where the magnetic band is still in use.

Source: Media

3.1.11 Online gaming and online trading platforms

203. Although the survey results did not identify specific cases of involving online gaming platforms or internet trading platforms for foreign exchange and other financial markets, several countries have also raised the issue of opportunities for money laundering in this context.

204. Such platforms are also the vulnerable to cybercrime attacks or fraud aimed primarily at customers' funds appropriation and present specific ML/TF vulnerabilities, which have been analysed in other typologies specific surveys.[148]

205. The software provided by online games' organisers allows to move and accumulate large amounts of funds, depositing and prize money withdrawing being possible by bank transfers or various electronic payment systems. A trend towards the organised use of bookmaker houses with registered gaming sites was noted (Bulgaria), whereby such platforms were used for money laundering, concealment of assets and tax evasion, with assets mainly used for financing criminal groups, opening of new gambling places, corruption and other offences.

3.2 Indicators of potential money laundering activity: money laundering red flags/ indicators

206. As regards cyber laundering, red flags of anomalous behaviour can be similar to the indicators in the traditional payment systems, or sometimes might bear some particular features. Occurrence of one or more of these indicators may be a warning sign of unusual activity that may be linked to money laundering or terrorist financing. While not all inclusive, this list does reflect ways that launderers have been known to operate, based on the responses to the survey. Transactions or activities listed here may not necessarily be indicative of money laundering if they are consistent with customer's legitimate business. Reporting entities should focus on identifying suspicious activity rather

[147] TJX data theft leads to money-laundering scam: http://www.usatoday.com/money/2007-06-11-tjx-data-theft_N.htm

[148] For further details on ML/TF areas of vulnerability related to Internet trading platform services, see for example the FATF-GAFI – Money Laundering and Terrorist Financing in the Securities Sector (2009) at : http://www.fatf-gafi.org/dataoecd/32/31/43948586.pdf. For details on ML/TF areas of vulnerability related to online gaming and ML/TF methods and techniques, MONEYVAL is conducting a separate survey which will be published early 2012.

than on determining whether the transactions are in fact linked to money laundering, terrorist financing or a particular crime:

- persons holding large number of accounts with the same Internet payment services provider;
- discrepancies between submitted customer identification and IP address;
- suspicious IP addresses, and suspicious usernames (monikers, nicknames, ICQ numbers) would help in the detection of criminal money flows;
- log-ins or attempting log-ins from non trusted IP addresses or from user's ID previously identified as associated with suspicious activity; attempted placement of previously identified as bad "cookies";
- unusual conditions and complexity of the transaction: high frequency of money transfers in a short time, large and diverse source of funds, large and diverse payment methods for the beneficiaries;
- in case of legal persons customers, lack of apparent economic grounds or links between the transaction and the business activity of the client;
- unclear information on the business activity of the client or on the reasons for using Internet payment methods instead of traditional channels (usual for companies and business payments);
- for private persons (i.e. manager of a company) – lack of data on the business area of the performed activity; for a company – stated business activity like "investment", "international", "global investor", "import-export of every kind";
- overlaying corporate officers, holders of specimens or apparent similarities associated with addresses, activities related to recommendations or finances;
- the person's appearance and behaviour are not in conformity with the nature of the transaction being concluded or the person's behaviour is not trustworthy;
- the person uses assistance in filling documents or cannot fill them in;
- the person is not familiar with the nature of the activities of the legal person being represented;
- the person cannot explain the need for the service for the use of which the person called upon the credit or financial institution;
- the person requests unusually high limits (especially the ones used through long distance channels) which do not conform to the person's presumed turnover, previous financial behaviour and social appearance;
- the person requests two or more bank cards which do not conform to the person's presumed turnover or nature of activity;
- the person does not know the real beneficiaries (owners) of the legal person being represented or the location or contact information of the legal person.
- the person cannot describe their possible partners and/or areas of activity.
- the person wants to open an account in a bank branch in one county/town while the address/location of the representative and legal person is elsewhere and no reasonable explanation for such need is provided.
- the deposits to the account of a person/company with normally low income or no income have remarkably increased.
- international transfers received from/sent to foreign countries not in accordance with the profile of the person.
- foreign payments received and subsequent cash withdrawals and transfers via money transfer services.
- transaction does not correspond to previous operations of the client;
- regular transactions of sums below the threshold required for declaring the origin of the assets; high total amount of the transferred assets;
- account held with Internet payment services used only for cash withdrawals;

- funding provided mainly in cash or cash-like instruments (such as prepaid cards), usually under the reporting threshold.
- funding provided by unknown third parties immediately followed by cash withdrawals or international transfers;
- operations from and to foreign countries combined with unclear data on the external beneficiaries, on the payers or on the origin of the assets;
- setting of durable commercial relations or conducting a transaction through electronic statement, electronic document of electronic signature or other form without the physical presence of the client;
- corporate accumulation (transfers between bank accounts of related persons or donations without reasonable grounds):
- telegraphic transfers from donor organizations in favour of companies located in countries known to be bank or tax heavens:
- transactions of funds originating from offshore zones, countries which do not enforce the international AML/CFT standards, etc.:
- transactions or withdrawals (in cash, cheques, telegraphic transfers, etc.) under accounts which do no correspond to the previous conditions on deposits;
- transactions involving large amounts of incoming or outgoing transfers, without logical or apparent purpose and which are received or sent to/from 'at risk jurisdictions' (i.e. sanctioned countries, non-cooperating nations, nations supporting terrorism);
- unexplained clearing or contracting with cheques of third parties or their deposits in foreign bank accounts:
- using multiple accounts to raise funds which are then transferred in favour of the same foreign beneficiaries;
- schemes for cash debiting in which the deposits (i. e. in the USA) are directly related to cash withdrawal from ATM in problem countries. Reverse transactions of this nature are also suspicious;
- issuing of cheques, payment orders or other financial instruments sequentially numbered, in favour of one and the same person or company or persons and companies with name similar in sound;
- an enterprise with a usually passive economic turnover or a newly established enterprise receive unusually high volume transactions not in accordance of the profile of the person;
- accounts opened by non-residents without any relations to the jurisdiction where the payment services is located;
- frequent foreign income registered into a bank account followed by cash withdrawals and transfers via money remittance services Online payment system or currency system hosted on a server based in a weak regulatory environment or a jurisdiction of ML/FT concern, as defined by the FATF, a regional FSRB or a relevant national authority;
- activity by money mules is a red flag for money laundering and should trigger action by or an involvement of FIUs.

4 COUNTERMEASURES

207. In response to increasing criminal money flows on the Internet, public and private sector organisations have adopted a range of measures, as the examples in this chapter show.

208. These measures may serve as good practices and could become elements of more systematic future approaches and strategies that are aimed at the prevention of money laundering and the financing of terrorism, and at the search, seizure and confiscation of proceeds from crime on the Internet:

- Mechanisms for reporting on fraud and other proceeds generating offences on the Internet;
- Prevention and public awareness;
- Regulation, risk management and due diligence;
- Creation of a legal framework based on international standards;
- Establishment of specialised units for high-tech crime;
- Interagency co-operation, in particular between authorities responsible for financial investigations, money laundering and cybercrime;
- Public-private co-operation and information exchange;
- Training.

209. Before summarising good practices and measures taken, it is useful to provide an overview of the many public and private sector institutions that have a stake, hold important information and therefore should be involved:

Institutions	**Responsibilities**	**Type of information held**
Anti-money laundering system		
➢ Financial sector institutions obliged to report	- Ensure compliance with regulations related to money laundering and the financing of terrorism - Exercising due diligence - Reporting suspicious or unusual transactions to FIUs	- Customer and beneficial owner data - Data on financial transactions
➢ Financial intelligence units (FIUs)[1]	- National centre responsible for receiving, analysing and disseminating to competent authorities disclosures of suspicious transaction reports and other concerning suspected money laundering or financing of terrorism activities - Co-operation and information exchange between FIUs through the Egmont Group.[2]	- Information on suspicious or unusual transactions and related analysis
➢ Asset recovery/financial investigation agencies[3]	- Carry out financial investigations related to criminal offences involving	- Data on specific criminal investigations

[1] See http://conventions.coe.int/Treaty/EN/Treaties/Html/198.htm

[2] http://www.egmontgroup.org/

Institutions	Responsibilities	Type of information held
	crime proceeds - Follow up on information received from FIUs - Implement provisional measures to seize or freeze suspected crime proceeds	- Intelligence
➢ Prosecutors and judges	- Prosecution and adjudication of cases - Supervising criminal investigations - Authorising investigative measures, including search, seizure and freezing of assets - International judicial co-operation	- Data on specific criminal investigations
➢ Supervisors and regulators	- Prevent the misuse of the financial systems for money laundering and financing of terrorism - Ensure compliance by financial sector institutions with AML/CFT regulations	- Data on financial sector institutions - Information on regulations
➢ International monitoring bodies[4]	- Monitoring compliance with international standards on money laundering and the financing of terrorism	- Information on domestic regulations and functioning of AML/CFT systems
Anti-cybercrime institutions		
➢ Specialised prosecution services	- Prosecuting cybercrime - Supervising investigations and authorising investigative measures - International co-operation	- Data on specific criminal investigations
➢ High-tech crime units	- Perform cybercrime investigations - Collect and analyse data - Search computer systems - Assist other police departments in cybercrime investigations - Intelligence gathering - Exchange information with similar bodies of other countries - International police co-operation and support to international judicial co-operation	- Data on specific criminal investigations - Intelligence
➢ Computer forensic laboratories	- Examination of electronic evidence in support of criminal investigations	- Data on electronic evidence
➢ 24/7 points of contact for international co-operation against cybercrime[5]	- Ensure expedited preservation of data in international co-operation - Collecting evidence - Locating suspects	- Data on specific international investigations

[3] For a network of asset recovery agencies see CARIN at: http://www.europol.europa.eu/publications/Camden_Assets_Recovery_Inter-Agency_Network/CARIN_Europol.pdf

[4] See MONEYVAL (http://www.coe.int/t/dghl/monitoring/moneyval/) and Financial Action Task Force (FATF) (www.fatf-gafi.org).

[5] See Article 35 of the Budapest Convention on Cybercrime

Institutions	Responsibilities	Type of information held
	- Facilitate judicial co-operation	
Financial sector (online)		
➢ Payment cards industry	- Online payments by customers	- Data on customers and transactions - Data on fraud and attempted fraud - Redflags/criteria for detecting fraud
➢ Online banking services	- Management of accounts by users	- Data on customers and transactions - Data on fraud and attempted fraud - Redflags/criteria for detecting fraud
➢ Online payment platforms	- Online payment services and solutions for individuals and companies - Compliance with AML/CFT and other financial sector regulations	- Data on customers and transactions - Data on fraud and attempted fraud - Redflags/criteria for detecting fraud
➢ Content providers[6]	- Providing services online, including auctions, shops, social networks	- Information on customers - Data on fraud and other malicious activities against their services or customers
➢ Money transfer services	- Transfer of money online or to and from locations worldwide	- Data on customers and transactions
Internet service providers (ISPs)		
➢ Telecommunication providers	- Provide access to telecommunication channels and high-speed broad-band connections and other services - "Common carriers" of electronic signals (not liable for content)	-
➢ Internet access providers	- Provide users with access to the Internet on demand - Usually "Common carriers" of electronic signals (not liable for content) - Terms and conditions of access and acceptable use policies help cope with abuse	- Subscriber information - Internet traffic data (log files, IP-related data) - Content data - May filter for spam, malware or child pornography - Deep packet inspections[7] (although encryption, use of

http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG. See also: http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf

[6] With Web 2.0 a distinction between professional versus non-professional content providers is necessary as any use can become a content provider.

Institutions	Responsibilities	Type of information held
		proxy servers, overseas account multi-protocol tunnelling etc reduces the possibilities of ISPs for DPI)
➢ Hosting providers	- Registration and hosting of domains - Hosting of servers - Hosting of mail servers	- Subscriber information - Limited knowledge of content hosted unless a specific problem arises
ICANN, registries and registrars[8]		
➢ ICANN[9]	- Coordinate the allocation of domain names (the Domain Name System), Internet Protocol (IP) addresses and automous system numbers, and protocol port and parameter numbers	- Information on registries and registrars
➢ Registries[10]	- Manage Generic Top Level Domains (gTLD) (e.g. .com, .org) - Manage Country Code Top Level Domains (ccTLDs) (e.g. .fr, .uk) - Allocate and assign Internet resources such as IP address space, Autonomous System Numbers (groups of IP networks) etc to organisations	- WHOIS database on registrants ("telephone book of the Internet") including name, postal address, telephone number, email address
➢ Registrars (ISP)	- Obtains a domain name from a registry under a Registry Registrar Agreement (RRA) - Provides end user with a domain name service against a fee	- Information on registrants for the WHOIS register. Under the RRA this information should be accurate and complete[11]
Institutions monitoring Internet activity		
➢ CERT/CSIRT	- Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) are public or private sector institutions that study vulnerabilities and respond to incidents	- Information on security incidents

[7] While Deep Packet Inspections helps improve security, it also allows ISPs to monitor Internet traffic and potentially to collect and analyse communications by millions of users. It is considered highly problematic with regard to net neutrality and non-discrimination, content filtering, freedom of speech, profiling, privacy and protection of personal data.
http://www.deeppacketinspection.ca/
http://userpage.fu-berlin.de/~bendrath/ISA09_Paper_Ralf%20Bendrath_DPI.pdf
http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf

[8] For a description on the functioning of system see this report prepared for the Council of Europe's Project on Cybercrime: http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_wolfgangkleinwaechter1.pdf

[9] Internet Corporation for Assigned Names and Numbers

[10] For Europe, see http://www.ripe.net/

[11] It seems that in most cases this is not the case.

Institutions	Responsibilities	Type of information held
	by providing advisories and technical solutions[12]	
➢ Industry, research institutions, associations or initiatives against cybercrime[13]	- Monitoring Domain Name Servers - Monitoring routing protocols (BGP) - Monitoring for malicious activities - Investigation of criminal activities - Promoting co-operation and action against fraud and other types of cybercrime	- Information on malicious activity on the Internet and compromised machines - Information on botnets and other types of attack - Information on suspected offenders[14]

4.1 E-crime reporting

210. Limited data and knowledge of fraud and other types of cybercrime is considered a key obstacle to preventing and controlling cybercrime and criminal money flows as pointed out by countries in their replies to the questionnaire: capabilities to analyse Internet fraud and related money flows are missing in most countries. Awareness and understanding that organised criminal structures may be behind what appears to be instances of minor fraud among is limited. While suspicious money

[12] For the CERT coordination centre at Carnegie Mellon University see: http://www.cert.org/
For a government CERT see: http://www.us-cert.gov/ or
https://www.bsi.bund.de/cln_156/DE/Themen/CERTBund/certbund_node.html
For the Forum of Incident Response and Security Teams see: http://www.first.org/
For the informal grouping of European governmental CERTs see
https://www.bsi.bund.de/cln_156/ContentBSI/Themen/CERT_Bund/InternatKooperation/egovcert_en.html

[13] Such private sector initiatives follow billions of sets of data traffic per day to identify malicious activities and thus dispose of huge amounts of data that appear to be largely untapped by law enforcement.
Examples:
http://mynetwatchman.com/
http://www.team-cymru.org/Services/
http://www.spamhaus.org/organization/index.lasso
http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_emea_Internet_security_threat_report_xv_04-2010.en-us.pdf
http://www.messagelabs.com/resources/
For a list of initiatives see:
http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/networks/Networks_en.asp
Examples of initiatives focusing on fraud are:

- the Anti-Phishing Working Group (http://www.antiphishing.org/), a global pan-industrial and law enforcement association focused on eliminating fraud and identity theft resulting from phishing, pharming and email spoofing of all types
- The London Action Plan (http://www.antiphishing.org/) which is to promote international spam enforcement co-operation and address spam related problems, such as online fraud and deception, phishing, and dissemination of viruses. The participants also open the Action Plan for participation by other interested government and public agencies, and by appropriate private sector representatives, as a way to expand the network of entities engaged in spam enforcement co-operation
- The Messaging Anti-abuse Working Group (http://www.maawg.org/) (MAAWG) that is to bring the messaging industry together to work collaboratively and to successfully address the various forms of messaging abuse, such as spam, viruses, denial-of-service attacks and other messaging exploitations.

[14] See for example the ROKSO database of Spamhouse at http://www.spamhaus.org/rokso/

flows are detected, law enforcement and private industry are often not able to collate the data, that is, "to connect the dots" to obtain the full picture of criminal operations and to detect patterns.

211. Examples of good practice related to Internet crime reporting are available or in the making.

4.1.1 Internet Crime Complaint Centre (IC3)[15]

212. The IC3 was created as a partnership between the Federal Bureau of Investigations and the National White Collar Crime Center. It accepts complaints online from persons who believe they were defrauded or from a third party to the complainant and it refers complaints to law enforcement authorities for further investigation. According to its mission statement:

> IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, local, and international level, IC3 provides a central referral mechanism for complaints involving Internet related crimes.

213. In 2009, the IC3 received 336,655 complaint submissions, of which 146,663 were referred to law enforcement.[16] Most of these referrals were complaints related to the non-delivery of goods and services (19.9%), identity theft (14.1%), debit/credit card fraud (10.4%) and auction fraud 10.3%).

214. The new classification introduced in 2009 comprises 79 complaint types that go beyond fraud and also cover drug trafficking, intimidation, pornography, terrorism and a range of other offences involving the Internet.[17]

215. The complaint reporting allows law enforcement to detect not only individual offences but to identify trends and to analyse Internet-related crime in a more comprehensive manner.

216. The IC3 publishes annual Internet Crime Reports, as well as awareness and educational materials aimed at preventing fraud and other forms of Internet crime.

4.1.2 MELANI[18]

217. In Switzerland, the "Melde- und Analysestelle Informationssicherung" (MELANI) was established in 2004. It is a centre for reporting and analysis related to the security of information systems that provides information on threats and countermeasures, analytical situation reports on threats and trends and the possibility to report incidents.

218. MELANI is maintained by GovCERT.CH, the Federal Intelligence Service (NDB) and the Federal Strategy Unit for Information Technology (ISB).

219. As of 1 January 2010, MELANI has the authority to block, under certain conditions, domain names that are suspected of identity theft (phishing) or spreading of malware.

---

[15] http://www.ic3.gov/default.aspx

[16] Internet Crime Complaint Center (2010): Internet Crime Report 2009 (http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).

[17] (See: Internet Crime Complaint Center (2010): Internet Crime Report 2009 at http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).

[18] http://www.melani.admin.ch

4.1.3 National Fraud Reporting Centre[19]

220. The United Kingdom, in 2010, established "Action Fraud" as the national fraud reporting centre to provide a central point of information on fraud and allows 24/7 online fraud reporting.

221. Action Fraud is managed by the National Fraud Authority which is an executive agency of the Attorney General's Office. Partners include the City of London Police, National Fraud Intelligence Bureau (NFIB), the Association of Chief Police Officers and the Home Office. Cases reported are registered and referred to the NFIB for investigation or intelligence purposes. Action Fraud, furthermore, provides preventive information, including fraud warnings, and support to victims.

4.1.4 Internet Crime Reporting Online System (I-CROS)[20]

222. The establishment of I-CROS at Europol was initiated in 2010 with the support of the European Commission. It will allow European Union member States and eventually third parties to submit offences noted on the Internet to EUROPOL. The focus will be on offences as defined in articles 2 to 8 of the Budapest Convention on Cybercrime. [21]

223. I-CROS is the European level of the so-called European Alert Platform for reporting offences noted on the Internet, as approved by the Council of the EU in its Conclusions on setting up national alert platforms and a European alert platform for reporting offences noted on the Internet (24 October 2008). It complements national alert platforms being set-up in the member States. Reports made by citizens and businesses are received first by national platforms, who process them, and then forward those reports of relevance to other member States and Europol for cross-checking within I-CROS.

224. I-CROS is part of European Cybercrime Platform (ECCP) that includes also the Analysis Work File "Cyborg" that is focusing on criminal groups operating on the Internet, and the Internet & Forensic Expert Forum (IFOREX) to host technical data and training for cybercrime law enforcement. ECCP is a first step towards a more consistent and effective approach to fighting Internet criminality at the EU level.

4.1.5 Signal Spam[22]

225. Signal Spam is a public-private partnership in France that allows Internet users to report spam messages which are recorded in a single database that is then used for criminal and administrative investigations, as well as research, and that allows to enhance network security and email delivery.

226. Members include associations (such as the French ISP association AFA, the French Advertising Union, Business Software Alliance and others), industry (such as CERT-LEXI, eBay/PayPal, Microsoft, Orange and others) and national authorities (Gendamerie Nationale, French Police High-tech Crime Unit, the French Data Protection Authority CNIL, the Investigation Brigade o Fraud and Information Technology and others).

---

[19] http://www.actionfraud.org.uk/home

[20] Information provided by the European Commission.

[21] The draft EU Framework on attacks against information systems (COM(2010) 517 final) in Article 15 contains a specific obligation for member States to record, produce and provide statistical data on cybercrime http://www.statewatch.org/news/2010/sep/ceu-com-atacks-on-info-systems-com-517-10.pdf

[22] https://www.signal-spam.fr/

4.1.6 E-Crime reporting: using a common data format

227. Data relevant to cybercrime investigations is often voluminous, scattered across different jurisdictions and venues, and archived in disparate file formats that obstruct machine- based sharing and processing.

228. In order to overcome this problem, the Anti-Phishing Working Group developed an XML-based scheme for reporting technical aspects of phishing, fraud and other forms of electronic crime.

229. The APWG defined a set of extensions to the Incident Object Description Exchange Format (IODEF), a reporting standard for network events adopted by the Internet Engineering Task Force (IETF).[23] This will enable a common reporting format and provide data on the fraud source and target of the attack, the web servers involved, the malware used, domain name service and registry information, evidentiary files, and others.

230. As a common reporting format it will thus facilitate data sharing between public and private sector institutions and may permit more automated mechanisms for e-crime detection in the future.

4.2 Prevention and public awareness

231. Public education and awareness and other measures obviously are essential elements to prevent fraud and other forms of crime, and thus money laundering and criminal money flows on the Internet.

232. The offer in this respect is increasing, ranging from public website with general fraud prevention information,[24] or materials and educational materials and courses,[25] to recommendations for employees of public or private sector organisations or specific resources to prevent risks in a specific sector,[26] or assistance to victims of fraud.[27]

233. An example, combining reporting on botnet activity, informing users that their systems are infected, providing assistance in the cleaning of user systems and preventive measures is the Anti-botnet Advisory Centre www.botfrei.de which is a public-private initiative of the German Federal Office for Information Security and the service provider association ECO. The offer is available in several languages.

4.3 Regulatory and supervisory measures

4.3.1 Risk management and due diligence measures

234. Financial institutions should design and implement appropriate measures and controls to mitigate the potential money laundering risks in respect of the relevant products, services or

[23] http://www.rfc-archive.org/getrfc.php?rfc=5901&tag=Extensions-to-the-IODEF-Document-Class-for-Reporting-Phishing
http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_if09_pres_APWG_ADVISORY_Reporting_eCrime_via_IODEF.pdf

[24] http://www.ic3.gov/preventiontips.aspx
http://www.stoppbetrug.ch/4/fr/1prevention_methodes_descroquerie/40201ventes_aux_encheres.php

[25] For example: http://www.polizei-nrw.de/koeln/Vorbeugung/kriminalitaet/Internet-und-datenkriminalitaet/

[26] For example, Resources for merchants to prevent payment card fraud
http://www.visa.ca/en/merchant/fraud-prevention/index.jsp

[27] For example: http://www.actionfraud.org.uk/home

customers, based on a thorough risk assessment process. Such measures and controls may require investments both in terms of resources and time in order to identify and capture appropriate risk data. Such measures and controls may include one or more of the following:

- increased awareness by the institution of higher risk situations determined by types of financial services and/or products and/or customers;
- appropriate levels of know your customer ("KYC") or enhanced due diligence;
- escalation for approval of the establishment of an account or relationship;
- record-keeping;
- increased monitoring of transactions ; and
- increased levels of on-going controls and reviews of relationships.

235. While guidance has been provided on risk based approaches for managing money laundering risks[28] in general, specific guidance on Internet-related risks is being developed for financial organisations offering services on the Internet.

236. One example is Recommendation No. 1 of 2009 (10 February) of the Board of the Hungarian Financial Supervisory Authority on Internet security risks.[29]

237. The financial sector has measures in place to manage risks such as:

- Centralised transaction databases that can be used to correlate transactions, perform analysis, identify suspicious transactions, create red flags and rapidly detect criminal activity both within a financial institution and between financial institutions;
- Behaviour profiling and monitoring for mule account activity in financial institutions;
- "Hot lists" of known or suspected accounts;
- Information sharing between financial institutions;
- Adopting a holistic view of all money movement within a particular financial institution;
- Implementation of protective measures in online banking services, including two factor authentication, TAN (Transaction Authorisation Number) and MTAN (mobile TAN);
- verification of documentation or requirements for additional documents to confirm customer identity;
- requiring first payment transaction to be carried out between domestic accounts or other pre-approved countries;
- monitoring and analysis of statements of transactions using bank cards;
- limiting the amounts of funds that can be transferred using bank cards;
- analysing and seeking links from a bank card to specific bank accounts from which card value has been transferred or to which card value has been transferred;
- monitoring card transactions and recording suspicious activities;
- denying anonymous, encoded or numbered accounts via electronic systems or Internet as well as those accounts offered by offshore banks in Internet banking.

238. Commercial websites and Internet payment systems have been moving towards a pro-active risk-based approach that includes applying risk-based customer due diligence, building and using risk

[28] http://www.wolfsberg-principles.com/risk-based-approach.html

[29] Recommendation No. 1 of 2009 (10 February) of the Board of the Hungarian Financial Supervisory Authority on Internet security risks.

models and software to detect unusual and suspicious activities based on red flags and indicators, manual review of suspicious transactions, delaying of transactions, maintaining of audit trails. [30]

239. Specific measures adopted by the payment card industry include the implementation of security standards by merchants, processors and financial institutions[31] or risk management guides for merchants.[32]

4.3.2 Due diligence for registrars and registries

240. The use of domains for criminal purposes, such as botnet operations, is a building block of the infrastructure for cybercrime. The process of domain registration[33] offers an opportunity to prevent and disrupt the risk of misuse of domains by criminals.

241. A set of due diligence recommendations was therefore drafted in 2009 by law enforcement agencies for adoption by ICANN.[34]

242. They foresee that:

- ICANN performs due diligence investigations on all registrars and registries;
- ICANN amends the Registrar Accreditation Agreement (RAA) to ensure that registrars collect accurate and complete data of those registering domain names;
- WHOIS information of all generic Top Level Domains (gTLD) is accurate and detailed and can be provided to law enforcement;
- ICANN requires that all domain name resellers and third party beneficiaries are held to the same terms as registrars and registries.

243. The draft recommendations were discussed in different fora[35] and supported by the ICANN Governmental Advisory Committee in June 2010. The GAC Communiqué (Brussels, June 2010) stated among other things:

> "The GAC encourages the Board, the RAA Working Group and registrars to work with law enforcement agencies to address their concerns and implement necessary changes without delay." [36]

244. By December 2011, progress had been made with respect to some recommendations only.[37]

---

[30] See the measures taken by the sector in: Financial Action Task Force: Money Laundering & Terrorist Financing Vulnerabilities Of Commercial Websites And Internet Payment Systems (June 2008). This was further discussed in the preparation of the present typology study.

[31] Such as the Payment Card Industry Data Security Standard (PCI DSS) and related requirements https://www.pcisecuritystandards.org/security_standards/index.php

[32] http://usa.visa.com/download/merchants/visa_risk_management_guide_ecommerce.pdf

[33] For a better understanding of this process see the report of Wolfgang Kleinwächter prepared for the Council of Europe Project on Cybercrime http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_wolfgangkleinwaechter1.pdf

[34] Internet Corporation for Assigned Names and Numbers (www.icann.org)

[35] Including the 2010 Octopus Conference of the Council of Europe. http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/Ws%202/LEA_ICANN_Recom_oct2009.pdf

[36] http://gac.icann.org/system/files/Brussels-communique.pdf

[37] http://www.icann.org/en/announcements/announcement-2-12dec11-en.htm

4.4 Harmonised legal framework based on international standards

245. The creation of a legal framework for the criminalization of conduct related to criminal money flows on the Internet, for the effective investigation of cybercrime, money laundering and the financing of terrorism, for financial investigations and the confiscation of crime proceeds and for international co-operation is considered essential. The Budapest Convention and the Warsaw Conventions help countries meet this challenge.

4.4.1 Implementation of the Budapest Convention on Cybercrime

246. Several countries pointed at the implementation of Budapest Convention on Cybercrime as an important measure to enable criminal justice responses:

- Adoption of substantive criminal law provisions in line with articles 2 to 12 means the criminalisation of the different acts involved when fraud and other offences are committed on the Internet. Of particular relevance are article 2 (illegal access), article 3 (illegal interception), article 4 (data interference), article 5 (system interference), article 7 (computer-related forgery) and article 8 (computer-related fraud).

- Implementation of the procedural law provisions (such as articles 16 and 17 on expedited preservation, article 18 on production orders, article 19 on search and seizure and articles 20 and 21 on the interception of traffic and content data) permit law enforcement to seize volatile electronic evidence in an efficient manner. They also stipulate the co-operation of Internet service providers in criminal investigations.

- Parties to the Convention can make use of this treaty as a framework for international co-operation, including the expedited preservation of data in other jurisdictions (article 29) and efficient mutual legal assistance in accessing computer data (article 31).

- The Budapest Convention helps ensure harmonisation of legislation between countries which in itself is an important prerequisite for international co-operation. A large number of countries around the world is using this treaty as a guideline for developing domestic legislation.

247. Examples of countries that recently adopted or updated legislation include Estonia, Germany and Portugal. The example of Romania is useful in that it closely follows the Budapest Convention on Cybercrime. [38]

4.4.2 Implementation of the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism[39]

248. The Warsaw Convention of 2005 sets out requirements for State Parties to adopt a number of measures, including:

Changes are to be reflected in amendments to the Registrar Accreditation Agreement (RAA), and subsequent enforcement. Further discussions are to be held at ICANN 43 in Costa Rica in March 2012.

[38] See country profiles on cybercrime legislation at: http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp

[39] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=198&CM=8&DF=&CL=ENG

- Confiscation (article 3), investigative and provisional measures (article 4), freezing, seizure and confiscation (article 5), management of frozen or seized property (article 6) and investigate powers and techniques (article 7);
- The criminalisation of laundering offences (article 9);
- The establishment of financial intelligence units, FIUs (article 12);
- Preventive measures (article 13);
- The postponement of domestic suspicious transactions;
- International requests for information on bank accounts (article 17), on banking transactions (article 18), for monitoring of banking transactions (article 19), for the execution of provisional measures (articles 21 and 22) and for confiscation (articles 23 and 24);
- Cooperation between FIUs (article 46).

249. An adequate implementation of this treaty's provisions should enable public authorities to take effective measures to search, seize and confiscate crime proceeds, to prevent and control money laundering and the financing of terrorism and to cooperate internationally with each other.

250. This Convention provides for a monitoring mechanism through a Conference of the Parties to ensure that its provisions are being effectively implemented. [40]

4.5 Establishment of specialised units for high-tech crime[41]

251. Many countries have established specialised units for cybercrime. Examples include[42]:

- *Albania*: The State Police under the Financial Crime Investigation Department has two specialized structures of which one is responsible for the investigation of computer crimes (Cyber Crime Investigations Sector), and one for the investigation of criminal assets.

- *Belarus:* Department for Financial Monitoring of the State Control Committee (DFM) and Units for high-tech crime under the Ministry of Internal Affairs and the State Security Committee have been established.

- *China:* A special department (Cybersecurity Bureau) to counter cybercrime has been established in the Ministry of Public Security. The China Anti-Money Laundering and Monitoring Centre monitors criminal money flows, including on the Internet.

- *Hungary*: Establishment of a Cybercrime Unit of National Bureau of Investigation of Hungarian Police, and Financial Forensic Department of HFSA and Establishment of national cyber incident management capacity –CERT-Hungary.

- *Romania:* A service for countering cyber criminality has been created within the Organised Crime and Terrorism Investigation Directorate at the Prosecutor's Office attached to the High Court of Cassation and Justice. The functions of this unit have been defined in line with Law no.161/2003. A special cybercrime unit has been operating at General Inspectorate of the Romanian police (organized crime Directorate of the Police) since 2003.

[40] http://www.coe.int/t/dghl/monitoring/cop198/default_en.asp

[41] For a good practice study on specialised cybercrime units prepared in 2011 see: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf

[42] Source: replies to the questionnaire.

– *Slovakia*: the Department of Cybercrime at the Bureau of Judicial and Criminal Police of the Presidium of the Police Force of the Slovak Republic deals with methodology, trends and cases related to cybercrime at the national level in the Slovak Republic.

– "*The former Yugoslav Republic of Macedonia":* the department of cybercrime and counterfeiting was established in January 2005, as part of the Sector of Organised Crime. Since 2008, this Department is now a special unit for fighting cybercrime, as a part of the Department of Organised Crime.

– *Ukraine:* in 2001 a specialised department on the fight against offences in intellectual property and computer systems was established at the Ministry of Interior. Appropriate departments of the Security Service of Ukraine are also responsible for the fight against cybercrime, in particular, units for counter-espionage at the State Economy Protection Department; units of Senior Department on combat against corruption and organized crime of Security Service of Ukraine counteract to illicit proceeds flows through Internet/computer systems.

252. Police-type high-tech crime units typically have the following tasks:[43]

– Cybercrime investigation
  - perform investigations for combating cybercrime;
  - collect and analyse data and information;
  - carry out technical activities for researching computer systems;
  - draft internal rules and procedures for cybercrime investigation;
  - assist other police departments in performing investigations;
  - perform activities for international judicial assistance for criminal issues, within national and international mutual assistance;
  - conduct public awareness cybercrime prevention activities.

– Research
  - conduct quality research activities into cybercrime trends both domestically and internationally to inform the future requirements for countering cybercrime;
  - work with academic and industry partners to develop tools and techniques to assist in the efforts to combat cybercrime.

– Intelligence gathering
  - perform activities for international co-operation and information exchange with other similar bodies from abroad;
  - perform analyses, studies, and evaluation of the criminal phenomenon;
  - gathering both open source and covert Internet intelligence.

– Training
  - establish a professional training programme for digital forensic specialist and cybercrime investigators to ensure that the correct level of knowledge and skills are available.

[43] Source: Council of Europe/EU joint Project on Cybercrime in Georgia (2009): Proposals for the establishment of a High Tech Crime Unit. Paper prepared by Nigel Jones (United Kingdom) and Virgil Spiridon (Romania).

253. In 2010, the European Union established the EU Cyber Crime Task Force which comprises the heads of cybercrime or high-tech crime units of the EU. In 2011, this Task Force and the Council of Europe cooperated in the preparation of a good practice study on specialised cybercrime units. [44]

4.6 Inter-agency co-operation

254. Cooperation between authorities responsible for financial investigations and confiscation of proceeds, measures again money laundering and cybercrime is considered an important condition for success against criminal money on the Internet. The replies to the questionnaire provide some examples.

4.6.1 Germany: Project group "Electronic payment systems"

255. The German Federal Criminal Police (BKA) has established a project group on "electronic payment systems" led by the financial intelligence unit of the BKA with the participation of five State Criminal Police Offices (LKAs). It comprised experts in financial investigations, Internet and computer crime and confiscation of assets as well as experts from the Federal Financial Supervisory Authority (BAFIN). The tasks of the group were to:

- identify and analyse representative cases involving electronic payment systems by carrying out checks with the national police authorities;
- describe problem areas from the police point of view;
- describe enforcement approaches from the view of the police and the supervisory authority.

256. The project group issued the following recommendations for action:

- A newsletter on the general functioning of electronic payment systems is to raise the awareness of all police offices in Germany.
- This topic is to be dealt with in the training of police officers from the fields of financial investigations, Internet and computer crime and confiscation of assets.
- The FIU will also publish a Newsletter on these problems and make it available on its website.
- Close co-operation with the online payment providers is also important, especially having points of contact.
- The co-operation between the police and the supervisory authorities will have to be intensified as well; similar to the already existing co-operation between BAFIN and the BKA/FIU.
- The information exchange between supervisory authorities at the international level is important so that, for example, coordinated prohibition orders can be issued against online payment providers not holding an authorisation.
- Finally, the international supervision of providers should be coordinated and intensified. This is not a problem that can be solved at national level.
- This topic should be dealt with in an appropriate, intensified and coordinated manner by international bodies, such as the FATF.

257. The BKA furthermore began to set up an information pool on electronic payment systems that can be accessed by all police officers at the national level. However, the setting up and maintenance of such a database at international level was considered to be more efficient.

[44] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf

4.6.2 Albania: Memoranda of co-operation

258. In Albania, two memoranda of co-operation have been concluded between the prosecution, police, customs, taxes, bank, High Inspectorate for the Declaration and Audit of Assets, Financial Intelligence Unit and National Intelligence Service. Seven task forces have been formed against corruption and financial crime (including cybercrime) that operate in seven districts (Tirana, Durres, Shkoder, Fier, Vlora, Korca and Gjirokastra).

4.7 Public-private co-operation and information exchange

259. Public-private co-operation and information exchange is arguably the measure with the strongest impact on the prevention and control of criminal money flows on the Internet. It addresses a key problem, namely the limited sharing and use of existing information between domestic financial institutions, and between financial institutions and law enforcement.

260. It is therefore no coincidence that many examples have been provided in the replies to the questionnaire and other sources. Most of these examples related to co-operation and information exchange at domestic levels. Enhanced public-private co-operation and information exchange at the international level was considered desirable.

261. Further public-private co-operation could help address a major problem of all forms of cybercrime, that is, to attribute criminal conduct to a person.

4.7.1 The Irish Bankers Federation (IBF) High Tech Crime Forum

262. The Forum consists of Senior staff in information security, fraud and risk management functions from all of the retail banks operating in Ireland that offer an online banking service:

- An Garda Siochana.
- The Police Service of Northern Ireland.
- The Irish Payment Services Organisation.
- The Internet Service Providers Association of Ireland.
- The University College Dublin Centre for Cybercrime Investigation (UCD CCI).

263. The High Tech Crime Forum meets bi-monthly to exchange information on recent and emerging threats and to formulate a coordinated approach to high tech crime threats against online banks operating in Ireland.

264. One of the key successes of the Forum has been an effort, working in conjunction with an Garda Siochana and UCD CCI, to identify threats to banking and payment services occurring in other jurisdictions in order to be able to assess the potential threats posed by emerging attacks and proactively defend against these attacks before any losses are incurred by the banks operating in Ireland. Periodic reports on emerging attacks are delivered to the high tech crime forum.

265. The key achievement of the Forum is to develop confidence between the members so that they can share information freely in a trusted environment. Members of such a Forum must also be convinced that the issues of cybercrime prevention, detection and response are not issues of competition.

266. Further, there should be a general understanding that even though a particular member of the Forum is under attack at a given time, it could just as easily be any of the other members at any time in the future.

267. Another aspect of best practice implemented by the IBF High Tech Crime Forum is proactive action against emerging cybercrime threats. UCD CCI carries out research on behalf of the Forum. The members of the Forum identify key areas of concern, priorities for research are set by law enforcement, and UCD CCI carries out the research. This process, consisting of:

- engaging with all members of the high tech crime forum;
- receiving advice and direction from law enforcement;
- leveraging the expertise of the UCD CCI;
- leads to a significant volume of valuable research being carried out in Ireland.

268. The main focus of research carried out to date by UCD CCI for the Forum has consisted of identifying threats emerging in other countries before they are seen in Ireland so that the Irish banks can assess their risk and take appropriate preventative measures before any losses are suffered.

269. The UCD CCI also attempts to examine the industry response to various new threats that have been seen in recent months in order to identify areas where a greater level of co-operation between the members would be beneficial.

4.7.2 Hungary: Incident management working group

270. In Hungary, an Internet security/incident watch and management working group has been established with the participation of banks, law enforcement (National Bureau of Investigation), the Computer Emergency Response Team (CERT-Hungary[45]) and the Hungarian Financial Supervisory Authority (HFSA).[46] At least four times per year the situation is analysed and new methods of perpetration are reviewed in view of preventive measures. Once per year, a practical exercise is carried out in which an attack is simulated and incident response capabilities are strengthened.

271. A professional protocol to react to phishing attacks (in case of attack: who to contact at police and financial institution, how to cooperate, type and structure of data to be exchanged etc.) is being developed with the participation of the police and experts from credit institutions to enable immediate and efficient responses.

4.7.3 US National Cyber-Forensics & Training Alliance - NCFTA[47]

272. The core mission of the NCFTA – created in 1997 – is to identify criminals responsible for cyber-based attacks. It provides a conduit for intelligence exchange between industry and law enforcement, including small and medium enterprises.

273. Specific initiatives include:

- CyFin – a forum against online stock manipulation schemes;
- Reshipping – an initiative against the concealment of the true recipients of merchandise purchased with stolen payment credentials;
- Digital Phishnet – developing intelligence of high-priority and sophisticated phishing schemes;

[45] http://www.cert-hungary.hu/en

[46] http://www.pszaf.hu/en/

[47] http://www.ncfta.net/

- Pharmacy – a neutral forum for information exchange between private industry and law enforcement related to illicit online pharmaceutical sales and other threats;
- Malware and botnet – to collate intelligence to attribute malicious code to criminals;
- Internet Fraud Alert – a central clearing house and alert mechanism to report compromised credentials.

4.7.4 Information Sharing and Analysis Centres (ISAC) for the financial sector

274. In the USA, the "Financial Services – Information Sharing and Analysis Center" (FS-ISAC)[48] is a US industry forum for co-operation on critical (physical and cyber) security threats to the financial sector. It collects and analyses information and alerts member organisations of threats and attacks in order to help the financial services sector to prepare and respond to threats. In this, the FS-ISAC cooperates with the US Department of Treasury and is the "operational arm" of the Financial Services Sector Coordinating Council (FSSCC).

275. It was established in 1999 in response to a US Presidential Directive mandating "that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure".

276. Examples of advisories include:

- Fraud advisory for business: corporate account take over (October 2010)[49];
- Fraud advisory for consumers: involvement in criminal activity through work from home scams (October 2010)[50];
- Distributed Denial of Service (DDOS) attacks: an overview and analysis (June 2010)[51].

277. Similar "ISACs" have been established in other countries.[52]

278. For example, in the Netherlands, an ISAC-style "Cybercrime Information Exchange" was established in 2006 as part of the National Infrastructure against Cybercrime (NICC) which is a public-private partnership.[53] The first to join the information exchange was the financial sector (FI-ISAC).[54] It provides a platform for the exchange of information between the National Police Services Agency (KLPD), the General Intelligence and Security Service (AIVD), the Government Computer Emergency Response Team (GOVERT.NL), banks and the Netherlands bankers' association with the NICC as a facilitator. About eight meetings are held per year. It involves exchanging information during meetings, notice and take down measures and the monitoring if threats.

279. The creation of a European-level FI-ISAC has been under discussion since 2008.[55]

---

[48] http://www.fsisac.com/

[49] http://www.fsisac.com/files/public/db/p265.pdf

[50] http://www.fsisac.com/files/public/db/p264.pdf

[51] http://www.fsisac.com/files/public/db/p244.pdf

[52] For an analysis of the challenges related to ISACs see http://www.unixworks.net/papers/wp-017.pdf
See also http://www.surfacetransportationisac.org/SupDocs/Library/ISAC_Products/isac_role_in_cip.pdf

[53] http://www.samentegencybercrime.nl/

[54] http://www.samentegencybercrime.nl/Informatie_knooppunt/Sectorale_ISACs/FIISAC?p=content
Other sectors are Water-ISAC, Energy-ISAC, Nuclear-ISAC etc.

[55] http://www.enisa.europa.eu/act/res/workshops-1/2010/information-sharing-workshop/presentations/wim
http://www.enisa.europa.eu/act/res/workshops-1/2010/information-sharing-workshop/copy_of_agenda-of-the-information-sharing-workshop

4.7.5 European Financial Coalition against Commercial Sexual Exploitation of Children Online[56]

280. The European Financial Coalition was established in 2009 as a partnership of financial, Internet and technology corporations with police agencies to "track, disrupt and to ultimately confiscate commercial gain made" by those distributing child abuse materials. The 14-months pilot phase was funded with the support of the European Union.

281. Five working groups have been established:

- Law enforcement co-operation working group;
- Payment systems monitoring and detection working group[57];
- Legal working group;
- Internet and technology working group;
- Prevention and awareness raising working group.

282. Among other things, a best Practice guide for the financial industry on the prevention and detection of commercial child abuse images has been prepared.[58]

4.7.6 Electronic Crimes Task Forces (US Secret Service)[59]

283. From October 2001, a network of Electronic Crime Task Forces as well as Working Groups were established in the USA at federal, state and local levels to prevent, mitigate and investigate attacks on financial and critical infrastructure. They bring together law enforcement, prosecutors, private industry and academia.

284. Investigations focus on priority cases meeting the following criteria:

- Significant economic or community impact;
- Participation of organized criminal groups involving multiple districts or transnational organisations;
- Use of schemes involving new technology.

4.7.7 The European Electronic Crime Task Force (EECTF)[60]

The EECTF was created in June 2009 as a result of an agreement between the Italian Post, the Italian Police and the US Secret Service. It defines its mission as follows:

---

http://www.enisa.europa.eu/act/res/workshops-1/2010/information-sharing-workshop/copy_of_agenda-of-the-information-sharing-workshop

[56] http://www.ceop.police.uk/EFC/Public-Library/Latest-News/Conference-Roundup/

[57] This group is co-chaired by VISA Europe and MasterCard and includes representatives from a number of key payment processing organisations. This working group is responsible for identifying best practice within the financial industry across Europe, ensuring that policies and procedures are in place to prevent organisers from utilising the payment systems. The group are also looking to identify how to improve relations and information exchange between the financial industry and law enforcement.

[58] http://www.ceop.police.uk/Documents/Finan%20Best%20Pract2010_080910a.pdf

[59] http://www.secretservice.gov/ectf.shtml

[60] In February 2011, the EECTF published its 2011 European Cybercrime Survey that primarily focuses on "cyberfraud".See: http://www.gcsec.org/sites/default/files/doc/CYBER_CRIME_survey.pdf

> "Support the analysis and the development of best practices against Cyber Crime in European countries through the creation of a strategic alliance between law enforcement, academia, legal, and private sector entities "

A number of European law enforcement authorities, financial sector and Internet security institutions as well as academic institutions joined this task force in the meantime. It meets quarterly and offers a trusted community to share information and identify solutions.

4.7.8 Contact Initiative against Cybercrime for Industry and Law Enforcement (CICILE)[61]

285. CICILE is a secure web-based communication platform that has been set up by the European Commission to facilitate the exchange and dissemination of information concerning the prevention of and the fight against cybercrime between stakeholders, such as law enforcement, government agencies, the private sector and NGOs. While this community is hosted by the European Commission, it is managed by its members.

286. CICILE is based on the existing platform SYNAPSE. SINAPSE is a web communication platform offering tools to promote a better use of expertise in EU policy making and governance (networking of advisory bodies, support to expert groups, ad-hoc/public consultations and e-debates, etc.). SINAPSE is a free public service of the European Commission. SINAPSE in particular allows the creation of "e-Communities" which enables groups of members and organisations with a common interest to share and exchange information in a dedicated environment which can be graphically personalised and linked to the initiator website.

4.7.9 Guidelines for law enforcement/ISP co-operation in the investigation of cybercrime

287. Cooperation between law enforcement authorities and Internet service providers is of crucial importance in the investigation of cybercrime

288. In 2008, the Octopus Conference organised by the Council of Europe under the Global Project on Cybercrime adopted guidelines[62] to help law enforcement and ISPs structure their co-operation. They:

- include common guidelines for both law enforcement and service providers and specific guidelines for each of them;
- are not to substitute legislation or other formal regulations, but rather to supplement and help regulations work in practice;
- are based on good practices already available;
- are to be adapted to the specific circumstances in each country.

289. In practical terms, representatives of law enforcement and service providers in a given country may establish a working group with the aim of reaching an understanding or even a formal agreement on how to cooperate with each other. The guidelines could serve as a blue-print or simply as a basis for discussion.

290. Following the adoption of these guidelines in April 2008:

[61] Information provided by the European Commission.

[62] http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp

- The European Court of Human Rights referred to them and specifically to the need for a "culture of co-operation" between law enforcement and ISPs in its judgment K.U. v. Finland (application no. 2872/02)[63].
- the European Union's Justice and Home Affairs Council in November 2008[64] recommended that the European Commission work on the basis of the guidelines adopted by the Council of Europe conference and took note of eight specific recommendations.
- the Government of Romania decided in January 2009 that judicial, law enforcement and regulatory bodies should make use of these guidelines. They were posted on the websites of the Ministry of Justice, the Office the Prosecutor General, the Ministry of Interior and other bodies.
- the Ministry of Interior of France and the French Internet service provider association AFA drafted an agreement based on the guidelines in Ukraine a working group was established in July 2009 to reach an agreement between law enforcement and service providers.
- in India the guidelines were presented to law enforcement and industry (March 2009) in view of the amendments to the Information Technology Act adopted by Parliament in December 2008 (see presentation).
- In Georgia, a memorandum of understanding was signed between the Ministry of Interior and ISPs in May 2010.

4.8 Training

4.8.1 The European Cybercrime Training and Education Group (ECTEG)[65]

291. This group manages the accredited cybercrime training materials developed under various European Union (AGIS and ISEC) funded law enforcement only training programmes, including:

- A two week introductory course basic skills for forensic investigators;
- NTFS forensics;
- Network Investigations;
- Internet Investigations;
- Linux as an investigative tool;
- Wireless LANs and VoIP;
- Mobile Phone Forensics;
- Live data forensics (under development);
- Advanced Scripting (under development);
- Malware investigation (under development);
- Visa Forensics (due for development in 2010);
- Data mining and databases (due for development in 2010);
- Advanced mobile phone forensics (due for development in 2010).

[63] http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/LEA_ISP/1429_ECHR_CASE_OF_K.U._v%20Finland.pdf
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp
For an interesting example of self-regulation see the Austalian Internet Code of Good Practice http://iia.net.au/images/resources/pdf/icode-v1.pdf

[64] http://www.eu2008.fr/webdav/site/PFUE/shared/import/1127_JAI/Conclusions/JHA_Council_conclusions_Cybercrime_EN.pdf

[65] http://www.ecteg.eu/

292. University College Dublin (Centre for Cybercrime Investigations) continues to accredit the training and education programme that is run under the auspices of ECTEG.

4.8.2 The University College Dublin Centre for Cybercrime Investigation (UCD CCI)

293. UCD has been involved in efforts to harmonise law enforcement cybercrime training since 2001. The CCI was formally established in 2006 with the stated aims of:

- Developing, delivering and maintaining accredited cybercrime education programmes for cybercrime investigators/security specialists charged with the prevention and investigation of high tech crime.
- Carrying out applied and theoretical research into cybercrime and publish the results for the benefit of cybercrime investigators/security specialists in the prevention and detection of high tech crime.
- Developing, validating and maintaining software tools for use by cybercrime investigators/security specialists in the prevention and fight against high tech crime.
- Working in partnership with other stakeholders in the area of cybercrime prevention and detection.

294. The CCI has had success by engaging with law enforcement and industry stakeholders both nationally and internationally.

295. One tangible result has been the law enforcement only MSc in Forensic Computing and Cybercrime Investigation provided by UCD CCI. To date, over 110 students have completed, or are currently enrolled in, this course. Students are from Ireland, UK, Germany, France, Italy, Greece, Spain, Norway, Sweden, Netherlands, Romania, Denmark and Cyprus. From outside Europe there are students from Ghana, United Arab Emirates, China, Japan, USA, Canada, New Zealand, Singapore and Hong Kong. As well as being the culmination of almost 15 years of efforts to harmonise cybercrime training for law enforcement, one of the key advantages of this type of programme is the community of alumni that have developed and the fact that knowing law enforcement officers in other jurisdictions facilitates international co-operation.

296. It is believed that law enforcement authorities of each country should have a minimum level of capability to react to cybercrime. Training and education programmes for police are a precondition.

4.8.3 South-eastern Europe – law enforcement training strategies

297. The CyberCrime@IPA joint project of the Council of Europe and the European Union supports countries in the preparation of comprehensive law enforcement training strategies for cybercrime investigations and computer forensics.[66]

4.8.4 Council of Europe training concept for judges and prosecutors

298. One of the lessons learned from strategies against money laundering and the financing of terrorism is the need for the training of judges. Based on the assumption that particular efforts are required to enable judges and prosecutors to prosecute and adjudicate cybercrime and make use of electronic evidence through training, networking and specialisation, the Council of Europe – under the

66 http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Cyber%20IPA%20reports/2467_LEA_Training_Strategy_Fin1.pdf

Global Project on Cybercrime and the Lisbon Network of judicial training institutions – in 2009 adopted a "concept for cybercrime training for judges and prosecutors".[67]

299. Its purpose is to help judicial training institutions develop training programmes on cybercrime and electronic evidence for judges and prosecutors and to integrate such training in regular initial and in-service training. The elements of the concept include:

- Institutionalising initial training;
- Institutionalising in-service training;
- Standardised and replicable courses/modules;
- Access to training/self-training materials;
- Pilot centres for basic and advanced training;
- Enhancing knowledge through networking;
- Public private co-operation.

300. Implementation of this concept is now underway, for example, in South-eastern Europe with support of the CyberCrime@IPA project.[68]

[67] http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Training/default_en.asp

[68] See www.coe.int/cybercrime

5 FINDINGS

301. 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.

5.1 Cybercrime and criminal money flows

302. 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.

303. 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.

304. 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.

305. 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.

5.2 Money laundering and cybercrime issues

306. 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 undetected 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 offences[69] may result in excluding certain proceeds-generating types of cybercrime from qualifying as predicate offences for money laundering.
- 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.

[69] 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

- 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.

5.3 Conclusion and direction for development

307. 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:

308. *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.

309. *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.[70]

[70] 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

310. *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.[71]

311. *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.

312. *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.

313. *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 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.

314. *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. The participation of cybercrime investigators in permanent or temporary multi-disciplinary groups specialised in financial or asset investigations should be considered.[72] 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.[73] 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

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

[72] Further to FATF Recommendation 30 (as revised, February 2012)

[73] FATF Recommendations 30 and 31 (as revised, February 2012) should encourage cooperation and information exchange between FIUs and law enforcement, including cybercrime investigators.

jurisdictions particularly affected by these phenomena.[74] In many jurisdictions, prosecutors may play a major role in coordinating different agencies in specific investigations.

315. *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

316. *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.

317. *International cooperation*. Linking anti-money laundering and terrorist financing measures and financial investigations with cybercrime investigations and computer forensics offers added opportunities for international cooperation. International standards – such as Council of Europe Convention CETS 198, FATF Recommendations or the Budapest Convention on Cybercrime – offer opportunities that are yet to be fully exploited.[75] For example, provisional measures in international cooperation on money laundering and financial investigations (articles 21 to 22 of the Warsaw Convention, or FATF Recommendation 38) could be accompanied by provisional measures to preserve electronic evidence not only by Internet service providers but also other legal or physical persons (Budapest Convention -articles 16 and 17 for preservation at the domestic level and articles 29 and 30 at the international level). This also applies, *modus modendi*, to other forms of international cooperation. FATF Recommendation 40 specifically encourages countries to "permit their competent authorities to exchange information indirectly with non-counterparts".[76] This should allow for information exchange between an FIU of one country with a cybercrime unit of another country either via the FIU of the other country or in urgent cases directly.

[74] As proposed in FATF Recommendation 31 (as revised, February 2012).

[75] See FATF Recommendation 36 (as revised, February 2012).

[76] See paragraph 17 of the Interpretative Note on FATF Recommendation 40 (as revised, February 2012).

6 APPENDIX

6.1 Study concept note

Concept note[77]

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

Led by: Russian Federation and the Council of Europe Secretariat (MONEYVAL Secretariat & Project on Cybercrime & MOLI Russia Project)

Description:

This project will examine criminal money flows and methods of money laundering through information and communication technologies (ICT), including the Internet. It will furthermore document good practices such as multi-stakeholder action aimed at the search and confiscation of crime proceeds and prevention.

Issues:

Cybercrime is increasingly targeted at generating economic proceeds involving different types of fraud and economic crime (such as phishing and other forms of identity theft, credit card fraud, auction fraud, Internet marketing and retail fraud, online gambling, lottery fraud, intellectual property and related offences, stock market manipulation, advance fee fraud, extortion, espionage, insider trading, electronic trade in stolen goods and many others) through illegal access, data interception, data and system interference and with the help of malware, including botnets and spam. The Internet and information and communication technologies facilitate money laundering and the financing of terrorism. Commercial websites and Internet payment systems are vulnerable to money laundering and terrorist financing as documented by the FATF.[78] Criminals may receive money to their own accounts or accounts which they control and from where they can withdraw it, or through accounts of beneficial owners in different countries, or through e-money, or they launder proceeds through e-gold, e-casinos, Internet auctions or similar methods. All these crimes are highly transnational in nature.

A wide range of stakeholders is involved in measures against such forms of crime not only from the public sector but in particular the private sector. Although there are examples of multi-stakeholder action, efforts remain rather fragmented. Initiatives against fraud on the Internet are not necessarily linked to activities carried out by financial intelligence units or law enforcement authorities responsible for financial investigations.

Better knowledge of methods used for fraud, money laundering and terrorist financing on the Internet through exchange of information between relevant public and private sector stakeholders will help investigate, seize and confiscate proceeds and prevent fraud, money laundering and terrorist financing.

[77] Approved by the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) in September 2009.

[78] Financial Action Task Force: MONEY LAUNDERING & TERRORIST FINANCING VULNERABILITIES OF COMMERCIAL WEBSITES AND Internet PAYMENT SYSTEMS (June 2008). The project will also take into account and coordinate with the ongoing work of the FATF on ML and TF through new payment methods.

Objective of the project:

The objective of the project is:

- to examine specific ML/TF risks and methods, trends and typologies
- to develop indicators to identify criminal money flows and money laundering on the Internet
- to identify possible solutions with regard to multi-stakeholder action aimed at preventive measures, the seizure and confiscation of criminal money and the investigation of money laundering and terrorist financing on the Internet.

Potential resources required:

The project team will ideally include experts from FIUs, financial investigation services and high-tech crime units. It will consult with key stakeholders from the private sector so that they can contribute their experience to the project.

The project team's work will be assisted by one to two experts (one money laundering/financial investigation expert, one experienced in high-tech crime) who will support the Project Leader and Secretariat to coordinate the process and contributions from stakeholders.

Co-operation between MONEYVAL and the Council of Europe's Projects on Cybercrime and MOLI Russia will permit a pooling of resources and expertise as well as access to different stakeholders.

Planned product:

The project team will draw up a report consisting of two main parts:

- Typologies: this part will document identified methods and trends of ML through the Interned, based on case studies contributed by participating countries and indicators/red flags developed.
- Good practices: the second part will document good practices in terms of counter-measures, that is, strategies, policies and investigative techniques. It should in particular provide information and guidance on multi-stakeholder action involving financial intelligence units, financial investigators, high-tech crime units and the private sector (ICT industry, financial sector etc.).

If you have any questions regarding this project, please contact:

Alexander Seger
Economic Crime Division
DG of Human Rights and Legal Affairs
Council of Europe
F-67075 Strasbourg CEDEX
Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email: alexander.seger@coe.int

Livia Stoica Becht
MONEYVAL Secretariat
Directorate of Monitoring
DG of Human Rights and Legal Affairs
Council of Europe, F-67075 Strasbourg CEDEX
Tel. +33-3-9021-4260 / Fax +33-3-8841-3017
E-mail: dghl.moneyval@coe.int

6.2 References[79]

Brunst, Philip/Sieber, Ulrich (2010): Cybercrime legislation. In: Basedow, J./Kischel, U./Sieber, U. (eds): German National Reports to the 18th International Congress of Comparative Law, Washington 2010.

Bundeskriminalamt[80] (2010): FIU Jahresbericht 2009. Wiesbaden.
http://www.bka.de/profil/zentralstellen/geldwaesche/pdf/fiu_jahresbericht_2009.pdf

Bundeskriminalamt (2010a): IUK-Kriminalität – Bundeslagebild 2009. Wiesbaden.
http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_2009.pdf

Castells, Manuel (2000): The Rise of the Network Society. Malden/Oxford/Carlton (Second edition).

Commtouch Internet Threats Trend Report Q1 2010.
www.commtouch.com/download/1679

Council of Europe (2002): Organised Crime Situation Report 2001. Strasbourg (Committee PC-S-CO).
http://www.coe.int/t/dghl/co-operation/economiccrime/organisedcrime/Report2001E.pdf

Council of Europe (2003): Organised Crime Situation Report 2002. Strasbourg (Committee PC-S-CO).
http://www.coe.int/t/dghl/co-operation/economiccrime/organisedcrime/PC-S-CO%20_2003_%207%20E%20OC-Report%202002-Provisional.pdf

Council of Europe (2004): Organised Crime Situation Report 2004 – Focus on the threat of cybercrime. Strasbourg (Octopus Programme).
http://www.coe.int/t/dghl/co-operation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf

Council of Europe (2005): Organised Crime Situation Report 2005 – Focus on the threat of economic crime. Strasbourg (Octopus Programme).
http://www.coe.int/t/dghl/co-operation/economiccrime/organisedcrime/Report2005E.pdf

Council of Europe (2005a): Convention on the Laundering, Search, Seizure and Confiscation of Proceeds from Crime and the Financing of Terrorism (CETS 198).
http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=198&CM=8&DF=05/12/2010&CL=ENG

Council of Europe (CyberCrime@IPA) (2011): Law Enforcement Training Strategies. Strasbourg.
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Cyber%20IPA%20reports/2467_LEA_Training_Strategy_Fin1.pdf

Council of Europe (Global Project on Cybercrime) (2008): Guidelines for the co-operation between law enforcement and Internet service providers against cybercrime. Strasbourg.
http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp

Council of Europe (Global Project on Cybercrime) (2010): The Internet domain name registration process – from the registrant to ICANN. Strasbourg (report prepared by Wolfgang Kleinwächter)

[79] Selected list only. See also footnotes in the text.

[80] German Federal Criminal Police Office.

http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_wolfgangkleinwaechter1.pdf

Council of Europe (Global Project on Cybercrime) (2010a): Cybercrime training for judges and prosecutors – A concept. Strasbourg.
http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Training/default_en.asp

Council of Europe (Global Project on Cybercrime) (2011): Cybercrime Strategies. Strasbourg.
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf

CyberCrime@IPA/EU Cyber Crime Task Force/Global Project on Cybercrime (2011): Specialised Cybercrime Units – Good Practice Study. Council of Europe, Strasbourg.
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf

Deutsche Gesellschaft für Technische Zusammenarbeit (GTZ) (1998): Drugs and Development in Asia (Eschborn). http://www2.gtz.de/dokumente/bib/99-0026.pdf

Europol (2007): High tech Crimes within the EU: Old crimes new tools, new crimes new tools. Threat assessment 2007. The Hague.
http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf

Financial Action Task Force (2008): Money Laundering & Terrorist Financing Vulnerabilities Of Commercial Websites And Internet Payment Systems. Paris.
http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf

Financial Action Task Force (2010): Money Laundering Using New Payment Methods. Paris.
http://www.fatf-gafi.org/dataoecd/4/56/46705859.pdf

Financial Fraud Action UK (2010): Fraud the Facts 2010 – The definite overview of payment industry fraud and measures to prevent it
http://www.ukpayments.org.uk/files/fraud_the_facts_2010.pdf

Friedman, Thomas L. (2006): The World is Flat. London.

G Data Whitepaper 2009: Underground Economy.
http://www.gdata-software.com/uploads/media/Whitepaper_Underground_Economy_8_2009_GB.pdf

Information Warfare Monitor/Shadowserver Foundation (2010): Shadows in the Cloud – Investigating Cyber Espionage 2.0. http://www.nartv.org/mirror/shadows-in-the-cloud.pdf

Internet Crime Complaint Center (2010): Internet Crime Report 2009.
http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

Koops, Bert-Jaap/Leenes, Ronald (2006): Identity Theft, Identity Fraud and/or Identity-related Crime. In: Datenschutz und Datensicherheit 30 (2006) 9.
http://www.fidis.net/fileadmin/fidis/publications/2006/DuD09_2006_553.pdf

M 86 Security (2010): White Paper: Cybercriminals Target Online Banking Customers (August 2010)
http://www.m86security.com/documents/pdfs/security_labs/cybercriminals_target_online_banking.pdf

Microsoft Security Intelligence Report, Volume 9, January through June 2010
http://www.microsoft.com/security/sir/

OECD (2007): Malicious Software (Malware) – A security threat to the Internet Economy.
http://www.oecd.org/dataoecd/53/34/40724457.pdf

Schmidt, Howard (2006): Patrolling Cyberspace. North Potomac.

Seger, Alexander (2007): Identity Theft and the Convention on Cybercrime. In: Demosthenes Chryssikos, Nikos Passas, Christopher D. Ram (eds.): The evolving challenge of identity-related crime: addressing fraud and the criminal misuse and falsification of identity (UN ISPAC).
http://www.ispac-italy.org/pubs/ISPAC%20-%20Identity%20Theft.pdf

Sophos Security Threat Report 2010 (August 2010).
http://www.sophos.com/security/topic/security-report-2010.html

UNODC (2010), The Globalization of Crime - A transnational organised crime threat assessment at http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf