



Project funded by  
the European Union



**T06**

**PROGRAMME**

**Enquêtes Financières - Avancé**  
UE/MENA Partenariat pour la Formation à la Lutte Anti-terroriste  
(CEPOL CT 2)  
DG Formation, Sûreté Nationale  
24-27 juin 2019  
Tunis, Tunisie

	<b>Jour 1 24 juin</b>	<b>Jour 2 25 juin</b>	<b>Jour 3 26 juin</b>	<b>Jour 4 27 juin</b>
09:00	Bienvenue et Introduction de CEPOL	Coopération inter-institutionnelle: Police, Interpol, Europol	Bureaux de transfert d'argent et autres systèmes bancaires informels	Comptabilité forensic
09:45	Introduction à la méthodologie de la formation et présentation de la cas d'étude	Exercice Pratique Enregistrer pour entraide judiciaire	Western Union	
10:30	Pause-café	Pause-café	Pause-café	Pause-café
10:45	Exercice Pratique Développement d'une stratégie des enquêtes financières	Exercice Pratique Obtenir d'information/prévue de l'étranger	Western Union	Exercice Pratique Analyse de l'information financière
11:30	Exercice Pratique Profilage financières des suspects, création d'une équipe d'investigation	Exercice Pratique Gardiens (avocats, comptables)	Western Union	Exercice Pratique Analyse de l'information financière
12:30	Déjeuner	Déjeuner	Déjeuner	Déjeuner
13:30	CTAF comme un élément essentiel du système de renseignement financier	Information des banques	Coopération Internationale	Etude d'apprentissage
14:30	Pause-café	Pause-café	Pause-café	Pause-café



Project funded by  
the European Union



14:45	CTAF comme un élément essentiel du système de renseignement financier	Exercice Pratique Formation d'une société, l'usage de véhicules de corporations offshore	Exercice Pratique Gestion de cas et Financement du terrorisme – Contrebande d'espèces	Localisation et récupération de biens	Evaluation de la formation
15:30					
16:30	Fin des sessions			Fin des sessions	Fin des sessions

Project funded by  
the European Union



EU/MENA COUNTER-TERRORISM  
TRAINING PARTNERSHIP 2  
FINANCIAL INVESTIGATIONS - ADVANCED  
PARTICIPANT LIST



Name	Surname	Department
		DG Training
		DG Training
		DG Special Services
		DG Training
		DG Technical Services - Financial Investigations
		DG Technical Services - Financial Investigations
		Financial Brigade
		DG Training
		DG Training
		Financial Brigade
		National Unit for the Investigation of Terrorist Crimes
		Headquarters
		Financial Brigade
		Financial Brigade
		Financial Brigade



The cover features a blue-tinted photograph of a person writing on a document. The CEPOL logo is in the top left corner. The title 'Financial Investigation Case Study' is prominently displayed in the center, with the location 'Salamambo, Tunis' and dates '23-27 June 2019' below it. At the bottom, the text 'EUROPEAN AGENCY FOR LAW ENFORCEMENT TRAINING' is visible.

CEPOL

**Financial Investigation Case Study**  
Salamambo, Tunis  
23-27 June 2019

EUROPEAN AGENCY FOR LAW ENFORCEMENT TRAINING



The slide has a black background with a white rectangular area in the center containing the text 'This information cannot be disclosed due to public security'. The CEPOL logo is in the bottom right corner, and a small blue square with the number '7' is in the bottom left corner.

This information cannot be disclosed due to public security

CEPOL


7

This information cannot be disclosed due to public security



This information cannot be disclosed due to public security





This information cannot be disclosed due to public security

CEPOL

5



This information cannot be disclosed due to public security

CEPOL

6



This information cannot be disclosed due to public security



2




This information cannot be disclosed due to public security



3

This information cannot be disclosed due to public security



This information cannot be disclosed due to public security







This information cannot be disclosed due to public security



11



This information cannot be disclosed due to public security



12

This information cannot be disclosed due to public security




33

This information cannot be disclosed due to public security




34

This information cannot be disclosed due to public security



15

This information cannot be disclosed due to public security



16

This information cannot be disclosed due to public security




17

This information cannot be disclosed due to public security





18

This information cannot be disclosed due to public security



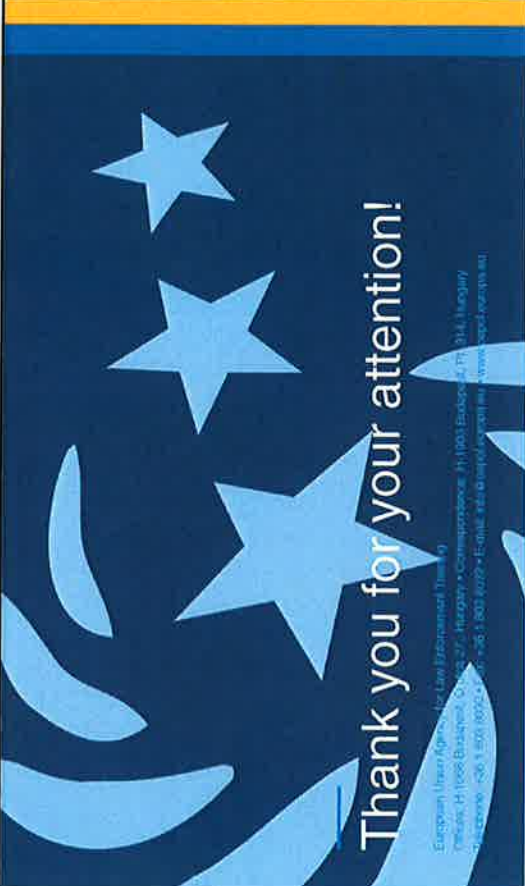
This information cannot be disclosed due to public security



This information cannot be disclosed due to public security




21

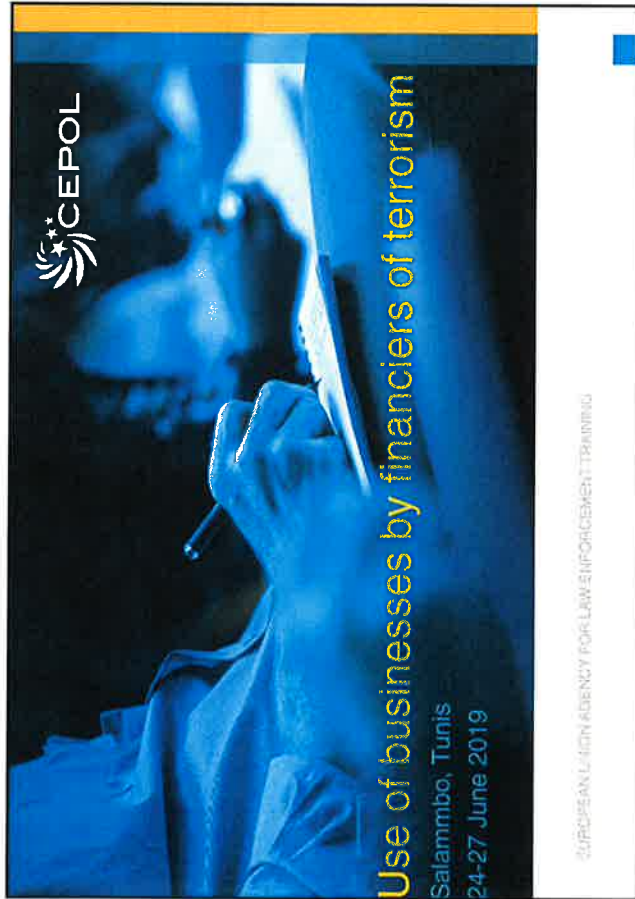


Thank you for your attention!

European Union Agency for Law Enforcement Training  
Társaság, H-1098 Budapest, Szabadság tér 27. - Házaspárk • Contact Centre: H-1003 Budapest, Tűz 31A, Hungary  
Tel: +36 (0)6 3 590 1000 • Fax: +36 3 590 1009 • E-mail: [info@cepola.eu](mailto:info@cepola.eu) • [www.cepola.eu](http://www.cepola.eu)



22



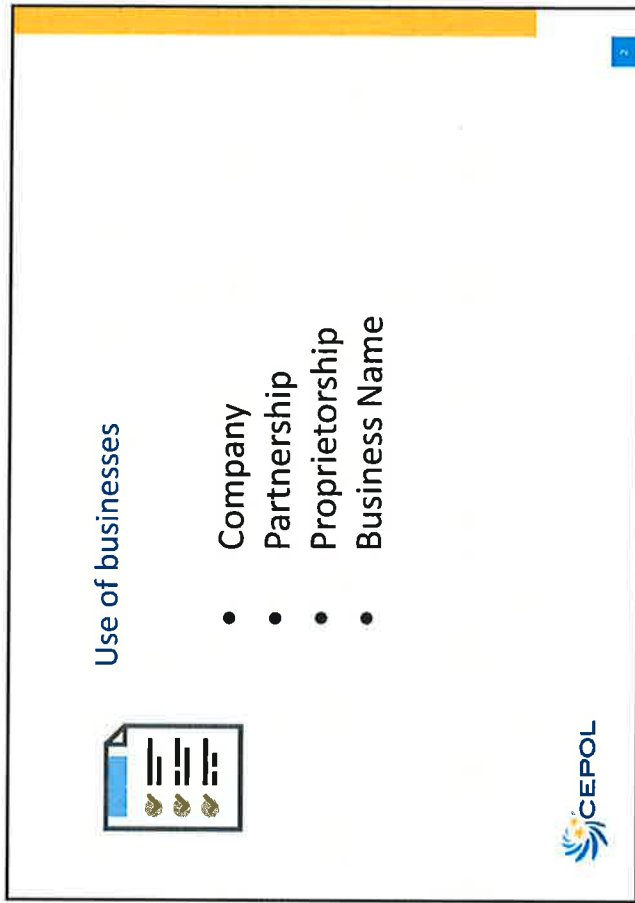
The image shows the cover of a training document. The background is a blue-tinted photograph of a person's hands writing on a notepad. The CEPOL logo is in the top left corner. The title 'Use of businesses by financiers of terrorism' is written in yellow and white text. Below the title, the location 'Salammbou, Tunis' and dates '24-27 June 2019' are listed. At the bottom, it says 'EUROPEAN AGENCY FOR LAW ENFORCEMENT TRAINING'.

CEPOL

**Use of businesses by financiers of terrorism**

Salammbou, Tunis  
24-27 June 2019

EUROPEAN AGENCY FOR LAW ENFORCEMENT TRAINING




The slide features a document icon with three gold coins on the left. The title 'Use of businesses' is centered. To the right is a bulleted list. The CEPOL logo is in the bottom right corner.

Use of businesses

- Company
- Partnership
- Proprietorship
- Business Name


CEPOL



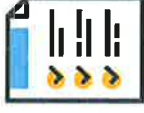
### Company

There are various types of company that can be formed in different jurisdictions, but the most common forms of company (generally formed by registration under applicable companies legislation) are:

- A company limited by guarantee
- A company limited by shares
- A limited liability company
- An unlimited liability company




3



### INCORPORATED BUSINESS

- SEPARATE LEGAL ENTITY
  - LIKE A PERSON AT LAW
- FILE SEPARATE TAX RETURNS
- MINUTE BOOKS SHOW OWNERSHIP, WHO OPERATES COMPANY, SIGNING AUTHORITY ON BANK ACCOUNTS AND SHARES ISSUED



4





### Partnership

A partnership is a type of business entity in which partners (owners) share with each other the profits or losses of the business undertaking in which all have invested.


- **TWO OR MORE PERSONS**
- **EQUALLY LIABLE**
- **MAY USE A TRADESTYLE**
- **ONE RESPONSIBLE FOR DECISIONS OF THE OTHER**



### Proprietorship


A business structure in which an individual and his/her company are considered a single entity for tax and liability purposes. A proprietorship is a company which is not registered with the state as a limited liability company or corporation.






### Sole Proprietorship

- **INDIVIDUAL CARRYING ON BUSINESS**
- NOT INCORPORATED
- **MAY USE A TRADESYTLE**
- **IS PERSONALLY RESPONSIBLE FOR DEBTS**




7




### Terrorist Finances

**IDENTIFYING AND TRACKING ILLICIT FUNDS THROUGH ACCOUNTING RECORDS**




8




**REQUIRED RECORDS**

- **CORPORATE STRUCTURE**
  - **WHO IS OPERATING MIND**
    - **DAILY DIARY**
- **GENERAL JOURNAL**
- **PURCHASE JOURNAL**
- **SALES JOURNAL**
- **FINANCIAL STATEMENTS**
- **LEDGERS**




9



**REQUIRED RECORDS**

- **BANK STATEMENTS**
  - **US BANK ACCOUNTS**
  - **WIRE TRANSFERS**
  - **DEBIT / CREDIT MEMOS**
- **CHEQUE REGISTER**
- **CANCELLED CHEQUES**
- **DEPOSIT BOOKS**
- **CASH RECEIPT BOOKS**
- **SOURCE DOCUMENTS**
- **ACCOUNTANTS WORKING PAPERS**





10

This information cannot be disclosed due to public security




11

This information cannot be disclosed due to public security




12

This information cannot be disclosed due to public security





13

This information cannot be disclosed due to public security





14

This information cannot be disclosed due to public security




15

This information cannot be disclosed due to public security




16

11




This information cannot be disclosed due to public security




12

12



This information cannot be disclosed due to public security




13

This information cannot be disclosed due to public security



13


This information cannot be disclosed due to public security



14





This information cannot be disclosed due to public security



21

This information cannot be disclosed due to public security



22


This information cannot be disclosed due to public security

33

**Remember**


**OTHER CRIMINAL OFFENCES  
MONEY LAUNDERING, FRAUD,  
FORGERY, OTHER RELATED PROPERTY  
OFFENCES**

34




Thank you for your attention!

European Union Agency for Law Enforcement Training  
Zrínyi u. 110/2 Budapest, H-1052 \* Hungary \* Erzsébet körút 110/2 Budapest, H-1052 \* Hungary  
Tel: +36 1 402 6992 Fax: +36 1 402 6922 E-mail: [info@cepola.eu](mailto:info@cepola.eu) [www.cepola.eu](http://www.cepola.eu)




**Financial Analysis**  
Salammbou, Tunisia  
23-27 June 2019

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING




### Concealed Income Analysis


- Financial gain is a primary motive in complex criminal activity.
- Retention of the money acquired, without detection, is an associated motive for those involved in the activity.
- Skills in concealed income analysis are important to the analysis of most types of criminal activity, and to the analysis of terrorism finances, organized crime, and related conspiracies in particular.




### Concealed Income Analysis




The purpose of concealed income analysis is to determine the extent to which a person, group, or organization is receiving and benefiting from money obtained from other than legitimate sources.




### Concealed Income Analysis



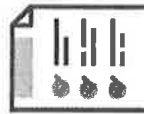

Concealed income analysis can be used both for developing hypotheses and testing hypotheses.



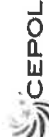


### Four types of inferences


- 1. Hypothesis:**
  - A tentative explanation; a theory that requires additional information for confirmation or denial.
- 2. Conclusion:**
  - An explanation that is well supported; an hypothesis that has been confirmed and which can be acted upon.



- 3. Prediction:**
  - An inference about something that will happen in the future.
- 4. Estimation:**
  - An inference made from a sample to the whole, typically quantitative in nature—amount of money, time required, size of operation, and so on.




### Definition of Financial Terms



**Asset**

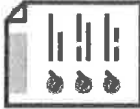
Anything of value that can be converted to cash, or cash itself.

- Real Property
- Personal Property
- Securities investments
- Savings & Checking Accounts



7


### Definition of Financial Terms




**Liability**

A written or oral agreement covering a financial obligation to pay.

- Short-Term
- Long-Term



6

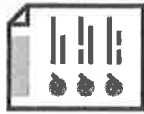



### Definition of Financial Terms


**Net Worth**  
Total liabilities subtracted from total assets at a given point in time.

**Income**  
Money received for services or work, including dividends, interest, returns from rentals and other investment returns.

**Expenses**  
Living costs and/or the costs of doing business.



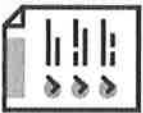
This information cannot be disclosed due to public security



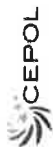


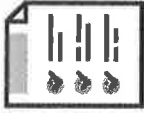


This information cannot be disclosed due to public security

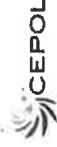


This information cannot be disclosed due to public security






This information cannot be disclosed due to public security




13

### Assessment of Net Worth


- A financial profile begins with a determination of net worth.
- Net worth is the individual's total assets less total liabilities at a given point in time.
- This is expressed in the following formula:

$$\text{Assets} - \text{Liabilities} = \text{Net Worth}$$



14




	1999	2000	2001
<b>ASSETS (A)</b>			
Home	\$85,000	\$85,000	\$85,000
Auto	7,200	7,200	10,400
Boat	11,000	11,000	11,000
Diamond Ring	4,000	4,000	4,000
Stocks	6,000	10,000	15,000
Etc.			
<b>TOTAL</b>	<b>\$113,200</b>	<b>\$117,200</b>	<b>\$125,400</b>
<b>LIABILITIES (L)</b>			
Mortgage	\$85,000	\$50,000	\$15,000
Auto Loan	5,000	2,000	-
Boat Loan	7,000	4,000	1,000
Etc.			
<b>TOTAL</b>	<b>77,000</b>	<b>\$56,000</b>	<b>\$16,000</b>
<b>NET WORTH (A—L)</b>	<b>\$36,200</b>	<b>\$61,200</b>	<b>\$109,400</b>




## NET WORTH TRUTH TABLE





ASSETS STATUS	LIABILITIES STATUS	EFFECT ON NET WORTH
assets increase and assets decrease	liabilities stay the same	net worth will increase
assets increase	liabilities decrease	net worth will increase
assets stay the same	liabilities decrease	net worth will increase
assets stay the same	liabilities increase	net worth will decrease
assets decrease	liabilities stay the same	net worth will decrease






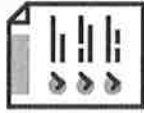


As of Date Year 1		As of Date Year 2		As of Date Year 3	
Assets		Assets		Assets	
Liabilities		Liabilities		Liabilities	
Net Worth Year 1		Net Worth Year 2		Net Worth Year 3	
		Net Worth Year 1		Net Worth Year 2	
		Change in NW For Year 2		Change in NW For Year 3	
		Living Expenses For Year 2		Living Expenses For Year 3	
		Total Outlay For Year 2		Total Outlay For Year 3	
		Known Income For Year 2		Known Income For Year 3	
		Income From Unidentified Sources For Year 2		Income From Unidentified Sources For Year 3	

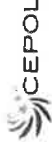



	1999	2000	2001
Net Worth	\$36,200	\$61,200	\$109,400
Change in Net Worth	XXXXX	25,000	48,200
Expenses	XXXXX	+65,000	+80,000
TOTAL	XXXXX	\$90,000	\$128,200
Income	XXXXX	52,000	53,800
CONCEALED INCOME	XXXXX	\$38,000	\$74,400





This information cannot be disclosed due to public security

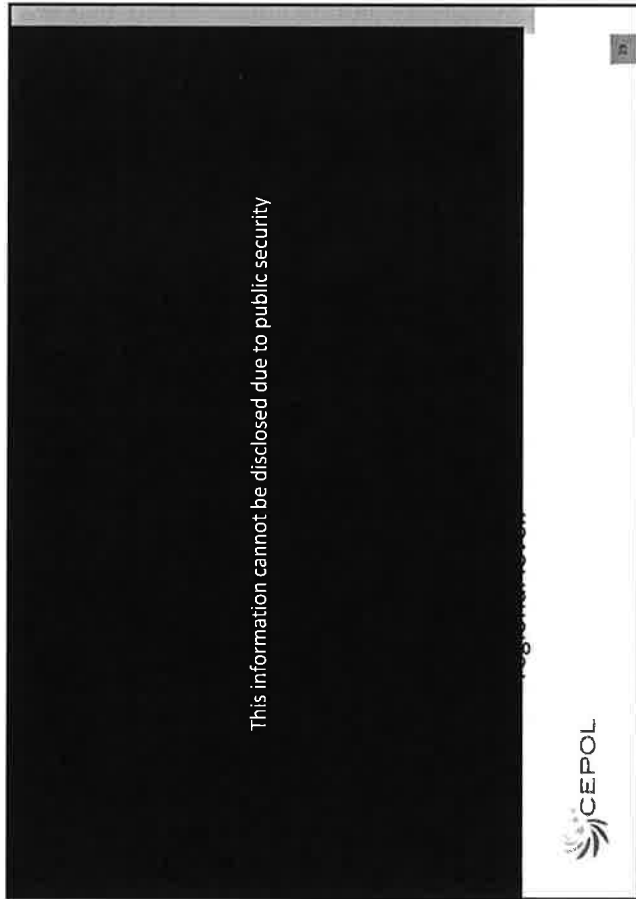


5


This information cannot be disclosed due to public security



7



This information cannot be disclosed due to public security




Thank you for your attention!

European Union Agency for Criminal Justice Cooperation  
Offices: H-1066 Budapest, Ö. Buda, 2/2. Híd utca • Budapest, HU 1066  
Telephone: +36 1 903 8030 • Fax: +36 1 903 8031 • Web: [www.cepola.eu](http://www.cepola.eu)









**Mutual Legal Assistance**  
Salammbô, Tunis  
24-25 June 2019

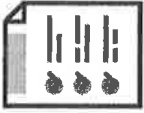
EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING



**Mutual Legal Assistance – Why?**

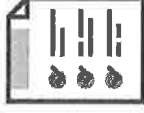

- Crime does not respect borders;
- Criminals use borders to hide;
- To counter that we need to work with different countries and understand different countries system;
- Communication is key;
- Professional relationships are important (knowing who to contact).






### Mutual Legal Assistance – What can be requested?

- Depends on treaties and laws of countries involved;
- Intelligence gathered by the parties;
- Assistance on investigations and gathering evidence;
- Assistance in getting the evidence presented;
- Extradition;
- Repatriation of money;
- Implementation of ancillary orders.



### Mutual Legal Assistance – Types of MLAT Agreements

- International convention;
- Local law which implements international agreement;
- Bi-lateral agreement between two countries.





### Mutual Legal Assistance – Factors which limit assistance

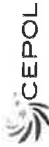
- The limit of the statute under MLAT – but you also have the principle of reciprocity;
- What is allowed by the implementing countries laws;
- The capability of the country you are requesting from – cannot request a video link from a country that doesn't have the technology;
- Speed of response;
- The relationship between the countries involved.



This information cannot be disclosed due to public security

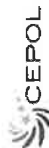


This information cannot be disclosed due to public security

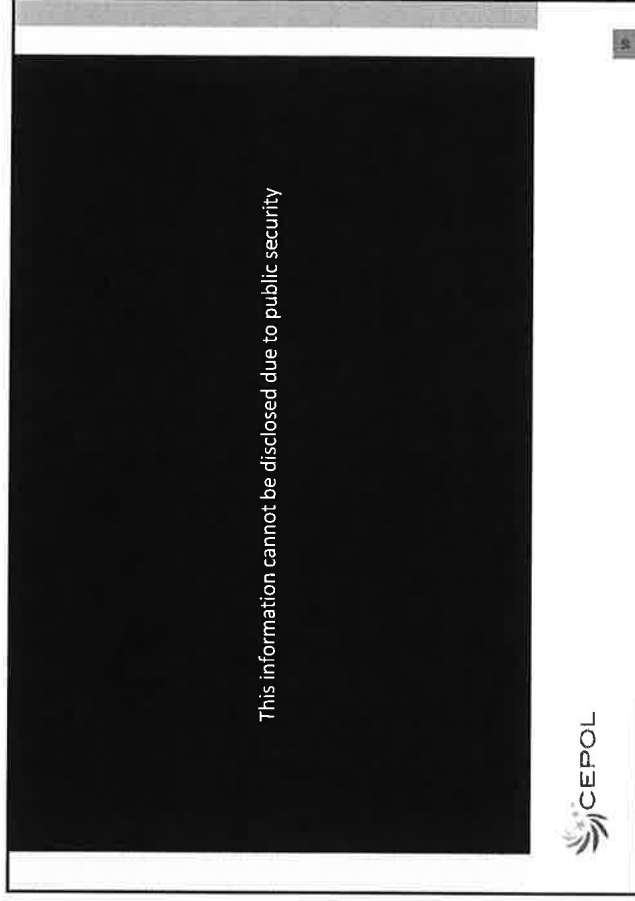


7

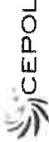
This information cannot be disclosed due to public security



8

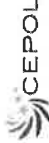


This information cannot be disclosed due to public security

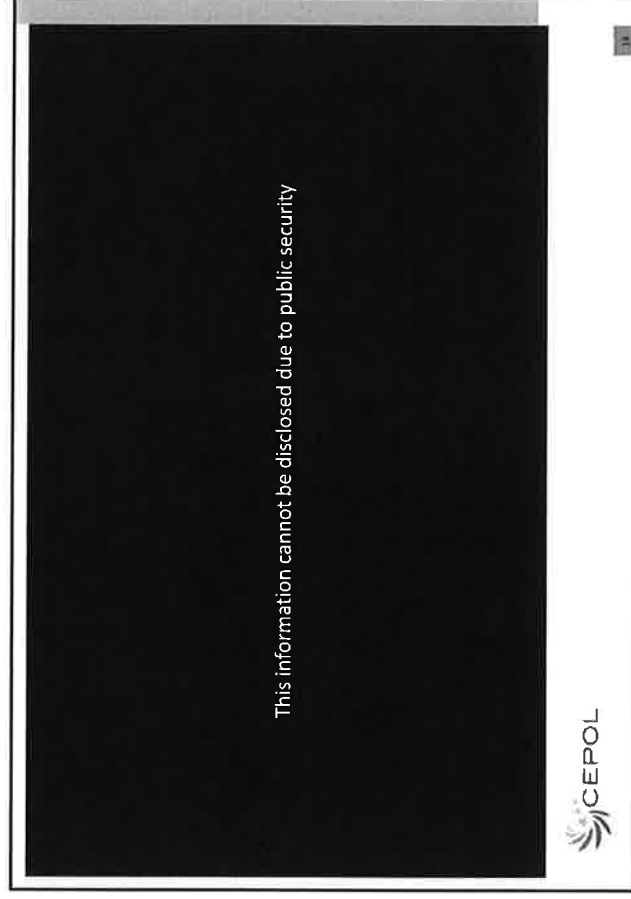
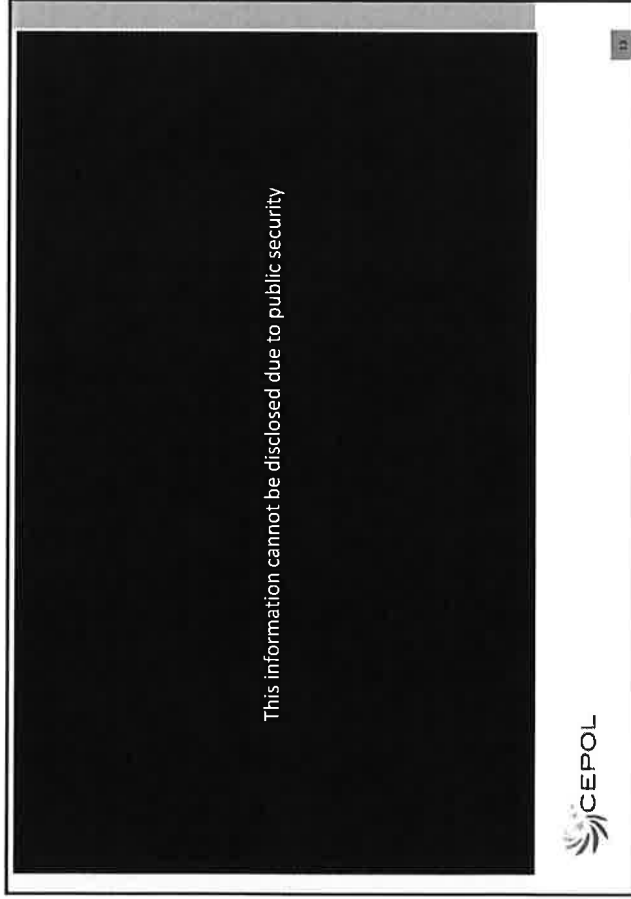


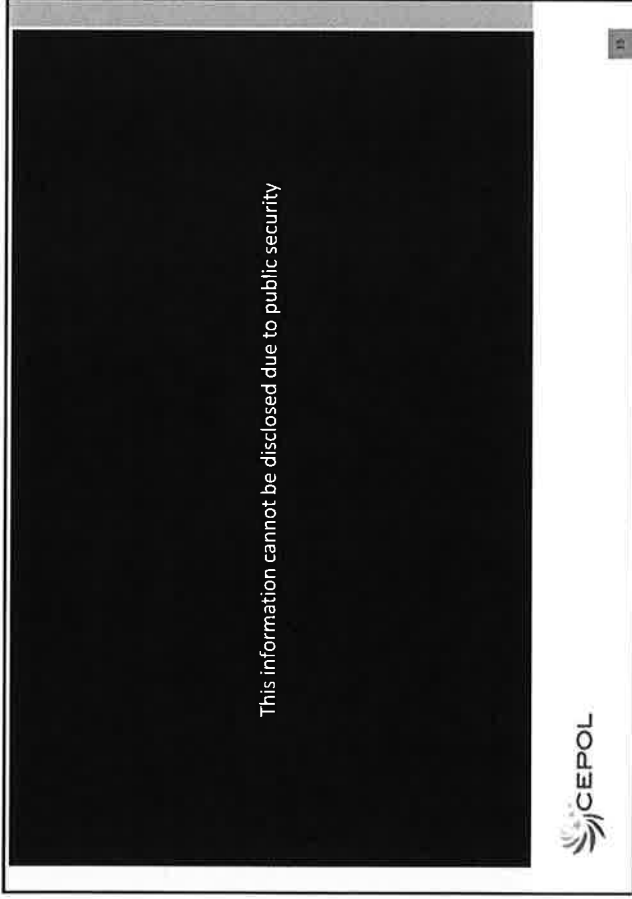
11

This information cannot be disclosed due to public security

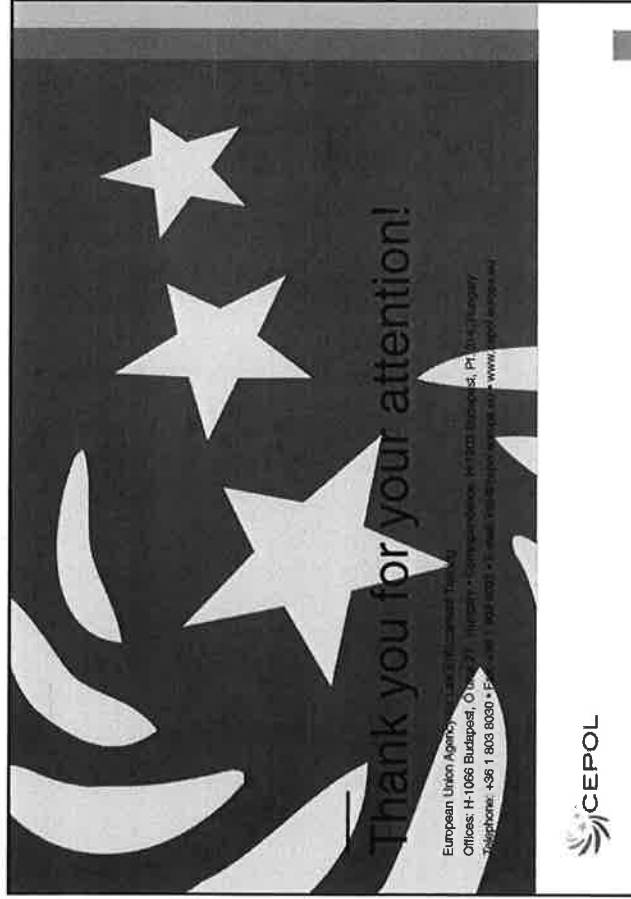


12











Thank you for your attention!

European Union Agency for Criminal Justice Cooperation  
Offices: H-1066 Budapest, Oroszlányi út 12-14. Hungary • 105333 Stockholm, Prinsessgatan 11, Sweden  
Telephone: +36 1 803 8080 • Fax: +36 1 803 8081 • E-mail: [info@cepjoc.eu](mailto:info@cepjoc.eu) • [www.cepjoc.eu](http://www.cepjoc.eu)




**Financing of Terror - MSB's and Informal Banking**  
Salammbao, Tunis  
24-27 June 2019

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

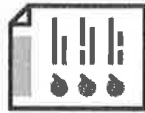


**Operational characteristics of MSB's**

- Classic Bureau de Change (currency exchange, traveler cheques etc.)
- Transfer of value (remitters etc.)
- Discounting (Cheque, notes, credit vouchers)
- Loans



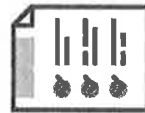
### Bureau de Change/Transfer of value



- Foreign currency purchased from customers, some from banks, and from other MSB
- Most customers are occasional, or tourists, though some are regular (Universities, other MSB's)
- No commission (profit in margin of exchange rate)
- Motto – reliable accessible fast efficient and cheap service
- Note exchange
- Consideration – Cash MSB Cheque or Bank account crediting



### Discounting/Loans



- Complimentary to banks (extra credit, export/import, donations, foreign contacts)
- Regular customers (Friend brings friend)
- Insolvent, firms in financial difficulty, rejected by banks
- Customers seeking immediate cash
- Good record keeping and retention of transactions and of client credit history
- Commission represents estimated risk
- Most discounting in local currency but some of foreign cheques + currency change
- Some use sub-discounter who provides credit



### Typical MSB - Bank Activity



#### Discounting /Loans

- MSB must operate with bank (Directly or indirectly)
- Several Cheque deposits, Bad cheques
- Mostly cheques of individuals
- Short term deposits
- Regular involvement of unknown depositors
- Large cash withdrawals and deposits
- Several bank accounts
- Depositing of cheques from foreign financial institutions
- Account credited under different identities by Credit Co.



### Typical MSB - Bank Activity

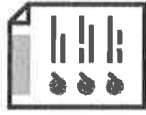
#### Bureau de Change/Transfer of value

- Large cash withdrawals and deposits.
- Use of foreign currency accounts (including cheques)
- Various currencies
- Several bank accounts
- Regular involvement of unknown depositors
- Depositing of cheques from foreign financial institutions



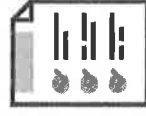
### MSB usage of the banking clearing system

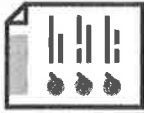
- Banks Honor cheques with several endorsements
- MSB's use banks to discount cheques
- Cheques deposited at payoff date
- Disengagement of audit trail – occurs at MSB



### The use of alternative value to cash

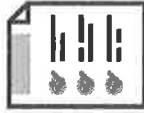

- Avoid border reporting
- Manipulation of value
- "Thicker" layering
- Use of stored value (Telephone cards)
- Easy transport (Diamonds, Gold)






### Modus operandi of MSB's with other MSB's abroad

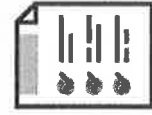
- Common characteristics (Language, Nationality, Family).
- No necessary actual shift of funds
- Many MSB's serve as agents of large international remittance Co (Moneygram, Western Union)
- Used for clearing foreign cheques



### Modus operandi of MSB's with other local MSB's

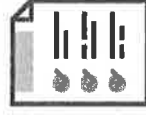
- Avoiding reporting requirements
- Unregistered MSB's
- Criminal elements registration of "front"
- "Thicker" Layering
- Cheque discounters with Bureau de Change
- Temporary shortage of currency
- Shifting of risk
- Relative advantage and access (Nationality, language, Proximity)





### Customer Identification

- Are MSB's "financial institutions"?
- MSB as financial institution dose not provide beneficiaries of its accounts at the bank
- Identification resulting in tipping off (when reporting requirements linked to threshold)
- Government provided Software



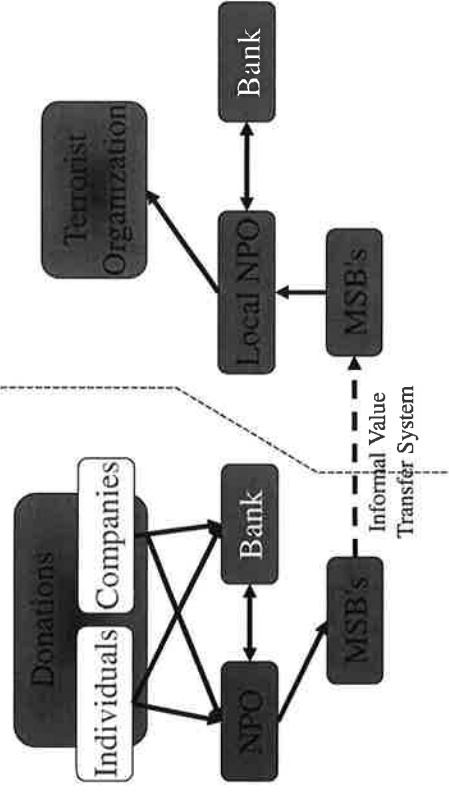
### The Egmont Group's six main signs of money laundering

#### Are they relevant to MSB's and FT?

- Large-scale cash transactions
- Atypical or uneconomical fund transfers to or from a foreign jurisdiction
- Unusual business activities or transactions.
- Large or rapid movements of funds.
- Unrealistic wealth compared with client profiles
- Defensive stance to questioning



### Terrorism funding through NPO's - A typical "money trail"




This information cannot be disclosed due to public security

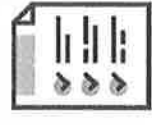




This information cannot be disclosed due to public security

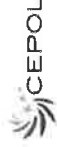


14

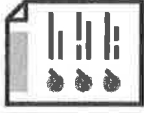


### Informal Banking - Hawala

- Definition
- Characteristics of Hawala
- Parties to the Hawala
- Reasons for Prevalence
- Risks





15




**Definition**

- An informal remittance system that does not require transferors identity verification, or detecting and reporting suspicious transactions.
- The transfer of money is carried out through unregulated network with no physical or electronic movement of money.
- The settlement takes place between the hawaladar (intermediary commander) and the other hawaladar (intermediary receiver) from whom the money is received.

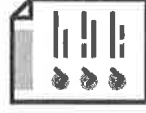



**Characteristics of the Hawala**

- **Anonymity:** Hawala hinges on complete secrecy of transactions carried out thereby in terms of content, form and procedure.
- **Oral:** Transactions are executed orally.
- **Trust:** Absolute trust among parties is a vital condition for transferring via hawala.



### Parties to the Hawala



1. **Transferor:** The holder of the money which is being transferred.
2. **Hawaladar (intermediary commander):** The service provider who collects the money intended to be transferred in return for a small percentage charge.
3. **Hawaladar (intermediary receiver):** The service provider who distributes the value on behalf of the transferee upon the order of the intermediary commander.
4. **Transferee:** The receiver of the hawala amount denominated in the agreed-upon currency from the intermediary receiver.

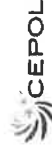


19

### Reasons of Prevalence

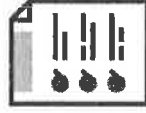


- The lack of banking and financial services in remote areas which funds are being transferred to.
- High fees and charges of formal transfers through licensed banks and financial institutions in comparison with low fees and charges of informal money transfer.
- Evading customs, income and consumption taxes and other levies in some countries.



20

### Reasons of Prevalence



- The speed of transfer through the informal transfer system at times in comparison with the speed via official conducts (licensed banks and financial institutions) and the need for transferring funds outside the official working days.
- Discrepancies between official and unofficial exchange rates at times in favour of transferors.
- Strict monetary restraints in some countries lay on money movement or transfer abroad.



31

### Reasons of Prevalence




- The largely increasing number of immigrants and/or expatriate workforce, wishing to transfer money to their native countries.
- Incapability to meet the standards of verifying identities of transferors or transferees, and the required measures of due diligence.
- Traditions and social values in many societies which bestowed credibility on these systems.
- Difficulties facing illegal immigrants in opening personal bank accounts at foreign banks.




32

**Reasons of Prevalence**




- Some exporters find themselves compelled - as a result of economic sanctions imposed on some countries- to seek informal transfer systems to get the return for their goods and services.
- Informal transfer systems are used for illegal activities such as money laundering, terrorism financing and tax evasion.




36

**Risks**

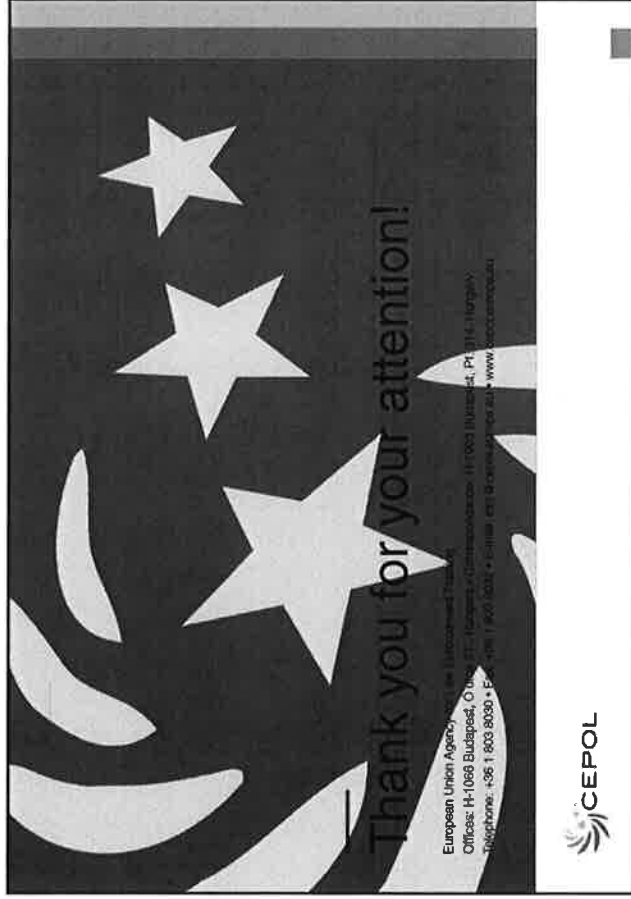


The informal remittance system does not require verifying the identity of transferors or detecting and reporting suspicious transactions, in addition to the lack of control or record keeping, transparency and accountability. Since large sums of money are being handed over through this system, there is a potential for misusing it in illegal activities.

- There are many economic impacts on the informal transfer system, either of which those related to the monetary policy and exchange rates, the fiscal policy, or the patterns of consumption and expenditure.




37



Thank you for your attention!

European Union Agency for Law Enforcement Training  
Offices: H-1058 Budapest, Orlai út 1. Hungary • Contact: +36 1 803 8100 • Fax: +36 1 803 8101 • E-mail: [info@cepola.eu](mailto:info@cepola.eu) • [www.cepola.eu](http://www.cepola.eu)

 CEPOL



Project funded by  
the European Union



## **UE/MENA Partenariat pour la Formation à la Lutte Anti-terroriste**

### **Programme Provisoire**

#### **Enquêtes Financières - Intermédiaire**

**DG Formation, Sureté Nationale**

**Académie de Police Salammbô**

**25 février – 1 mars 2018**

*Le contenu des sessions était développé sur la base des pratiques légales et respectant des droits de l'homme*

#### **lundi 25 février**

##### **Crime Organisé**

**08:15** Départ de la délégation de l'hôtel

**09:00** Admin, Accueil et Introduction – Exercice de groupe : Apprentissage assisté

**10:30** Pause-café

**10:45** Crime Organisé: Présentation de la perspective globale. Structure et liens : groupes terroristes, trafic

**11:30** Planification d'une opération, nécessité d'un enquêteur financier, cycle de renseignement. Collection de preuve et gestion, défis et bonnes pratiques

**12:30** Déjeuner

**13:30** Sources d'information à l'internet, Enquêtes, Opportunités, Menaces, Moteurs de Recherche, Sécurité des Officiers

**14:30** Pause-café

**14:45** Sources d'information à l'internet, Enquêtes, Opportunités, Menaces, Moteurs de Recherche, Sécurité des Officiers

**16:30** Fin de sessions

#### **mardi 26 février**

##### **Sources d'Information Ouverts**

- 08:30** Départ de la délégation de l'hôtel
- 09:00** Sources d'information à l'internet, Enquêtes, Opportunités, Menaces, Moteurs de Recherche, Sécurité des Officiers
- 10:30** Pause-Café
- 10:45** Sources d'information à l'internet, Enquêtes, Opportunités, Menaces, Moteurs de Recherche, Sécurité des Officiers
- 12:30** Déjeuner
- 13:30** Groupes d'Action Multi-Institutionnelle et coopération avec autres services répressifs - Exercice
- 14:30** Pause-Café
- 14:45** Groupes d'Action Multi-Institutionnelle et coopération avec autres services répressifs - Exercice
- 16:30** Fin de sessions

**mercredi 27 février**

**Blanchiment d'Argent**

- 08:30** Départ de la délégation de l'hôtel
- 09:00** Blanchiment d'argent – perspective globale
- 09:45** Structures d'entreprises, Propriété effective, Typologie de blanchiment d'argent – Exercice interactif
- 10:30** Pause-café
- 10:45** Structures d'entreprises, Propriété effective, Typologies de blanchiment d'argent – Exercice interactif
- 12:30** Déjeuner
- 13:30** Présentation de Agent de Conformité de Banque Tunisienne Commerciale
- 14:30** Pause-café
- 14:45** Identification de biens, mobiliers et immobiliers, retenue
- 15:30** Typologies Blanchiment d'argent – Cas d'étude Tunisien
- 16:30** Fin de sessions

**jeudi 28 février**

**Financement du Terrorisme**

- 08:30** Départ de la délégation de l'hôtel



- 09:00** Financement du terrorisme - perspective globale, comprenant le financement de prolifération
- 09:45** ONG, Organismes de bienfaisance, Contrebande d'espèces exercice comprenant, AQIM/Daesh
- 10:30** Pause-café
- 10:45** Typologies régionaux financement de terrorisme – Agent Tunisien CFT ou CT
- 12:30** Déjeuner
- 13:30** Contrebande d'espèces exercice comprenant, AQIM/Daesh
- 14:30** Pause-café
- 14:45** Exercice “de-brief” et leçons tirées
- 16:30** Fin de sessions

**vendredi 1 mars**

- 08:30** Départ de la délégation de l'hôtel
- 09:00** Exercice final – Quiz intergroupe
- 11:00** Pause-café
- 11:30** Evaluation
- 12:00** Clôture et Diplômes
- 13:00** Déjeuner
- 14:00** Départ à l'aéroport




Project funded by  
the European Union

EU/MENA COUNTER-TERRORISM  
TRAINING PARTNERSHIP 2  
FINANCIAL INVESTIGATIONS - INTERMEDIATE  
PARTICIPANT LIST



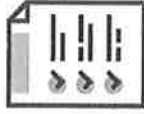
Name	Surname	Department
		DG Training
		DG Training
		DG Training
		DG Training
		DG Special Services
		DG Training
		DG Technical Services - Financial Investigations
		DG Technical Services - Financial Investigations
		Financial Brigade
		DG Training
		DG Training
		Financial Brigade
		National Unit for the Investigation of Terrorist Crimes
		Headquarters
		Financial Brigade
		Customs
		Financial Brigade
		Financial Brigade
		DG Special Services



**Understanding the threat posed by the misuse of charitable funds**


Personal Data  
Intermediate Financial Investigation Course  
Salambo, Tunis  
25 February – 1 March 2019

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING




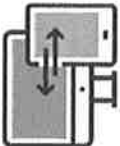
**Content**

- Level of threat of TF in charities
- Why there is a threat
- What methods of TF abuse occur
- Examples of TF abuse in charities
- How the UK has responded to this threat




7


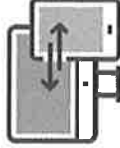
### Types of abuse in the charitable sector



- People successfully **exploiting vulnerabilities** in charities
- Vulnerability is not just concerned with terrorist financing but a range of serious issues of abuse




### Perspective: Size of sector vs enforcement action in the UK (2014/15)

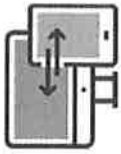


164,000  
registered charities

1,127  
investigations and compliance cases opened



## Why the charitable sector is targeted for abuse



Resource intensive and transnational in nature

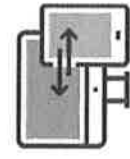
- **Large transitory workforce**
- **19 million full time employees**
- **10 million volunteers**
- **Work in areas of conflict / low governance**
- **Funds flow through areas of conflict / low governance**
- **Terrorist networks exist in same environment**
- **Same populations**



## Why the charitable sector is targeted for abuse

- Operational advantages that terrorist actors may seek use;
- FATF Typologies Report 2014:
  - Increased mobility;
  - Interconnectedness of networks;
  - Expanded and deepened access to areas of conflict or low-governance;
  - Diversified financial services and logistical networks (global presence – money, goods and people);
  - Decentralised communications and management;
  - Increased ability to engage the public (a ready made legitimate and needed social network).





## Risk of abuse in the charitable sector

- (Quite rightly) enjoy **high levels of public trust** because of voluntary and altruistic nature
- Operate in **high risk areas** where terrorist groups operate or exert control
- Subject globally to **different levels of oversight** and regimes
- Culture of trust within – can depend upon **one or two individuals** who play a key and often unsupervised role
- Risks due to **poor governance** and/or financial management

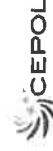


## Methods of abuse of charities for TF purposes

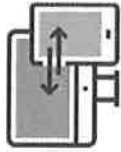
### Financial Action Task Force (FATF): Recommendation 8

“Countries should review the adequacy of laws and regulations that relate to non-profit organisations which the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused and proportionate measures, in line with the risk-based approach, to such non-profit organisations to protect them from terrorist financing abuse, including:

- (a) by terrorist organisations **posing as legitimate entities;**
- (b) by **exploiting legitimate entities** as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and
- (c) by **concealing or obscuring** the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.”



## FATF typologies report 2014

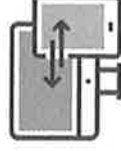


The main methods and risk from the case studies examined:

- Diversion of funds
- Affiliation with a terrorist actor/group
- Programming abuse
- Support for recruitment
- False representation

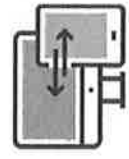


## Where are the TF risks and common difficulties?



- IN** Money from donors – provenance of funds; Reputational risks due to links / associations / conduct; Undue influence over decisions
- WITHIN** Risks from – activities; links and associations (trustees, employees, volunteers, fundraisers...); When conduct in personal capacity impacts on a charity
- OUT** Use of partners (overseas); Not just money – links, associations, control and reputational risks; Beneficiary influence





## How aspects of terrorist financing may affect charities



**RAISING**

- Street collections
- Donations – in person, via website, bank, mandate
- Appeals – specific and general
- Door to door collections and chugging



**STORING**

- Traditional banking
- Local cash storage
- Pre-payment cards, and PayPal



**MOVING**

- Bank transfers
- Cash couriers
- Money Service Bureaus: Alternative remittance (e.g. Hawala)
- Mobile phone payments



**USING**

- Cash
- Debit and credit cards
- Bank transfers, PayPal
- Cheques

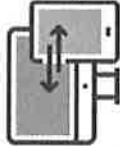


## Live TF issues: Conflict zones


- Charities working in conflict affected areas and where terrorist groups operate (e.g. Syria, Gaza)
- Aid convoys - may be abused for non-charitable purposes and facilitating travel for foreign fighters
- Charitable appeals and fundraising issues
- Other risks
  - diversion of funds and aid in country
  - safety risks including kidnapping for ransom
  - transmission of cash by charity representatives
  - use of local partners for delivery
  - effective monitoring and verifying end use of funds



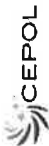




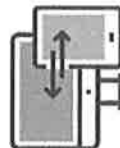
Instances of terrorist abuse of charities




This information cannot be disclosed due to personal data protection



11




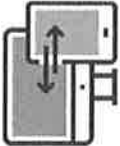

UK response to the threat of terrorist financing abuse of charities



12


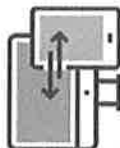
### The UK Model

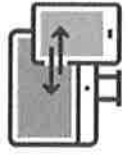
- The Police: NTFIU
- HM Treasury
- Charity Commission



### Why Use the Regulatory Framework?

- Civil v criminal
- Looking back v looking forward
- The distinction between abuse of a charity by people outside it and instances of abuse for terrorist purposes from within a charity
- Disruption
- Regulator able to act where others cannot
- Compliments and provides a range of proportionate measures to deal with abuse






## Response: Counter terrorism strategy

Government recommendations for:

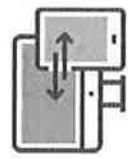
- Charity Commission
- NPO Sector
- Other agencies

**Charity Commission Counter-terrorism strategy:**

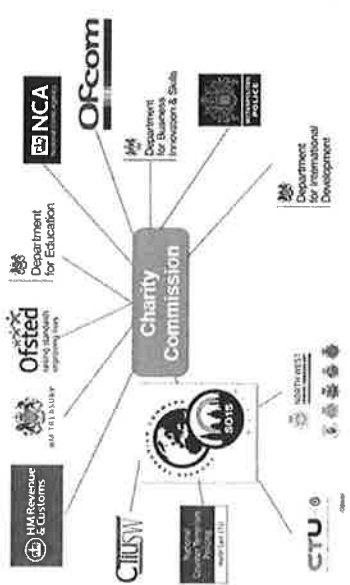

- Awareness:** raising awareness in the sector to build on charities' existing safeguards
- Oversight:** proactive monitoring of the sector and trends
- Co-operation:** strengthening partnerships with regulators and agencies
- Intervention:** dealing effectively and robustly with abuse



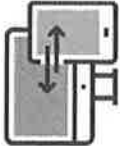
17



## Co-operation – other agencies





18

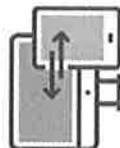


### Final Thoughts


- The **whole charity sector** should not be seen as high risk per se
- Each country and region – the **risk is different**
- **Allowing** legitimate humanitarian work to continue and donors' money to be used as intended is vital
- A **risk based approach is key**
- **Disruption** is a good result
- Underlines the importance for each government authority to have a **good understanding** of how the NPOs in their own country are vulnerable to abuse



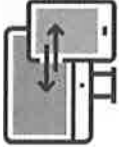
14




### Case Studies



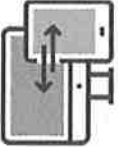
15



This information cannot be disclosed due to personal data protection




21



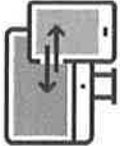
### Afghan Poverty Relief

- NTFIU (SO15) investigation
- Charity established for relief of need and poverty in Afghanistan
- Two trustees arrested in November 2011
- Commission opened investigation February 2012 – prohibited trustees from fundraising without prior consent
- Parallel investigations – criminal and civil




22

### Afghan Poverty Relief

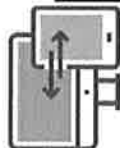


- Commission suspended trustees and served notice of intention to remove one trustee – appealed
- Commission supported criminal investigation and prosecution – provision of witness statement, attended court
- Guilty verdict – 5 and 3 year sentences
- Confiscation proceedings closing
- Commission investigation ongoing

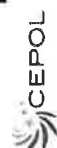
This information cannot be disclosed due to personal data protection

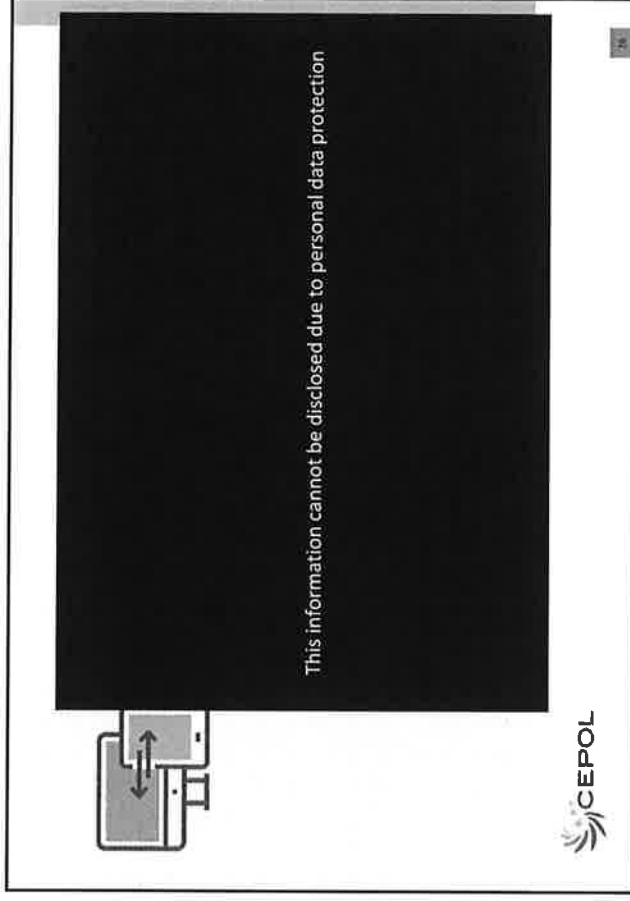
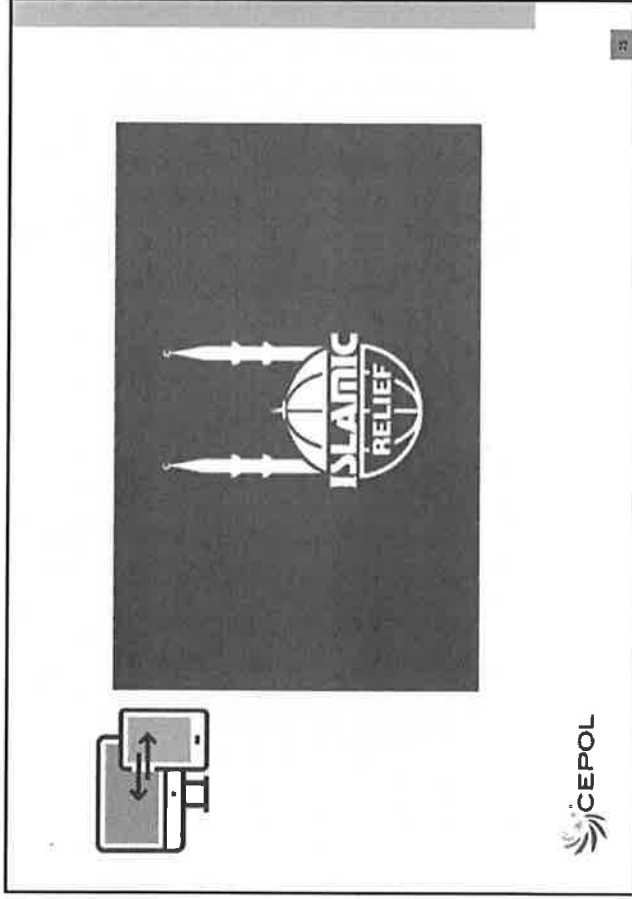



### Umar Ahmed Haque



This information cannot be disclosed due to personal data protection

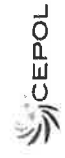






Thank you for your attention!

European Union Agency for Law Enforcement Training  
Offices: H-1066 Budapest, Ötödik út, 14. korszak (Károlyi utca) 114. korszak,  
Telephone: +36 1 803 8030 • Fax: +36 1 803 8031 • Email: [info@cepola.eu](mailto:info@cepola.eu) • [www.cepola.eu](http://www.cepola.eu)





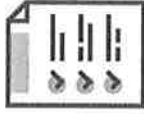


**Financial investigation strategy**

Personal data

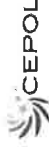
Intermediate Financial Investigation Course  
Sakambo, Tuni  
Tunis 25 February – 1 March 2019


EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING




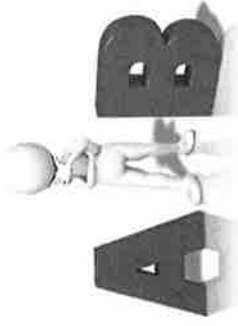
**Overview:**

- Case management
- Reactive and Proactive Investigations
- Targetted policing
- Financial investigation strategy
- Lifetime Offender Management







### Reactive and Proactive Strategy:




### Reactive challenges:

- Control
  - Where
  - When
  - How
  - Who
  - What




### Reactive challenges:

- Process
- Procedure
- Knowledge
- Power
- Authority
- Volume




The illustration shows a small, light-colored 3D figure standing in the center, looking up at three large, dark, semi-circular shapes that appear to be falling or pressing down on them, symbolizing reactive challenges.




CEPOL

### Proactive benefits:

- Preparation
- More control
- Focus on the threat
- Options
  - Arrest
  - Disrupt
  - Deter
  - Desist



The illustration shows a dark 3D figure on the left pointing towards a whiteboard on a stand. The whiteboard has a lightbulb icon and the text 'Asset Recovery STRATEGY'. A light-colored 3D figure on the right is looking at the whiteboard.

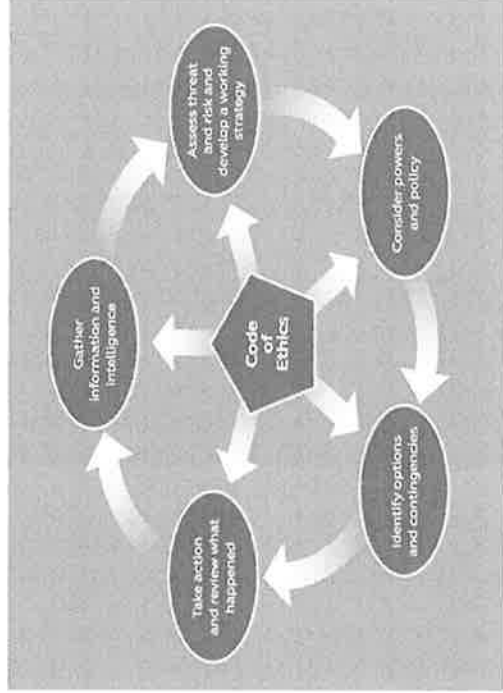


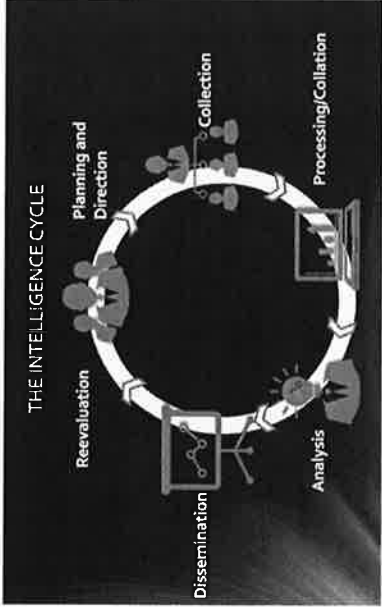
CEPOL

### Integrated financial investigation:



National Decision Model



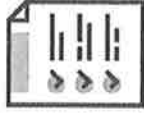


**THE INTELLIGENCE CYCLE**

The diagram illustrates a continuous cycle of six stages: Planning and Direction, Collection, Processing/Collation, Analysis, Dissemination, and Reevaluation. Each stage is represented by an icon and a brief description, connected by a circular path.

- Planning and Direction**: Represented by an icon of three people in a meeting.
- Collection**: Represented by an icon of a globe with arrows pointing to it.
- Processing/Collation**: Represented by an icon of a laptop displaying a bar chart.
- Analysis**: Represented by an icon of a person looking at a screen with a magnifying glass.
- Dissemination**: Represented by an icon of a person presenting to a group.
- Reevaluation**: Represented by an icon of a person looking at a screen with a magnifying glass.

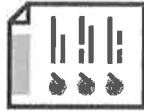
CEPOL



**Investigative options – 4 x P’s :**


- Pursue
- Prevent
- Protect
- Prepare
- Lifetime Offender Management

CEPOL

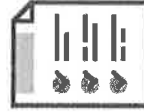


**Lifetime Offender Management:**

- Continued criminal behaviour
- Return to organisation
- Lifetime Offender Management
  - Disruption
  - Restriction
  - Removal




11



**Additional capabilities:**

- Director Disqualification
- Deportation
- Exclusion
- Revocation
- Serious Crime Prevention Orders
- Sexual Offences Prevention Orders
- Travel restriction
- Licence conditions
- Prison security



12



**Financial Capabilities:**

- Production Orders
- Cash seizure, Forfeiture and Restraint
- Financial Reporting Orders
- Disclosure orders
- Account monitoring orders
- Customer Information Orders
- Unexplained Wealth orders
- Further Information Orders – Money laundering

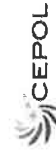


**Case exercise:**

This has just happened. The vehicle was stopped on the roadside in Sirtie with a puncture.



- What do you want to know
- What is your investigation strategy (including financial investigation)





**Thank you for your attention!**

European Union Agency for Law Enforcement Training  
Offices: H-1066 Budapest, Oroszlányi út 127. Hungary • [com@europa.eu](mailto:com@europa.eu) / <http://europa.eu>  
Telephone: +36 1 803 8030 Fax: +36 1 803 8031 E-mail: [info@europa.eu](mailto:info@europa.eu) [www.europol.europa.eu](http://www.europol.europa.eu)








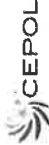
**Money Laundering - Global Perspective**  
Personal Data  
Intermediate Financial Investigator Course  
Salambo, Tunis  
25 February – 1 March 2019

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

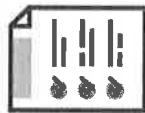


**THE CONSEQUENCES OF MONEY LAUNDERING AND FINANCIAL CRIME**

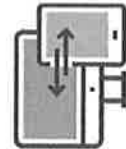
- EXPOSED EMERGING MARKETS
- THE ECONOMIC EFFECTS OF MONEY LAUNDERING
- SOCIAL COSTS
- PROFESSIONAL MONEY LAUNDERERS
- CURRENT TRENDS



## THE CONSEQUENCES OF MONEY LAUNDERING AND FINANCIAL CRIME



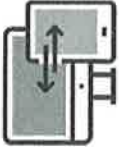
Money Laundering - a serious national and international security threat?



## EXPOSED EMERGING MARKETS


- ML affects emerging markets as well as major financial markets & offshore centres
- As economies open they become increasingly viable targets
- Negative impacts magnifies in emerging markets
- Organised crime groups investing in real estate and business
- Increased cash movements across borders



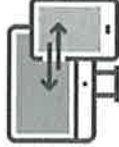


### Undermining the Legitimate Private Sector

- Use of front companies
- Access to illicit funds
- Not consistent with free market principles




1

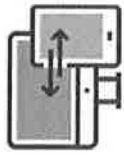


### Undermining the Integrity of Financial Markets

- Can cause liquidity problems
- Bank failures

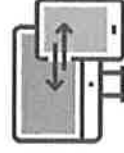


2



### Loss of Control of Economic Policy

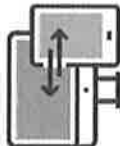
- ML equivalent to 2-5% of world GDP
- Dwarf government budgets
- Affects interest rates
- Monetary instability
- Unpredictable



### Economic Distortion and Instability

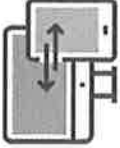

- Investments not economically beneficial
- Short term interest






### Loss of Revenue

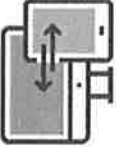
- Diminishes revenue
- Causes higher taxes



### Risks to Privatization Efforts


- Outbid legitimate purchasers
- Vehicle to launder funds



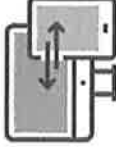


### Reputation Risk

- Confidence in the market eroded
- Diminishes development
- Once gone, difficult to restore




11

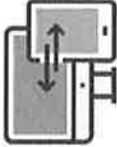


### SOCIAL COSTS

- Drives up cost of government
- Transfers economic power from market
- Can lead to take-over of legitimate government
- Complex and dynamic challenge




12

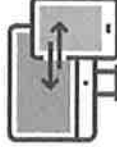


### PROFESSIONAL MONEY LAUNDERERS

- 3<sup>RD</sup> Party Money Launderers
- For fee, commission, other profit
- Specialised knowledge & expertise
- Exploit legal loopholes
- Find opportunities for criminals
- Help retain and legitimise proceeds of crime
- Often not familiar with predicate offence




21

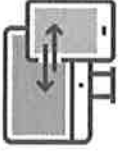
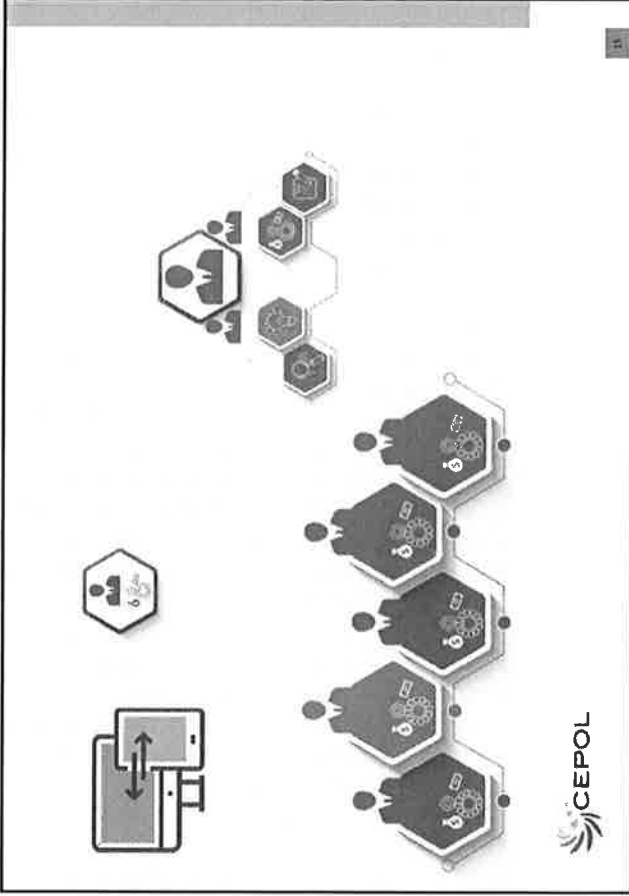


### PROFESSIONAL MONEY LAUNDERERS

- Individuals
- Professional Money Laundering Organisation
- Professional Money Laundering Network




24



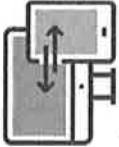
### SPECIALISED SERVICES

- Consulting and advising
- Registering and maintaining limited companies or other legal entities
- Serving as nominees for companies or accounts
- Providing false documentation
- Comingling legal and illegal proceeds
- Placing and moving illicit cash




14



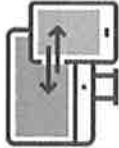


### SPECIALISED SERVICES

- Purchasing assets
- Obtaining financing
- Identifying investment opportunities
- Indirectly purchasing and holding assets
- Orchestrating lawsuits
- Recruiting and managing money mules




17

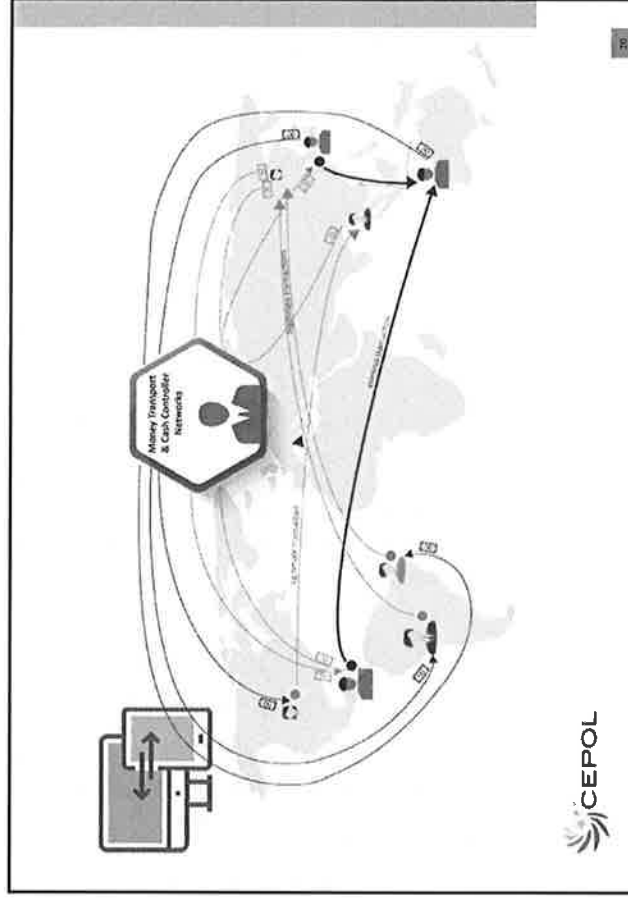
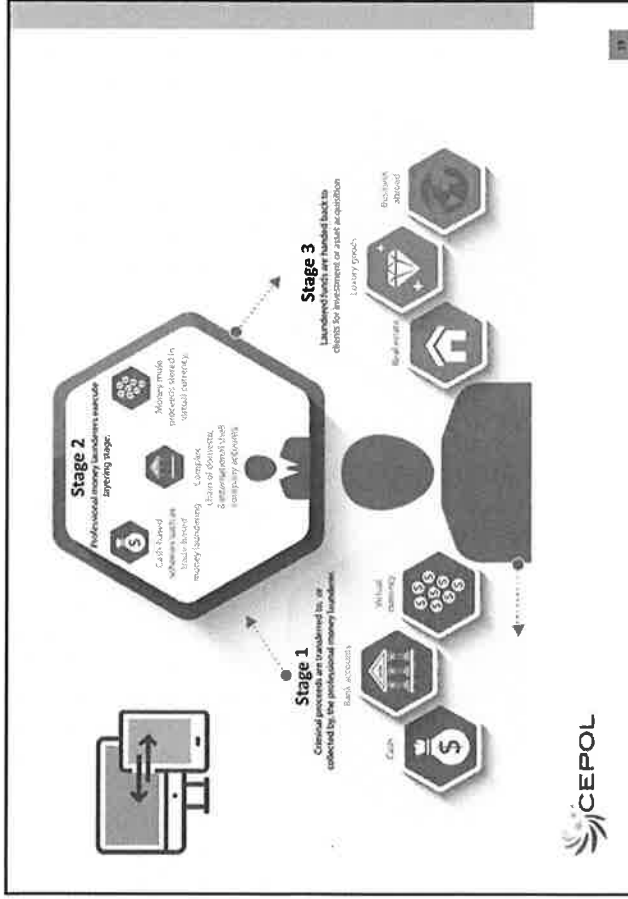


### ROLES AND FUNCTIONS









- Leading and controlling
- Introducing and promoting
- Maintaining infrastructure
- Managing documents
- Managing transportation
- Investing or purchasing assets
- Collecting
- Transmitting




18



**CURRENT TRENDS**  
Environmental crime has become largest financial driver of conflict

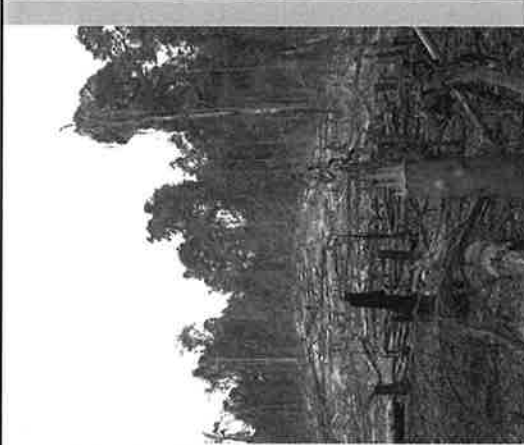
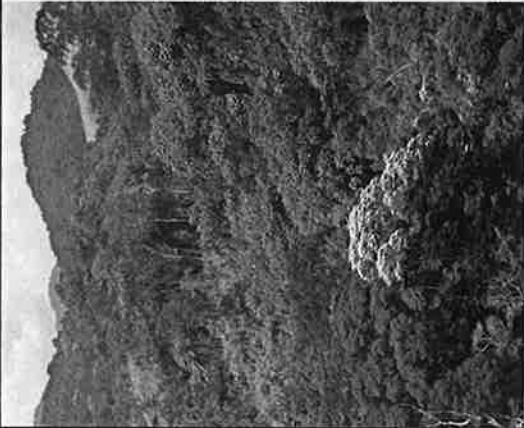


This information cannot be disclosed due to personal data protection



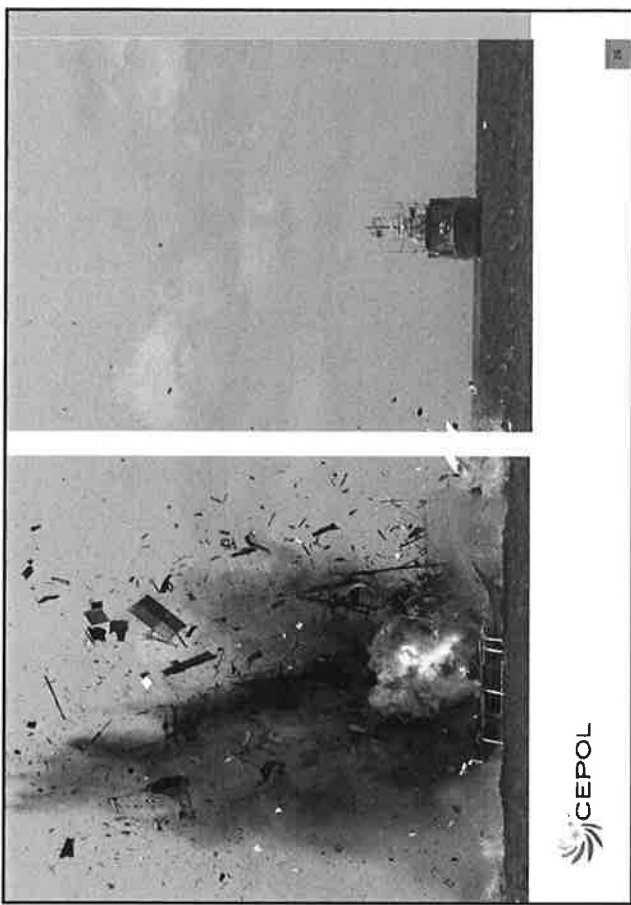
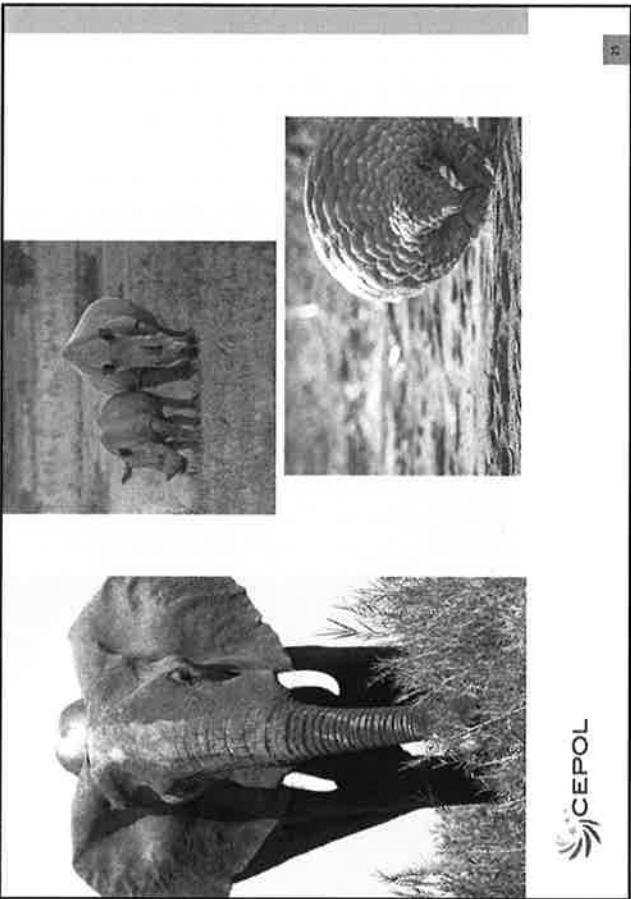
CEPOL

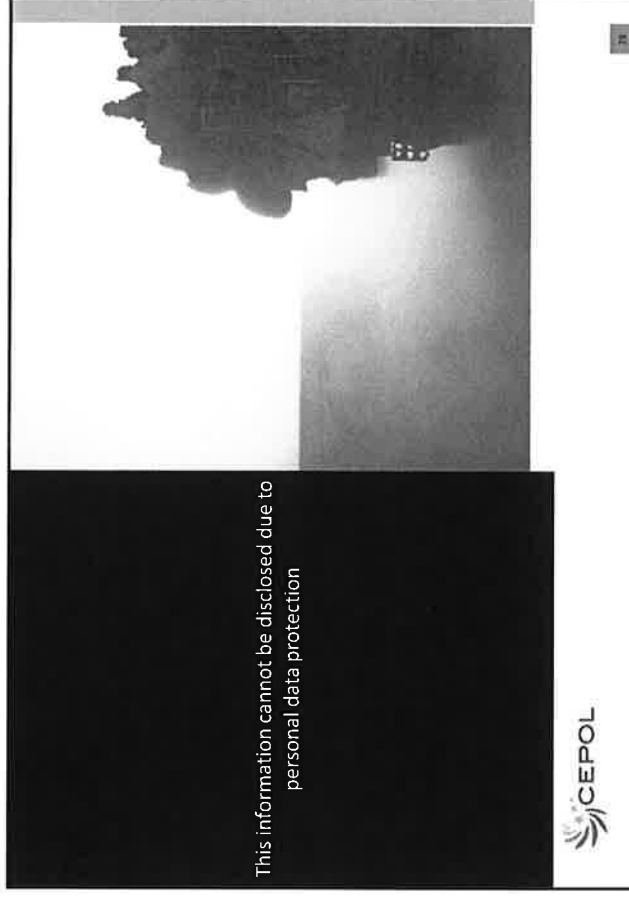
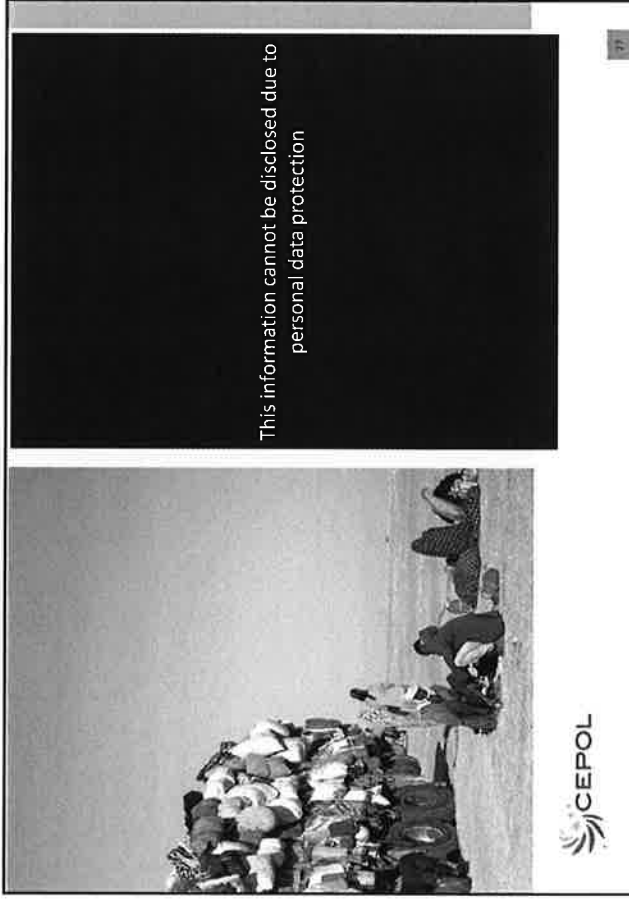
21



CEPOL


22






This information cannot be disclosed due to personal data protection

This information cannot be disclosed due to personal data protection




CEPOL

This information cannot be disclosed due to personal data protection



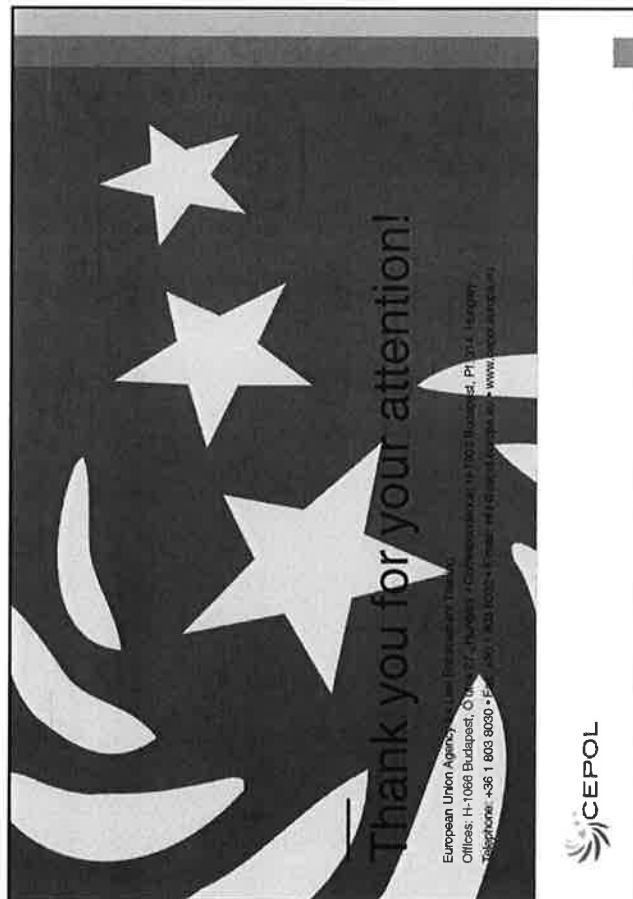
11

This information cannot be disclosed due to personal data protection



12








**Organized Crime – Global and Regional Perspectives**

Personal Data

Intermediate Financial Investigation Course  
Sokanibo, Tunis  
Tunis 25 February – 1 March 2019

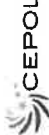


EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING





**Overview**

- Organized and Transnational Crime
- Typologies
- Regional threats
- A case example
- Conclusions



**Organized and Transnational Crime**



Serious crime planned, coordinated and conducted by people working together on a continuing basis. Their motivation is often, but not always, **financial gain**




7

**Organized and Transnational Crime**

A group of three or more persons that was not randomly formed; existing for a period of time; acting in concert with the aim of committing at least one crime punishable by at least four years' incarceration; in order to obtain, directly or indirectly, a financial or other material benefit. [UNODC 2000]





4




### Organized and Transnational Crime

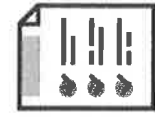
Transnational crimes are crimes that have actual or potential effect across national borders and crimes which are intra-State but which offend fundamental values of the international community. The term is commonly used in the law enforcement and academic communities



### Specific crime threats:

- Drug Trafficking
- Weapons Trafficking
- Irregular migration and Exploitation (People Trafficking)
- Cybercrime
  - On-line child exploitation
  - Malware/cryptoware
  - Payment card fraud
- Environmental
  - Illegal waste
  - Trafficking of endangered species



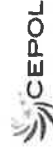
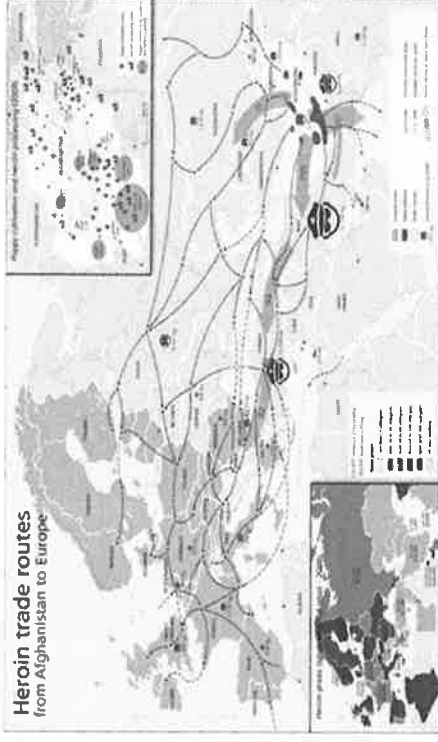


### Cross cutting crime threats:

- Criminal finances and money laundering
- Document fraud
- Online trade in illicit goods and services
  - Firearms
  - Drugs
  - Counterfeit goods



### Drug Trafficking



### Weapons Trafficking



### Irregular Migration and Exploitation



**Environmental crime**

- Illicit waste
- Trafficking in endangered species
- Fuel, Oil and charcoal



11



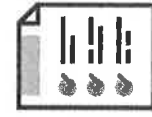
**Cyber crime**

- Child exploitation
- Malware and ID theft
  - 'Information stealers'
- Cryptoware
- Payment card fraud



12





## Transnational and Organized Crime in North Africa

- Crime syndicates are a common trans-border criminal element in the region. The long tradition of smuggling in North Africa has entrenched the cross-border trafficking in illicit goods.
- Poly-criminality is common for crime syndicates throughout North Africa as many criminal activities are often interrelated and interconnected.
- The region is increasingly connected to global illicit markets via various international criminal organizations, which are targeting North Africa in particular to maximize illicit gains. This involvement is suspected to be on the rise.

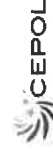


11




## Transnational and Organized Crime in North Africa

- Threat to security and safety
- Significant Illicit wealth
- Additional facilitators
  - Length of borders
  - Strategic position between Europe and sub-Saharan Africa
- War profiteering
- Conflicts
- Corruption



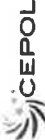
14






### Additional Regional Threats

- Counterfeit goods
- Illicit Trafficking of Cultural Heritage
- Terrorism




19



### Counterfeit goods

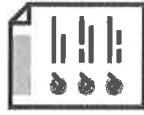
Counterfeit products are present throughout North Africa. The region is an origin (production), transit and destination point for counterfeit products. North African crime syndicates play a major role in the importation, production and distribution of these products.



18

### Counterfeit goods

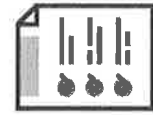
- OECD 2016
  - 2.5% of International Trade
  - \$461 billion
- Organized crime groups
- Flexibility
- Affordable technology
- Fictitious business – smuggling



### Counterfeit goods

- OTIC conference 2017
  - 80% automotive parts, clothing and cosmetics counterfeit
  - Represent health and economic risk
  - Majority originate from China
- Established contraband routes
  - Algeria - Tunisia
- Organized Crime Group connections
- OECD study
  - Algeria, Morocco, and Tunisia



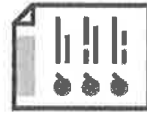


### Illicit Trafficking of Cultural Heritage

The illicit traffic in cultural heritage is a serious and lucrative transnational crime that affects Northern African countries. This type of traffic can take different forms, including but not limited to, theft, illicit excavation, removal of cultural property as well as illicit exportation and importation of works of art.



17



### Illicit Trafficking of Cultural Heritage

- UNESCO – 34 world heritage sites
  - 8 in Tunisia
  - Estimates between \$4-\$6 billion
- Interpol database of stolen works of Art
  - Libya and Egypt most affected
- Trafficking routes
  - Documentation and provenance
- Tunisia seized 4,000 artefacts 2011-2015
  - OCG Tunisia – 2018
    - Hebrew manuscripts
    - Deep web
    - Dismantled
- Europe and North America preferred destinations
  - Reuters – ISIS involvement in Syria and Iraq
    - Libya and Tunisia (lesser extent)



18

## Terrorism and Organized Crime

Financing of terrorism through engagement in organized crime activities is one of the most important aspects of the terrorism and organized crime nexus.

The two main terrorist organizations active in the region are, Al-Qaida in the Islamic Maghreb (AQIM) and the Islamic State in Iraq and Syria (ISIS).




## Terrorism and Organized Crime


- Historically three revenue streams
  - Smuggling
  - Cigarettes



### Terrorism and Organized Crime




This information cannot be disclosed due to personal data protection




2

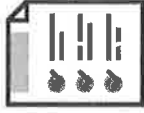
### Terrorism and Organized Crime



- Historically three revenue streams
  - Smuggling
  - Cigarettes
  - Arms
- Drug trade
  - Cocaine
- Kidnapping for ransom
- New sources
  - People Trafficking
  - Protection of infrastructure





4




### **Terrorism and Organized Crime**

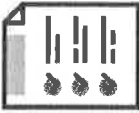
- Historically three revenue streams
  - Smuggling
    - Cigarettes
    - Arms
  - Drug trade
    - Cocaine
  - Kidnapping for ransom
- New sources
  - People Trafficking
  - Protection of infrastructure



### **Conclusions**


- Threats from criminal networks and criminal markets that they foster
- Largely financially driven
- Highly resourceful
- Leverage socio economic drivers
- Strong links and co-operation







**Conclusions**

- Law Enforcement:
  - Collective response
  - Information sharing between countries
  - Comprehensive picture
  - Clear and Effective strategies



17





18

Thank you for your attention!

European Union Agency for Criminal Justice Cooperation  
Office: H-1066 Budapest, Oroszlányi köztemető utca 14/A-1062 Budapest, Pf. 194, Hungary  
Telephone: +36 1 903 8090 • Fax: +36 1 903 8031 • Email: [info@cepola.eu](mailto:info@cepola.eu) • [www.cepola.eu](http://www.cepola.eu)





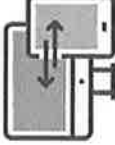
**Terrorism and Financing the Recruitment of Terrorists – Global Perspective**

Personal Data

Intermediate Financial Investigation Course  
Salambo, Tunis  
Tunis 25 February – 1 March 2019





EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING



### **Eight Major Groups**

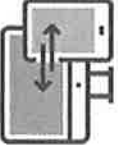

1. Al Qaida
2. Islamic State / Daesh
3. Hayat Tahrir al-Sham (HTS)
4. Jama'at Nasr al-Islam wal Muslimin (JNIM)
5. Taliban
6. Boko Haram
7. Al Shabaab
8. Fuerzas Armadas Revolucionarias de Colombia (FARC)






### Overview

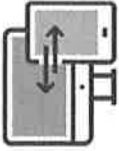
- 2001 – 2018 X 4 times as many Salafi Jihadists
- 230,000 in 70 countries
- Prédominant in Syria, Afghanistan, Pakistan
- IS 1% of territory from 2014-2015
- **Al Qaida and Islamic State / Daesh**
- Seperate entities BUT cooperation occasional & pragmatic in specific regions at various times



### Perspectives

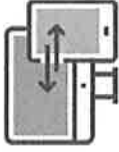

1. Intensification
2. Irrelevance
3. Al Qaida Ascendant
4. IS Rebounds






**Intensification**

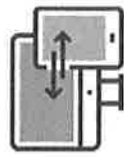
1. Diminished Western presence
2. False dawns
3. Global Jihadist movement
4. Potential



**Irrelevance**

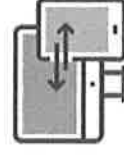
1. Global Jihadist movement ends
2. Hardening of borders
3. Advances in technology
4. Biometrics and AI
5. Shift in threat landscape





### Al Qaeda Ascendant

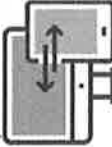
1. Increase in external support
2. Refashioned image
3. Potential to capitalize on IS missteps



### IS Rebounds


1. Believed demise of Al Qaida
2. IS reconstitutes itself
3. International response
4. IS elevates by default



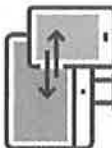


**Conclusions**

1. Al Qaida v IS
2. Transnational v Local
3. North Africa to South East Asia
4. Foreign fighter returns




10

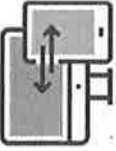


**Terrorism Recruitment Financing**

1. Methods of Recruitment and Associated Costs
2. Sources of Funds for Terrorist Recruiters
3. Use of Funds for Activities Related to Terrorist Recruitment




11

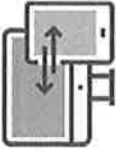


### Methods of Recruitment and Associated Costs

1. Active Recruitment
2. Passive recruitment




11

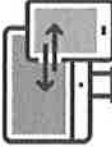


### Sources of Funds for Terrorist Recruiters


1. Support from Terrorist Organisations
2. Outside Donations
3. Misuse of NPOs
4. Criminal Activity



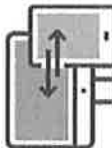
12




**Sources of Funds for Terrorist Recruiters**  
Support from Terrorist Organisations



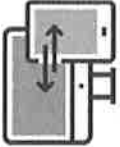
11




**Sources of Funds for Terrorist Recruiters**  
Outside Donations



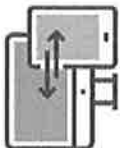
12




**Sources of Funds for Terrorist Recruiters**  
Misuse of NPOs



18

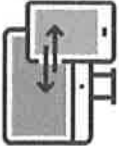


**Sources of Funds for Terrorist Recruiters**  
Criminal Activity




19



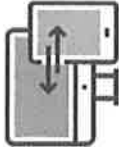


### Use of Funds for Activities Related to Terrorist Recruitment

1. Personal Needs & Upkeep of Individual Recruiters
2. Production & Dissemination of Recruitment Material
3. Paying for Goods & Services
4. Direct Payments to Recruits, Mercenaries, and Experts




17

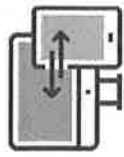


### Use of Funds for Activities Related to Terrorist Recruitment

Personal Needs & Upkeep of Networks & Individual Recruiters

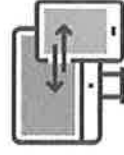


18



**Use of Funds for Activities Related  
to Terrorist Recruitment**

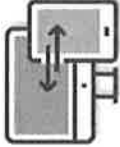
Production & Dissemination of  
Recruitment Material




**Use of Funds for Activities Related  
to Terrorist Recruitment**

Paying for Goods & Services







**Use of Funds for Activities Related to Terrorist Recruitment**  
**Direct Payments to Recruits, Mercenaries, and Experts**




19



**Conclusions**  
**Inter-Agency Co-operation**  
**International Co-operation**  
**Private Sector and NPO Sector Engagement**




20



**Thank you for your attention!**

European Union Agency for Law Enforcement Training  
Offices: H-1066 Budapest, Örményi út 17/A. Hungary • Slovenská republika: Hradcovská 14, 811 04 Bratislava  
Tel: +36 (0) 1 803 8000 • Fax: +36 (0) 1 803 8001 • E-mail: [info@cepola.eu](mailto:info@cepola.eu) • [www.cepola.eu](http://www.cepola.eu)






**CEPOL**

**Nouvelles méthodes de paiement par cartes  
prépayées et le blanchiment de capitaux basé  
sur le commerce**

**Personal Data**

International Investigation Course  
Paris, 2019  
September - March 2019

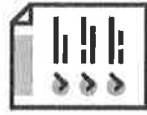
EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING



**Objectif**

- Connaître les évolutions du commerce international et ses moyens de paiement
- Identifier les risques liés au e-commerce
- Savoir distinguer les différents types de paiement par carte
- Identifier les risques des cartes prépayées anonymes

**CEPOL**



## Sommaire

1. Commerce et blanchiment de capitaux
2. Commerce et e-commerce
3. De la carte bancaire à la carte prépayée anonyme
4. Les cartes prépayées anonymes et la lutte contre le blanchiment



## I - Commerce et blanchiment de capitaux

- Les transactions commerciales : vecteur important des opérations de placement des espèces dans le système financier mondial
- Par des paiements en espèces d'opérations commerciales directement par les trafiquants et proches pour leur train de vie
- Solution rapide pour les criminels mais limitée au risque de ne pouvoir justifier de leurs ressources

This information cannot be disclosed due to public security



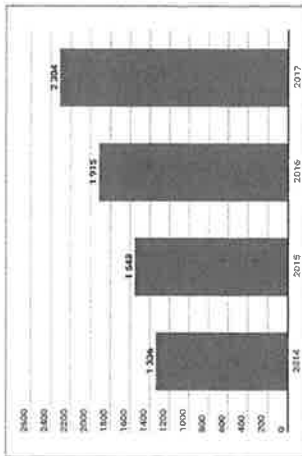
## I - Commerce et blanchiment de capitaux

- La lutte contre le blanchiment passe par la mise en place de limites à l'utilisation des espèces
- Vers le paiement par carte bancaire quel que soit le montant de la transaction
- Une évolution favorisée par le développement du e-commerce



## Evolution du E-Commerce dans le monde

- Une progression à deux chiffres du E commerce dans le monde
- Une place de plus en plus importante sur l'ensemble des transactions commerciales avec les particuliers
- Le commerce en ligne représente plus de 20% du commerce mondial



En milliards de dollars (Source eMarketer)





## II - Commerce et e-commerce

- De l'utilisation des espèces aux cartes bancaires
- L'évolution du E-commerce une solution à la problématique du blanchiment par des espèces ?
  - Pas de paiement par espèces avec le E-Commerce
  - Mals risques de fraudes et de cybercriminalité
  - Possibilité de paiement par monnaie virtuelle de plus en plus importante (y compris avec des commerces traditionnels)



7

## III – De la carte bancaire à la carte prépayée anonyme

Une distinction nécessaire entre les différents types de cartes proposées au public

- Les cartes rattachées à un compte bancaire
  - Les cartes de paiements et de retrait classiques
  - Cartes bancaires avec un code personnel au nom du titulaire du compte bancaire permettant :
    - Des achats en commerce et commerce sauf cas limités
    - Des paiements internationaux
    - Des retraits en Distributeurs de billets
  - Utilisable que par le titulaire du compte (sauf s'il donne son code personnel) et débitant le compte sur lequel la carte est rattachée
- Les paiements aux commerces sont garantis par l'établissement financier mais fort risque de fraudes dont la charge est principalement portée par les établissements financiers.



8



### III – De la carte bancaire à la carte prépayée anonyme

Une distinction nécessaire entre les différents types de cartes proposées au public

- Les cartes rattachées à un compte bancaire
  - Les cartes prépayées rattachées à un compte bancaire
  - Identiques aux précédentes et ayant un plafond de chargement et pouvant être rechargées selon un montant mensuel ou hebdomadaire variable en fonction des établissements de crédits.
  - N'est pas une carte de crédit mais de paiement
  - Le souscripteur et le bénéficiaire peuvent être différents mais le compte débité est celui du souscripteur (client)
  - Certaines cartes peuvent être créditées par un autre compte support du souscripteur
- Les cartes prépayées anonymes
  - Idem mais aucun nom ne figure sur la carte.
  - Il est toujours possible de remonter le compte pivot.



### III – De la carte bancaire à la carte prépayée anonyme

Une distinction nécessaire entre les différents types de cartes proposées au public

- Les cartes non attachées à un compte bancaire
  - Les cartes non prépayées
  - Cartes non anonyme quant au souscripteur
  - Carte pouvant être anonymisées permettant au souscripteur de la donner à un tiers
  - Ce n'est pas une carte de crédit mais de paiement
  - Le compte support est toujours approvisionné et le paiement est immédiat, débitant le compte support
  - Si le seuil maximum est inférieur ou égal à 250€, l'établissement de paiement doit identifier le client (souscripteur) et sauvegarder les informations à disposition des services répressifs



### III – De la carte bancaire à la carte prépayée anonyme

Une distinction nécessaire entre les différents types de cartes proposées au public

- Les cartes non attachées à un compte bancaire
  - Les cartes prépayées anonymes
    - Il n'y a aucun compte support (ni bancaire ni de paiement)
    - Le montant utilisable est le solde de la carte
    - Elle peut être rechargeable ou pas et toujours avec un seuil fixé par la réglementation (250 euros dans l'UE selon la 4<sup>ème</sup> directive européenne)
    - Elle peut être rechargeable en espèces mais le montant total des recharges est limité mensuellement
    - Elle peut aussi être rechargeable (pour certaines) par des monnaies virtuelles
    - Il est possible de les utiliser aux distributeurs de billets dans le monde entier (Visa et Master card)



11

### III – De la carte bancaire à la carte prépayée anonyme

Une distinction nécessaire entre les différents types de cartes proposées au public

- Les cartes non attachées à un compte bancaire
  - Les cartes cadeaux
    - Il n'y a aucun compte support (ni bancaire ni de paiement)
    - Le montant utilisable est le solde de la carte
    - Elles sont non rechargeables et limité à 250 euros
    - Elle peut aussi acquises (pour certaines) par des monnaies virtuelles
    - Il n'est pas possible de les utiliser en distributeurs de billets
    - Leur utilisation est limitée à un cercle restreint de commerces



11



**Conclusion : vers une totale dématérialisation des paiements**

- L'évolution du commerce vers les achats en ligne diminue directement l'utilisation des espèces mais n'enlève pas le risque et en crée d'autres
- Compte tenu de la possibilité d'acquiescer des paiements sécurisés anonymes
- Que ces moyens de paiement peuvent être acquis ou rechargés en espèces ou par des monnaies virtuelles
- Qu'elles peuvent être rechargées par virements provenant de toute part du monde
- Que les risques de cybercriminalité sont élevés
- Un plafond encore élevé n'interdisant pas le risque de blanchiment et de financement du terrorisme par shirroumfage
- Un anonymat restant limité, pour le moins quand à l'acquéreur



**Thank you for your attention!**


European Union Agency for Law Enforcement Training  
 Office: H-1066 Budapest, O. Buda 31, Hungary  
 Telephone: +36 1 802 8030 • Fax: +36 1 802 8031 • Email: info@cepel.eu • www.cepel.eu



**Coopération et groupe de travail multi services  
sur le plan national – expérience française**

Personal Data  
International Forensic Investigation Course  
Sofia, 2019  
25 February – 1 March 2019


EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

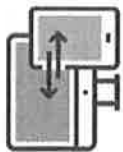


**Sommaire**

Introduction

1. Une organisation complexe : frein historique à des échanges et coopérations interservices
2. l'approche « policière » de la coopération
- 3- L'approche interministérielle



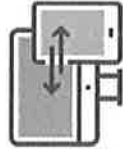


## Introduction

La coopération internationale : un passage obligé des services de police, douaniers ou fiscaux dans la lutte contre le blanchiment de fonds et le financement du terrorisme. Mais passant impérativement par une coopération nationale entre les différentes entités existantes

Cette coopération nationale est une nécessité :

- Dans le cadre d'enquêtes complexes et d'envergure et nécessitant des moyens humains et techniques importants
- Afin de partager des savoir-faire complémentaires de différents services – de renseignements, spécialisés dans l'interception et les écoutes, cyber services, services de surveillance et filatures, services judiciaires et financiers...



## Introduction

Une coopération nationale parfois ralentie par différents freins qu'il est nécessaire de lever

- L'organisation complexe des services de l'Etat en charge de la lutte contre le blanchiment
- Des services qui ne se connaissent pas voire s'ignorent
- Une rivalité interservices dans un esprit de compétition et à la recherche d'un résultat non partagé
- Des méthodes et des procédures antinomiques

Les organisations françaises et tunisiennes ont des points communs pouvant conduire à des constats et des évolutions similaires en matière de coopération interne (1)

Les évolutions sont d'abord selon une approche « policière » de la coopération entre les différents services du ministère de l'intérieur (2)

La coopération nationale est pourtant une coopération interministérielle (3)





## 1 – des organisations internes complexes : un frein à une coopération nationale

- Plusieurs ministères en charge de la lutte contre la criminalité organisée dont les principaux sont
  - Le ministère de l'intérieur
  - Le ministère des finances
  - Le ministère de la défense
- D'autres ministères pouvant être partie prenante dans certains aspects de la lutte contre la criminalité organisée et le terrorisme (dans leur domaine de responsabilités)



## 1.1 – Deux forces distinctes au ministère de l'intérieur

POLICE NATIONALE



La gendarmerie nationale (équivalent de la garde nationale tunisienne) bien que dépendante du ministère de la défense est rattachée au ministre de l'intérieur avec la Police nationale

- Une organisation nationale et territoriale avec les mêmes attributions pour chacune des entités
  - Conduisant à l'existence de services concurrentiels
    - Nationaux et régionaux
- Des services de renseignements ayant des activités judiciaires et vis-versa (DCRI ...)
- La police judiciaire n'est pas seule à avoir des attributions judiciaires
  - Existence de services de police judiciaire étouffés dans la direction de la sécurité publique et aussi à la DCRI

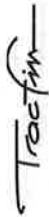


## 1.2 – Une dualité au sein du ministère des finances



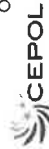
### Existence de plusieurs directions de lutte contre les fraudes fiscales et douanières

- Les douanes
  - Qui ont une partie judiciaire dans leur attributions mais séparé de leur pouvoir de transaction douanière
- Les services fiscaux
  - Qui peuvent engager des poursuites judiciaires outre des redressements (Direction Nationale des Enquêtes Fiscales)
- Particularité de la Cellule de renseignement financier
- Particularité de l'agence de lutte contre la corruption



## 2 – l'approche « policière » de la coopération nationale

- La Coopération ponctuelle
  - Création de « task forces » pour un objectif précis
    - Entre différents services d'une même direction (ex. services stupéfiants et financiers)
    - Entre différentes directions dans une enquête commune (co-saisine par un magistrat unique) principalement entre un service central et un service régional et non entre des entités différentes
- La coopération institutionnalisée dans un domaine précis :
  - Création d'unités de coordination de directions différentes devant coopérer
    - UCLAT – en matière de terrorisme (1984)
    - UCoFI – coordination des forces d'intervention de police/gendarmerie (2010)





## 2 – l'approche « policière » de la coopération nationale

- Les services mixtes police/gendarmerie
  - Le partage de la directions des offices centraux entre officiers supérieurs de gendarmerie et de police
    - Avec des équipes mixtes (conséquence de l'intégration de la gendarmerie dans le périmètre du ministère de l'intérieur)
    - Mais la partit e police gendarmerie n'est pas le principe
- L'expérience de la direction des douanes dans la lutte contre la contrebande et les fraudes fiscales
  - La Task force Dragon (2008)
    - Equipe mixte de différentes directions douanières avec des référents de la direction nationale des enquêtes fiscales



## 3 – l'approche « interministérielle » de la coopération

- L'exemple de la **Brigade nationale des enquêtes économiques**
  - A l'origine (1948) équipe mixte d'agents de police et agents du fisc (lutte contre le trafic de tickets de rationnement après guerre
  - A été rattaché à la Sûreté nationale (actuelle police nationale) en 1950 mais non mixte depuis cette date
  - Une équipe de fonctionnaires du fisc travaillant avec la sous direction des affaires économiques et financières de la police judiciaire
  - Des détachements dans les services régionaux de police judiciaire
    - Les fonctionnaires détachés participent aux opérations mais n'ont pas de pouvoir de police.
- Un apport essentiel sur l'aspect fiscal dans la lutte des services répressifs contre la criminalité organisée





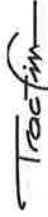
### 3 – l'approche « interministérielle » de la coopération

- Les groupes d'interventions régionaux
  - 37 GIR a compétence régionale ou départementale
  - Lutte contre la criminalité organisée régionale, nationale et internationale
  - Dirigés par des officiers supérieurs de police ou de gendarmerie
  - Composés de
    - une unité d'organisation et de commandement (UOC) permanente
    - Des policiers (sécurité publique, police judiciaire et police aux frontières) gendarmes, douaniers, fonctionnaires des impôts
    - Pour chaque opération, le niveau et la qualification des effectifs à mobiliser sont fixés par le chef de groupe, en fonction des objectifs.



### 3 – l'approche « interministérielle » de la coopération

- Le cas particulier de la cellule de renseignements financiers : des pouvoirs d'enquêtes administratives et d'échanges avec les services de renseignements ou répressifs
  - Tracfin (1990) – service de renseignements financiers
    - A l'origine uniquement des agents des douanes et un magistrat
    - Intégration de policiers et notamment spécialisés dans le financement du terrorisme
    - Intégration de fonctionnaires des services fiscaux depuis l'évolution du périmètre de la déclaration de soupçon aux fraudes fiscales
    - Recrutements de contractuels (non fonctionnaires) : analystes, informaticiens, spécialistes du blanchiment et du financement du terrorisme ...
- Echanges avec les services de renseignements ou répressifs ainsi qu'avec les CRF d'autres pays (groupe Egmont)



## Conclusion

- Les rivalités entre services ne profitent qu'aux criminels
- Les différentes expériences montrent que cela fonctionne malgré les difficultés et les appréhensions
  - A condition que les acteurs acceptent de travailler ensemble et apprennent à se connaître et à s'estimer
  - Un dossier totalement réussi et partagé par plusieurs directions est plus efficace et plus valorisant qu'une affaire à moitié élucidé par son service
- La pluralité des services dans nos organisations complexes ne doit pas être un frein mais une opportunité



Thank you for your attention!

European Union Agency for Law Enforcement Training  
Offices: H-1068 Budapest, O-10557, Hungary / 42, rue de la Woluwe, 1200 Brussels, Belgium  
Telephone: +36 1 803 8030 • Fax: 36 1 803 8037 • E-mail: info@cepola.eu • www.cepola.eu




**CEPOL**

Sources d'information à l'Internet, Enquêtes, Opportunités, Menaces, Moteurs de Recherche, Sécurité des Officiers

This information cannot be disclosed due to personal data protection

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING



1. Internet du Web 1.0 au Web 5.0
2. Le paysage du Web aujourd'hui
3. La cybercriminalité
4. Rechercher et surveiller l'information sur Internet
5. ADN et identité numérique
6. Les informations dans les enquêtes
7. Sécuriser mon environnement numérique ...

**CEPOL**

This information cannot be disclosed due to personal data protection

## Internet a été pensé sans la dimension sécurité !

(Louis Pouzin, l'un des 5 inventeurs d'Internet)

- Les données se sont décuplées
- Les attaques se sont développées
- Les modes opératoires dépassent les recherches
- L'ingénierie sociale a toujours un pas d'avance
- Difficulté d'adaptation à une société disruptive

**CEPOL**

## Tout va de plus en plus vite pour le numérique !

- 1 700 générations pour maîtriser le langage,
- 300 pour l'écriture,
- 30 pour l'imprimerie,
- 2 pour passer de l'analogique au numérique
- 1 pour la transformation numérique.
- 3 minutes pour attaquer aujourd'hui votre PC (40 mns en 2003 !)

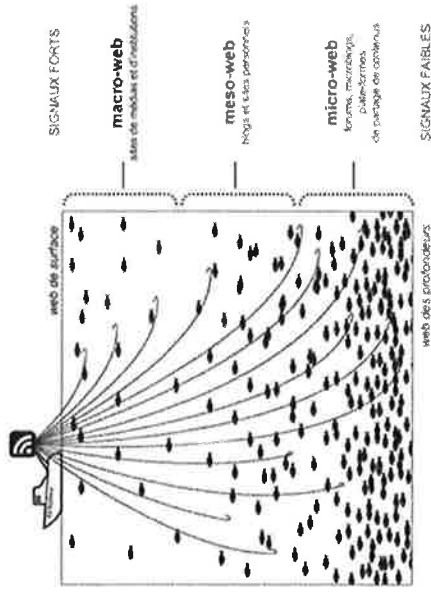
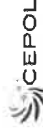
**CEPOL**

## Un univers informationnel infini ...

1. Les algorithmes nous construisent
2. Mobile first et nouvelles interfaces
3. Bots et chatbots
4. Réalité augmentée ou réalité virtuelle
5. Big Data
6. Méta données, micro données, mégadonnées
7. Du cloud à l'Edge
8. Réseaux sociaux et nouveaux usages informationnels
9. Blogs, wikis et forums
10. GDPR et protection des données personnelles



## Les profondeurs du Web




## Du Web 0.0 au Web 5.0 l'information évolue

- Web 0.0 le développement de l'Internet (1993)
- Web 1.0 ou le Web statique (1998)
- Web 2.0 ou le Web social (2004)
- Web 3.0 ou le Web sémantique (2010)
- Web 4.0 ou le Web mobile (2018)
- Web 5.0 ou le Web ouvert, lié et intelligent (2020)




<https://www.submarinecablemap.com/>



CEPOL

**285 câbles sous-marins**

L'Algérie partiellement privée d'Internet durant plus de 2 jours en avril 2017




CEPOL

**Du Besoin de nuire à celui de s'enrichir !**

- Aujourd'hui la téléphonie fixe et mobile sont touchées
- Les systèmes de traitement automatisés de données (STAD)
- Les cartes à puces, guichets automatiques, capteurs, centres de contrôle, systèmes de navigation assistée, jeux, etc.
- En fait tout ce qui manipule de l'information est touché !
- Le tout couplé à 50 milliards d'objets connectés en 2020 ... un cocktail détonnant !!!
- **La cybersécurité est devenue une priorité pour nos états.**

CEPOL




Des cybercriminels et Hackers recherchent des informations concernant la recherche et développement (R&D).


Des données stratégiques par les entreprises.

De l'Etat ne

CEPOL





**Hacker n°1 : le justicier**  
**Hacker n°2 : l'ado**  
**Hacker n°3 : l'espion**  
**Hacker n°4 : le mercenaire**  
**Hacker n°5 : l'ingénieur**  
**Hacker n°6 : l'escroc**


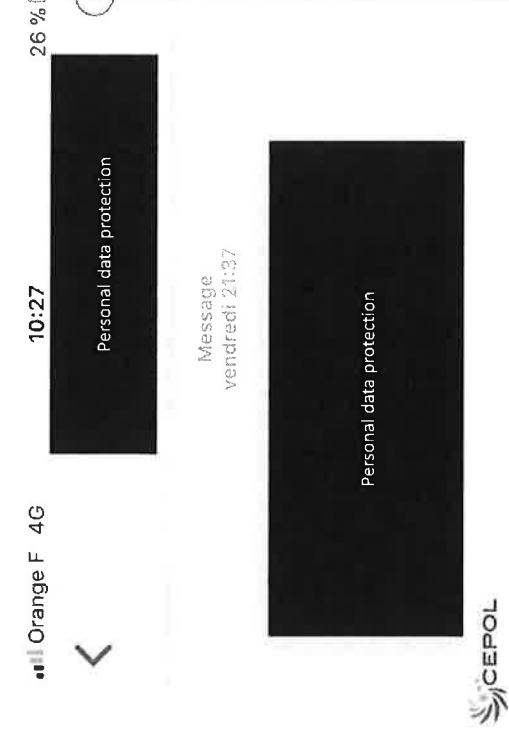


### De la cybercriminalité à la cybersécurité

- ▀ Toujours pas de définition universelle de la cybercriminalité
- ▀ Inclut les infractions informatiques (comme le piratage informatique) et les infractions dites de contenu
- ▀ D'une manière générale, la cybercriminalité est définie comme l'ensemble des infractions pénales commises via les réseaux informatiques.
- ▀ Il faut y rajouter les appareils nomades aujourd'hui

De nouvelles menaces utilisant l'information se développent dans chacun de ces Web.XX puis certaines personnes à la recherche de profit ou de pouvoir tentent d'atteindre leurs objectifs criminels...





Orange F 4G 10:27 26 %

Personal data protection

Message vendredi 21:37

Personal data protection





## Atteintes aux personnes



- Diffusion de contenus offensifs
- Incitation à la haine raciale, propagande
- Diffamation, chantage, intimidation, harcèlement, injures
- Vie privée, usurpation d'identité et e-réputation
- Vol de données personnelles et confidentielles, ressources et services
- Escroqueries, fraudes et abus
- Atteintes à l'image, au secret professionnel
- Les chaînes de solidarité
- .../...



## Atteintes aux organisations



- Espionnage industriel
- Manipulation d'informations, défiguration de sites Web, diffusion de rumeurs
- Intrusions
- Arnaques au président (FOVI)
- Manipulation des marchés financiers
- Fraude aux cartes de crédit
- Monnaies virtuelles comme placements alternatifs (Bitcoin, Ethereum, ...)
- Espionnage, fuite et pillage de données



## Atteintes aux états

- Intrusion dans cyber-administration
- Manipulation de l'expression démocratique (Fake news, systèmes de votes électroniques, comptage de bulletins, ...)
- Intrusion dans systèmes informatiques contrôlant les infrastructures critiques (l'énergie, l'eau, ...)
- Cyber-terrorisme, cyberconflits et cyberguerre
- Manipulation d'opinions



## Atteintes aux critères de sécurité

- Attaques en déni de service distribué (Ddos) portant préjudice aux utilisateurs, propriétaires et exploitants de ressources ou de traitements
- Ecoutes et vols de données
- Altération de données et de matériels
- Manipulation, brouillage de l'information et infox





## Internet:

### place de marché de la cybercriminalité

- Existence d'un marché des vulnérabilités et des logiciels d'exploitation qui les exploitent (Exploits)
- Existence d'un marché de la commercialisation des failles trouvées dans les applications (0-day)
- Des fournisseurs de service proposent aussi des récompenses pour la découverte de nouvelles vulnérabilités (notion de Bug Bounty) afin de rémunérer les découvreurs de failles et les dissuader de les vendre au marché noir.



## Autres cybermenaces ...

- Les atteintes d'espionnage et de sabotage
- La Malveillance ou la Propagande (La défiguration de site, le faux technicien informatique, les fausses pages, Les fake-news)
- Les infractions de presse
- La pédopornographie
- Le cyber-harcèlement, sextorsion, sex-tape etc...
- L'apologie du terrorisme



## EVOLUTION DES MENACES 2010-2018

- 2011 : l'année des violations de données
- 2012 : l'ère post-pc (attaques Android, plateformes média sociaux)
- 2013: les cambriolages à l'ancienne laissent place aux détournements numériques
- 2014 : l'ère de la cyberattaque
- 2015 : l'année des gros Botnets
- 2016 : l'ère de l'extorsion numérique
- 2017 : l'ère suprême des Ransomwares (Wannacry, Petya, ...)



27

## Les attaques homographes : ne croyez pas tout ce que vous voyez!

Une attaque homographe (ou Homograph Attack en Anglais) correspond à ce qui se produit lorsque des hackers enregistrent des domaines quasi similaires aux originaux, avec des certificats valides.



Une variante du ver Stuxnet plus sophistiquée et dangereuse a ciblé l'infrastructure réseau de l'Iran. L'agence de la défense civile de ce pays ne s'est pas étendue sur d'éventuels dégâts.



La bombe nucléaire de Boudak, au Iran, a été mise en service en septembre 2011. (photo : D.K.)



## Changement

- Les groupes APT étendent leur champ d'action
- Diversification des modes d'attaque
- Le cryptojacking, nouvelle plaie des entreprises
- Fraudes à la carte bancaire et au paiement sans contact
- La cybercriminalité s'attaque aux objets connectés
- Et l'intelligence artificielle s'en mêle ...



Nos données personnelles deviennent aussi des données intelligentes pour des personnes mal intentionnées voire des cyber-délinquants !

## Les profondeurs du Web







Un outil qui vous en dit plus sur les profils FACEBOOK

stalkscan.com

Navigation menu: Accueil, Recherche, Social Scan, Blog, Contact, Inscription

Recherche:  Rechercher

Footer: Tous droits réservés © Stalkscan 2019

CEPOL

Facebook Graph Search pour en savoir plus sur vos amis

CEPOL

Youseemii

Navigation menu: Accueil, Recherche, Social Scan, Blog, Contact, Inscription

Captez ce qui se dit !

Recherche:  Rechercher

Footer: Tous droits réservés © Youseemii 2019

Tous les réseaux sociaux à portée de main

CEPOL

La visibilité d'une personne sur Internet

WebMit

Recherchez une personne et découvrez son score de visibilité.

CEPOL

# La cartographie

Personal data protection

immersion

a people-centric view of your email life

# Cartographie d'une adresse GMAIL

This information cannot be disclosed due to personal data protection

11.4 years 11.4 years 17 Jan 2019

# ADN NUMERIQUE dans le cadre d'une enquête :

## Un peu de méthodologie

ADN NUMERIQUE

Savoir surveiller l'information en pratiquant :

- La veille manuelle
- La veille automatisée
- La veille cartographique
- La veille média

# Explorer le Web profond

The screenshot shows the Exalead search engine interface. At the top, there's a search bar with the text 'projet de loi' and a search button. Below the search bar, there are several search results. The first result is from 'Le Monde' and is titled 'Projet de loi relatif à la sécurité des données'. The second result is from 'Le Monde' and is titled 'Projet de loi relatif à la sécurité des données'. The third result is from 'Le Monde' and is titled 'Projet de loi relatif à la sécurité des données'. The interface also includes a sidebar with navigation options like 'Accueil', 'Recherche', and 'Filtres'.

# Des outils d'alerte

This slide features three logos for alerting tools. On the left is 'talkwalkeralerts' with a speech bubble icon. In the center is the 'Google Alerts' logo. On the right is 'alerti' with a circular icon containing a speech bubble.

# SUREVEILLER UNE PAGE

The slide displays the 'Distill' logo, which consists of a stylized white 'D' shape on a dark background.

# SpyOnWeb

The screenshot shows the SpyOnWeb website interface. It features a search bar with the text 'URL, IP Address, public IP ranges or ASN (153.104.0.0)'. Below the search bar, there are several search filters and results. The filters include 'Unique Domains', 'Unique IP Addresses', 'Unique Subdomains', 'Unique Autonomous IDs', and 'Unique Anonime IDs'. The results show a list of domains and their corresponding IP addresses.

## Les origines d'un site Internet

**DOMANTOOLS** [WHOIS](#) [DNS](#) [SECURITY](#) [SERVICES](#) [CONTACT](#) [ABOUT](#)

**Whois Record for CyberCriminalTech.blog**

Domain Profile  
 Registered: REDACTED FOR PRIVACY  
 Registered On: REDACTED FOR PRIVACY  
 Registrar: GoDaddy, US

Administrative Contact  
 Name: REDACTED FOR PRIVACY  
 Email: REDACTED FOR PRIVACY  
 Phone: REDACTED FOR PRIVACY  
 Address: REDACTED FOR PRIVACY

Technical Contact  
 Name: REDACTED FOR PRIVACY  
 Email: REDACTED FOR PRIVACY  
 Phone: REDACTED FOR PRIVACY  
 Address: REDACTED FOR PRIVACY

Registrar Contact  
 Name: REDACTED FOR PRIVACY  
 Email: REDACTED FOR PRIVACY  
 Phone: REDACTED FOR PRIVACY  
 Address: REDACTED FOR PRIVACY

Creation Date: 2019-02-19  
 Expiration Date: 2020-02-19  
 Updated Date: 2019-12-12  
 Registrar: GoDaddy, US

Nameservers  
 NS1.VISITORPRESS.COM (IP: 1.88.122.100)  
 NS2.VISITORPRESS.COM (IP: 1.88.122.100)

## Tineye pour retrouver les autres sources d'une image

Tineye est accessible en ligne sans inscription. En téléchargeant une image directement sur le site ou en renseignant son URL, on accède à une liste de sources où la même image est utilisée. Il peut s'agir de bases de données, de blogs ou de sites d'informations. Une simple recherche sur une image présentée comme une image d'actualité permet ainsi de vérifier si l'image est antérieure, c'est-à-dire si elle existait déjà sur internet avant sa date supposée. Mieux, encore : en la couplant avec un outil qui recherche les métadonnées de chaque image, on peut en trouver la date d'origine. Pratique !



## Connaître les données Exif pour identifier l'auteur ou le lieu

Exif signifie « exchangeable image file format »

**metapicz**  
(ORIGINE DES DONNÉES)

Something is wrong on the go? Try Secure Archive for images and images!

metapicz analyzes its your blog with our exclusive algorithm

Drop image files here

or select

or enter the picture URL

https://www.123.com

GO!

## Forensically pour détecter les retouches d'image





## L'origine d'une vidéo avec In Video Veritas

## L'origine d'un site

## La Threat Intelligence, le salut des entreprises

- Security report 2016 de Check Point a révélé une multiplication par neuf du volume de logiciels malveillants inconnus attaquant les entreprises.
- Près de 12 millions de nouvelles variantes de logiciels malveillants sont identifiées tous les mois. Les logiciels rançonneurs sont désormais particulièrement répandus.
- Ils deviendront aussi problématiques que les attaques DDoS en 2017.

## Protéger son environnement numérique

Quelques consignes ...

- Connaître ses vulnérabilités
- La protection du matériel
- Les lieux publics et le Wifi
- Protéger ses données
- Gérer ses mots de passe et ses autorisations
- Protéger sa navigation

## Bonnes pratiques en voyage

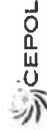


<https://www.ivision.fr/13-bonnes-pratiques-de-securite-informatique-en-voyage-daffaires/>

This information cannot be disclosed due to personal data protection

Merçi pour votre attention...

European Union Agency for Operational Cooperation in the Field of Police (EUROPOL)  
Office: H-1066 Budapest, Hungary  
Telephone: +36 1 803 8030 • Fax: +36 1 803 8031 • E-mail: [europol@europol.europa.eu](mailto:europol@europol.europa.eu) • [www.europol.europa.eu](http://www.europol.europa.eu)



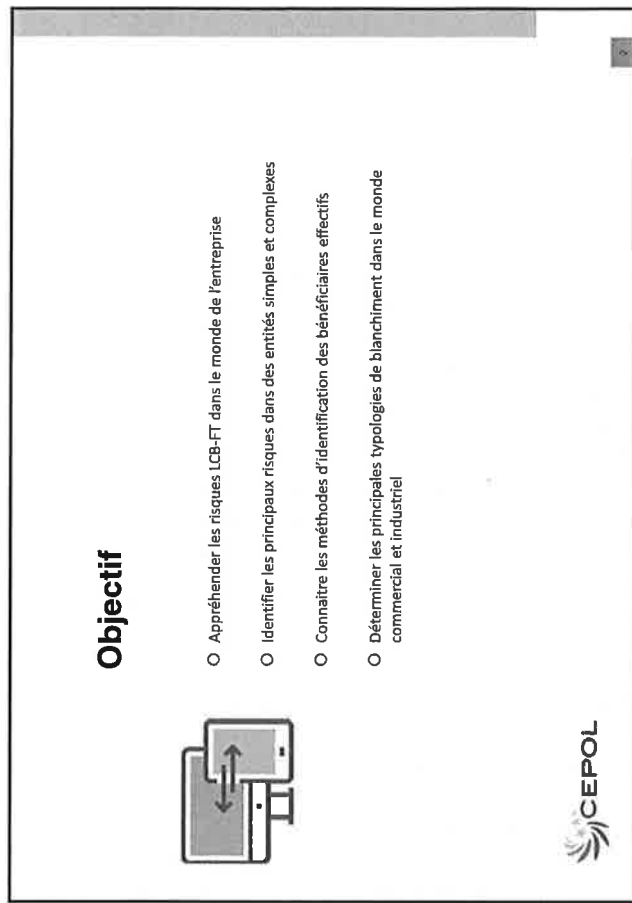


**CEPOL**

**Structures d'entreprises, bénéficiaires effectifs et blanchiment de capitaux**

**Personal Data**  
Investigative Financial Investigation Course  
Subjects: Funds  
26/03/2019 - 1 March 2019

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING



**Objectif**

- Appréhender les risques LCB-FT dans le monde de l'entreprise
- Identifier les principaux risques dans des entités simples et complexes
- Connaître les méthodes d'identification des bénéficiaires effectifs
- Déterminer les principales typologies de blanchiment dans le monde commercial et industriel

**CEPOL**



## Sommaire

1. Principes généraux
2. Structures simples et structures complexes
3. De l'actionnariat au bénéficiaire effectif
4. Principales typologies de blanchiment en lien avec l'entreprise
5. Mise en situation – cas pratique

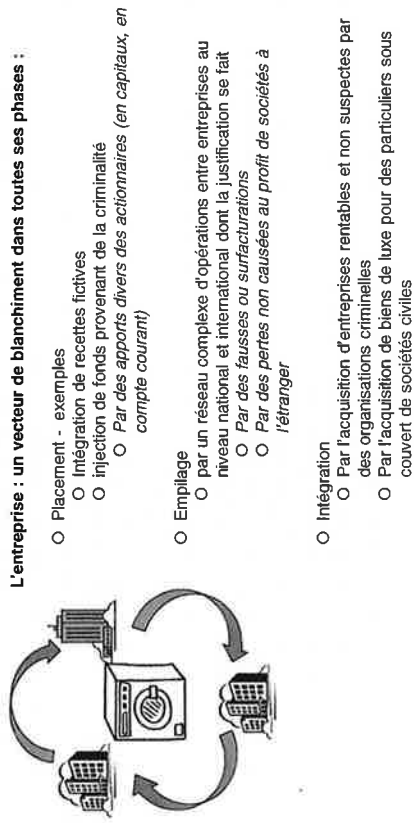


## Introduction

- Le monde de l'entreprise est le principal outil de la délinquance économique et financière /
  - Par de nombreuses infractions financières dont la corruption et les fraudes
  - Par le blanchiment de ces infractions et de celles de droit commun (dont les trafics de stupéfiants, d'armes, d'êtres humains, de biens culturels....)
- Les sommes en jeu sont considérables et la plus grande part des opérations de blanchiment passent par les sociétés, trusts et autres structures économiques
- L'entreprise est utilisée avec les mêmes moyens que ceux existants pour l'industrie et le commerce licite
  - Conséquences
    - *Très grande rapidité dans le processus de blanchiment*
    - *Difficultés à identifier les fonds douteux dans un système économique et financier mondialisé et dont la grande majorité est licite*

## 1- Généralités

L'entreprise : un vecteur de blanchiment dans toutes ses phases :



- Placement - exemples
  - Intégration de recettes fictives
  - Injection de fonds provenant de la criminalité
    - Par des apports divers des actionnaires (en capitaux, en compte courant)
- Empliage
  - par un réseau complexe d'opérations entre entreprises au niveau national et international dont la justification se fait
    - Par des fausses ou surfacturations
    - Par des pertes non causées au profit de sociétés à l'étranger
- Intégration
  - Par l'acquisition d'entreprises rentables et non suspectées par des organisations criminelles
  - Par l'acquisition de biens de luxe pour des particuliers sous couvert de sociétés civiles

## 1- Généralités

L'entreprise : un outil de blanchiment pouvant être utilisé :

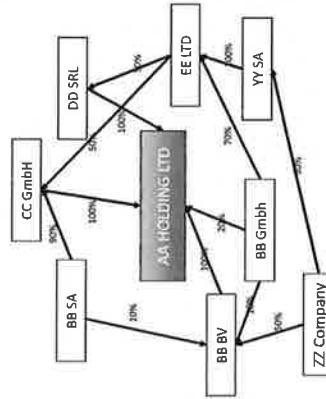


- Exclusivement pour des opérations de blanchiment
  - sociétés taxi / coquilles vides
  - Sociétés dans des domiciliations commerciales
  - Sociétés dans des paradis fiscaux
- En complément d'une activité licite
  - Sociétés ayant une existence et une activité réelle
    - Soit une part de l'activité est fictive
    - Soit les apports des actionnaires sont issus de la criminalité organisée
- Pour commettre des infractions primaires liées à l'activité licite
  - Corruption
  - Fraudes fiscales
  - Abus de biens sociaux

## 2 – Structures simples et structures complexes

### Rappel des différents types de structures entrepreneuriales

- Activité en nom propre
- Sociétés
  - En nom propre
  - De capitaux
  - Mixtes



Les sociétés peuvent être civiles ou commerciales  
 Des sociétés peuvent être actionnaires d'autres sociétés et avoir aussi des participations croisées  
 Elles peuvent être filiales ou succursales



## 2 - Structures simples et structures complexes

### 3 catégories distinctes

- **Les sociétés de personnes**
  - Sociétés basées sur un fort intuitu personae : exemples
  - Les sociétés civiles (ex. SCI, SCP et SNC)
  - Les sociétés en commandite simple
- **Les sociétés de capitaux**
  - Des sociétés le plus souvent commerciales constituées sur la base de capitaux apportés : exemples
  - Les sociétés anonymes et SAS
  - Les sociétés en commandite par actions
- **Les sociétés mixtes**
  - Des sociétés de capitaux mais avec un intuitu personae fort
  - SARL, EURL



## 2 – Structures simples et structures complexes



Le choix de la forme dépend de plusieurs critères :

- Le nombre d'associés/ actionnaires
- Les moyens financiers dont ils disposent
- L'importance de l'intuitu personae
  - Conséquences sur les cessions de parts nécessitant ou pas l'accord des autres associés
- La responsabilité financière des associés
  - Personnellement ou solidairement responsables
  - Limitée au montant de leurs apports
- Importance du paramètre fiscal



3

## 2 – Structures simples et structures complexes



Le choix de la structure par les organisations criminelles

- La finalité de la structure à court ou long terme
- Les coûts de mise en place
- La nécessité d'éviter les contrôles ou pas
- Le besoin de limiter les risques d'être identifiés

Exemples de choix de structures simples ou complexes

- Fraude à la TVA
  - Structures simples et récentes
- Blanchiment de capitaux provenant d'un trafic
  - Structures simples (intégration de recettes de deal de rue)
  - Structures complexes (si producteurs ou grossistes compte tenu des montants importants à blanchir)



17

## 2 – Structures simples et structures complexes

Quelques indicateurs de risques sur la structure des entreprises

• Risques sur la typologie des entreprises

- Entreprises unipersonnelles et SARL (petites structures avec peu ou sans salarié) ou holdings
- Structures complexes avec des liens capitalistiques croisés notamment
- Sociétés en domiciliation commerciale
- Sociétés de droit étranger immatriculé ou non en France
- Sociétés nouvellement créées ou/et sans activité depuis plusieurs mois
- Sociétés ayant un objet très large ou des activités diverses sans logique économique
- Sociétés sans salariés apparemment proposant de la sous-traitance
- Sociétés nouvelles ayant un nom ou une dénomination commerciale proche d'un nom ou d'une marque connue
- Sociétés en difficultés financières ayant un potentiel ou pas

Indicateurs de  
risques liés aux  
structures



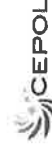
11

## 2 – Structures simples et structures complexes

Holdings, Trustes et Fiducies : des structures complexes présentant des risques intrinsèques de blanchiment de capitaux



- Holding
  - Société mère et consolidante, qui gère et contrôle des sociétés ayant des intérêts communs
  - Holding pure lorsqu'elle n'a pas d'activité
  - Holding mixte lorsqu'elle en conserve une ou plusieurs
    - Holding bancaire
    - Holding financière ...
- Trust
  - Notion par laquelle la propriété d'un bien, détenue par son fondateur (settlor), est confiée à un détenteur (trustee), à charge pour lui de l'administrer pour le compte d'un bénéficiaire (beneficiary)
- Fiducie
  - Un ou plusieurs constituants transfèrent des biens à un ou plusieurs fiduciaires, qui agissent au profit d'un ou plusieurs bénéficiaires, en les gérant séparément de leur patrimoine propre.



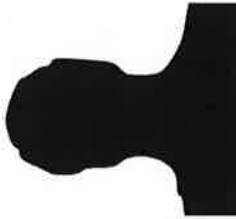
12



### 3 – De l'actionnaire au bénéficiaire effectif d'une entreprise ou d'un groupe d'entreprise

#### L'imbrication de structures complexes pour cacher le réel bénéficiaire

- Notion de bénéficiaire effectif
  - Une personne physique qui est le véritable détenteur du capital ou d'un pourcentage important ou des droits de vote
  - Une personne physique qui contrôle et qui tire les ficelles ... et les bénéfices
- Des recommandations du GAFI pour :
  - Obliger les entités personnes morales à déclarer leurs bénéficiaires directs ou indirects (personnes physiques)
  - Obliger les banques et établissements assujettis à n'entrer en relation d'affaires qu'après identification du bénéficiaire effectif
- Principe du GAFI
  - Toute personne physique qui détiend directement ou indirectement plus de 25% du capital ou des droits de vote
  - Toute personne physique contrôlant la société (pour éviter de limiter les recherches aux seuls porteurs d'actions pour le compte de tiers)



### 3 – De l'actionnaire au bénéficiaire effectif d'une entreprise ou d'un groupe d'entreprise

#### Indicateurs sur les dirigeants et actionnaires

- Risques liés aux dirigeants et détenteurs du capital social
  - Faiblesse du capital au regard des besoins pour l'activité
  - Les associés ont précédemment dirigé des entités éphémères en liquidation
  - Dirigeants jeunes ou très âgés
  - Pour les petites structures, le dirigeant n'est pas associé notamment dans les entreprises unipersonnelles
- Personnes physiques ou/et sociétés associées implantées à l'étranger et notamment dans des pays à risques ou et non cohérent avec l'activité
  - Changements récents et/ou successifs de dirigeants et/ou associés notamment peu de temps après création
- Risques liés à l'implantation géographique de la société
  - zones urbaines à risque (risques plus élevés d'économie souterraine)
  - Filiales ou succursales dans des pays à risque

### CAS PRATIQUE

IDENTIFICATION D'UN BÉNÉFICIAIRE EFFECTIF

Bénéficiaire(s) effectif(s) ?

M.A. = 60 %  
 M.A. = 3,0 %  
 M.M. = 60 %  
 M.M. = 15,6 %

CEPOL

### CAS PRATIQUE

This slide cannot be disclosed due to personal data

CEPOL

#### 4- Les principales typologies de criminalité organisée et de blanchiment dans le monde de l'entreprise

- Typologies relatives à la commission d'une infraction initiale
  - Schémas de fraude fiscale ou de dissimulation de bénéfices
  - Schémas de corruption (ou d'abus de biens sociaux)
  - Schémas de travail dissimulé
- Typologies de blanchiment d'infraction initiales
  - Schéma de blanchiment complexe lié au trafic de stupéfiants
  - Perte provoquée et apports en capitaux ou compte courant
  - Pénalités sur des contrats non causés
  - Rachat de sociétés par des fonds étrangers provenant de pays à risque

#### Schéma de fraude fiscale

This slide cannot be disclosed due to public security


This slide cannot be disclosed due to public security

## Les principales typologies de criminalité organisée et de blanchiment dans le monde de l'entreprise

- Typologies relatives à la commission d'une infraction initiale
  - Schémas de fraude fiscale ou de dissimulation de bénéfices
  - Schémas de corruption (ou d'abus de biens sociaux)
  - Schémas de travail dissimulé
- Typologies de blanchiment d'infraction initiales
  - Schéma de blanchiment complexe lié au trafic de stupéfiants
  - Perte provoquée et apports en capitaux ou compte courant
  - Pénalités sur des contrats non causés
  - Rachat de sociétés par des fonds étrangers provenant de pays à risque




This slide cannot be disclosed due to public security



21


### Les principales typologies de criminalité organisée et de blanchiment dans le monde de l'entreprise

- Typologies relatives à la commission d'une infraction initiale
  - Schémas de fraude fiscale ou de dissimulation de bénéfices
  - Schémas de corruption (ou d'abus de biens sociaux)
  - Schémas de travail dissimulé
- Typologies de blanchiment d'infraction initiales
  - Schéma de blanchiment complexe lié au trafic de stupéfiants
  - Perte provoquée et apports en capitaux ou compte courant
  - Pénalités sur des contrats non causés
  - Rachat de sociétés par des fonds étrangers provenant de pays à risque



22


This slide cannot be disclosed due to public security



71

### Les principales typologies de criminalité organisée et de blanchiment dans le monde de l'entreprise

- Typologies relatives à la commission d'une infraction initiale
  - Schémas de fraude fiscale ou de dissimulation de bénéfices
  - Schémas de corruption (ou d'abus de biens sociaux)
  - Schémas de travail dissimulé
- **Typologies de blanchiment d'infraction initiales**
  - Schéma de blanchiment complexe lié au trafic de stupéfiants
  - Perte provoquée et apports en capitaux ou compte courant
  - Pénalités sur des contrats non causés
  - Rachat de sociétés par des fonds étrangers provenant de pays à risque

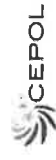


74


This slide cannot be disclosed due to public security

## Les principales typologies de criminalité organisée et de blanchiment dans le monde de l'entreprise

- Typologies relatives à la commission d'une infraction initiale
  - Schémas de fraude fiscale ou de dissimulation de bénéfices
  - Schémas de corruption (ou d'abus de biens sociaux)
  - Schémas de travail dissimulé
- Typologies de blanchiment d'infraction initiales
  - Schéma de blanchiment complexe lié au trafic de stupéfiants
  - Perte provoquée et apports en capitaux ou compte courant
  - Pénalités sur des contrats non causés
  - Rachat de sociétés par des fonds étrangers provenant de pays à risque



This slide cannot be disclosed due to public security




CEPOL

32

### Les principales typologies de criminalité organisée et de blanchiment dans le monde de l'entreprise


- Typologies relatives à la commission d'une infraction initiale
  - Schémas de fraude fiscale ou de dissimulation de bénéfices
  - Schémas de corruption (ou d'abus de biens sociaux)
  - Schémas de travail dissimulé
- Typologies de blanchiment d'infraction initiales
  - Schéma de blanchiment complexe lié au trafic de stupéfiants
  - Perte provoquée et apports en capitaux ou compte courant
  - Pénalités sur des contrats non causés
  - Rachat de sociétés par des fonds étrangers provenant de pays à risque



31




This slide cannot be disclosed due to public security



2

### Les principales typologies de criminalité organisée et de blanchiment dans le monde de l'entreprise

- Typologies relatives à la commission d'une infraction initiale
  - Schémas de fraude fiscale ou de dissimulation de bénéfices
  - Schémas de corruption (ou d'abus de biens sociaux)
  - Schémas de travail dissimulé
- Typologies de blanchiment d'infraction initiales
  - Schéma de blanchiment complexe lié au trafic de stupéfiants
  - Perte provoquée et apports en capitaux ou compte courant
  - Pénalités sur des contrats non causés
  - Rachat de sociétés par des fonds étrangers provenant de pays à risque



3

## Rachat de sociétés par des fonds étrangers provenant de pays à risque

Des entreprises françaises sous contrôle d'oligarques azerbaïdjanais via le paravent  
maltais  
Publié le mercredi 18 avril 2018 à 18h07 (source Radio France)

L'enquête de 18 médias internationaux sur la corruption à Malte révèle qu'une  
banque suspecte a permis l'entrée en Europe de capitaux liés à la dictature  
azerbaïdjanaise. Une partie d'entre eux a servi à acheter des entreprises en France.

- Comment une fabrique de haute porcelaine de Limoges, un vénérable atelier de linge  
de maison de luxe de Cambrai et un fabricant de figurines de Neuchâtel-en-Bray ont-  
ils pu tomber dans l'escarcelle d'une famille d'oligarques parmi les plus puissantes  
d'Azerbaïdjan, sans que personne – ou presque – ne le sache ?



11

## 5 – Exercice pratique

**Vous êtes responsable d'un service spécialisé dans la lutte  
contre la criminalité organisée et le blanchiment de capitaux**

- Selon une information recoupée de plusieurs directions de police  
Monsieur X, homme d'affaires important qui est dirigeant d'une  
holding utiliserait ses entreprises pour blanchir à grande échelle  
de l'argent de divers trafics et défendrait en sous main des  
établissements de nuit.



*Avant de démarrer toute enquête,  
quelles sont les premières vérifications que vous envisagez*



12

### 5 – Exercice pratique

- Lors de surveillances d'un établissement de nuit flambant neuf, des collègues, ayant des doutes sur Monsieur Z, gérant de cette entreprise, constatent à plusieurs reprises la présence de Monsieur X, entouré de gardes du corps, parmi les clients
- Il reste la plupart du temps assis, discute avec d'autres clients qui viennent le voir avant de partir sans payer ses consommations



*Quelles sont les éléments nouveaux et les informations nécessitant des vérifications*



39

### 5 – Exercice pratique

- L'établissement de nuit a été créé par un groupe de sociétés tunisiennes et étrangères ainsi que le gérant pour un capital de 120,000 dinars entièrement libéré
- Le gérant est salarié et associés à 28 %
- Il reste la plupart du temps assis, discute avec d'autres clients qui viennent le voir avant de partir sans payer ses consommations
- Le service travaillant sur le gérant souhaite dans le cadre d'une coopération votre expertise sur le gérant




*Quelles sont les éléments nouveaux et les informations nécessitant des vérifications*



38


11


### 5 – Exercice pratique



- L'enquête sur le gérant démontre qu'il n'avait auparavant jamais hormis au cours des 6 mois précédents comme salarié d'une des filiales de Monsieur X.
- Sa part libérée provient principalement d'économies réalisés grâce à des salaires relativement élevés versés sur son compte bancaire

*Quelles sont les éléments nouveaux et les informations nécessitant des vérifications et quelle seraient les étapes suivantes permettant de démontrer l'implication de Monsieur X dans un processus de blanchiment*





**Thank you for your attention!**

European Union Agency for Law Enforcement Training  
Offices: H-1066 Budapest, O. Buda, 210. Helység, 1066 Budapest, P. Helység  
Telephone: +36 1 803 8030 • Fax: +36 1 803 8031 • E-mail: [www.cepola.eu](mailto:www.cepola.eu)

