



This project is funded  
by the European Union



**T 06**

**CEPOL Western Balkan Financial Investigation In-Service Training (WB FI)  
'Financial Investigations in relation to Drug Trafficking'  
08-12 October 2018 in Prishtina, KOSOVO**

Arrival Sunday	Monday 08 October	Tuesday 09 October	Wednesday 10 October	Thursday 11 October	Friday 12 October
Arrival of participants	09.00-10.00 Course opening and Introduction of CEPOL and the WB FI Project	09.00-10.00 Intelligence led Investigations	09.00-10.00 Economic crime	09.00-10.00 Introduction to ciber threats	09.00-10.00 Investigation through data analysis
	10.00-11.00 'Family Photo' and Introduction	10.00-11.00 Preliminary investigations and Prosecutor led Investigations	10.00-11.00 Tax Crime	10.00-11.00 OSINT and Darknet Investigations	10.00-11.00 Evaluation
	11.00-11.30 Coffee Break	11.00-11.30 Coffee Break	11.00-11.30 Coffee Break	11.00-11.30 Coffee Break	11.00-11.30 Coffee Break
	11.30-12.30 From Money to crime or vice versa with Drug Trafficking	11.30-12.30 Joint Investigation Team(s)	11.30-12.30 Albanian speaking organised crime in the EU and Transatlantic	11.30-12.30 OSINT and Darknet Investigations	11.30-12.30 Certification
	12.30-13.30 Lunch	12.30-13.30 Lunch	12.30-13.30 Lunch	12.30-13.30 Lunch	12.30-13.30 Lunch











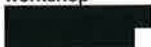





This project is funded  
by the European Union



**T06**

**CEPOL Western Balkan Financial Investigation In-Service Training  
'Financial Investigations in relation to Drug Trafficking'  
08-12 October 2018 in Prishtina, KOSOVO**

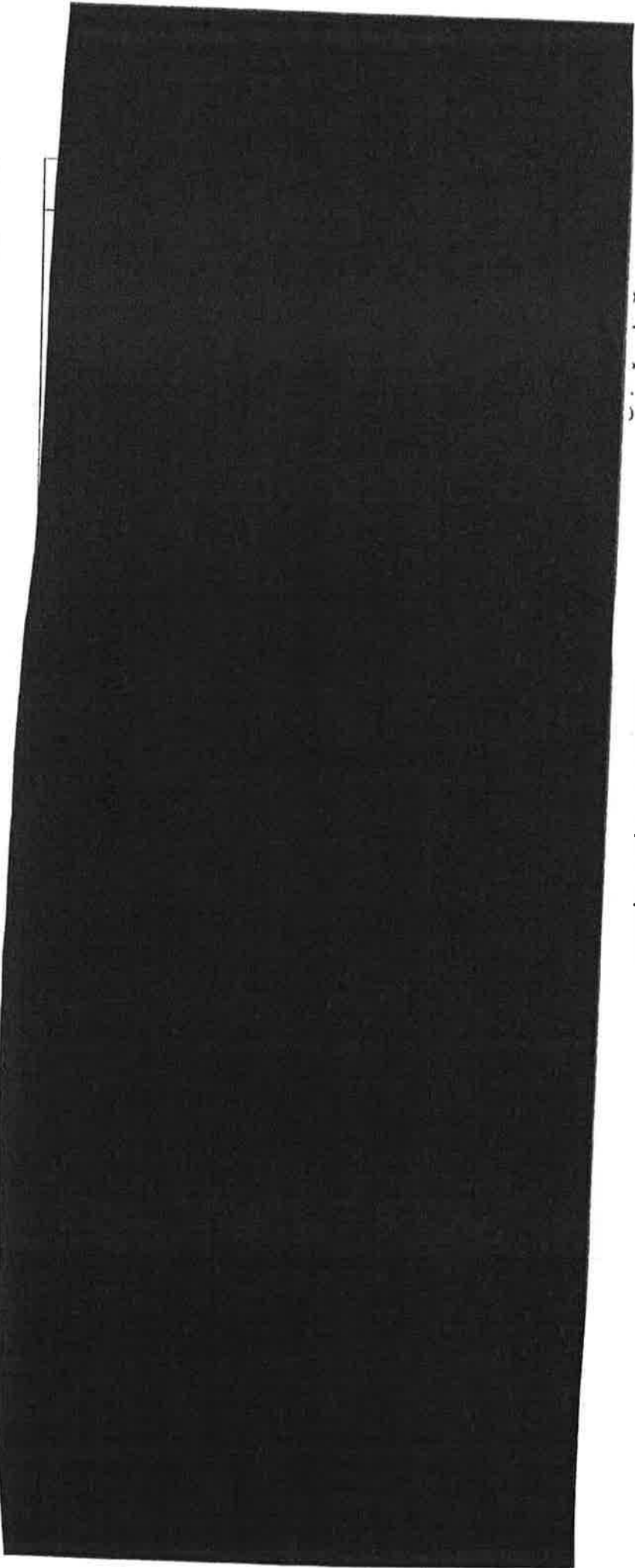
	<b>Monday 08</b>		<b>Tuesday 09</b>		<b>Wednesday 10</b>		<b>Thursday 11</b>	<b>Friday 12</b>
13.30-14.30	Example of Successful Action Plans, including National Drug Strategies 	13.30-14.30	Joint Investigation Team(s) 	13.30-14.30	Camden Assets Recovery Network (CARIN); Criminal Assets and Strategy against OC and Money Laundering; Development of Joint Investigation Unit; Financial Investigation Units 	13.30-14.30	OSINT and Darknet Investigations 	
14.30-15.00	Coffee break	14.30-15.00	Coffee break	14.30-15.00	Coffee break	14.30-15.00	Coffee break	Departure of participants  
15.00-16.00	Various forms of money laundering in Drug Trafficking 	15.00-16.00	JIT case study 	15.00-16.00	EUROPOL 	15.00-16.00	Drug Markets on the Internet and Darknet 	
16.00-17.00	Discussion / workshop 	16.00-17.00	Challenges in asset recovery: Discussion 	16.00-17.00	EUROPOL 	16.00-17.00	Cross cutting multidisciplinary challenges – discussion 	
19.00	Dinner	19.00	Dinner	19.00	Dinner	19.00	Dinner	



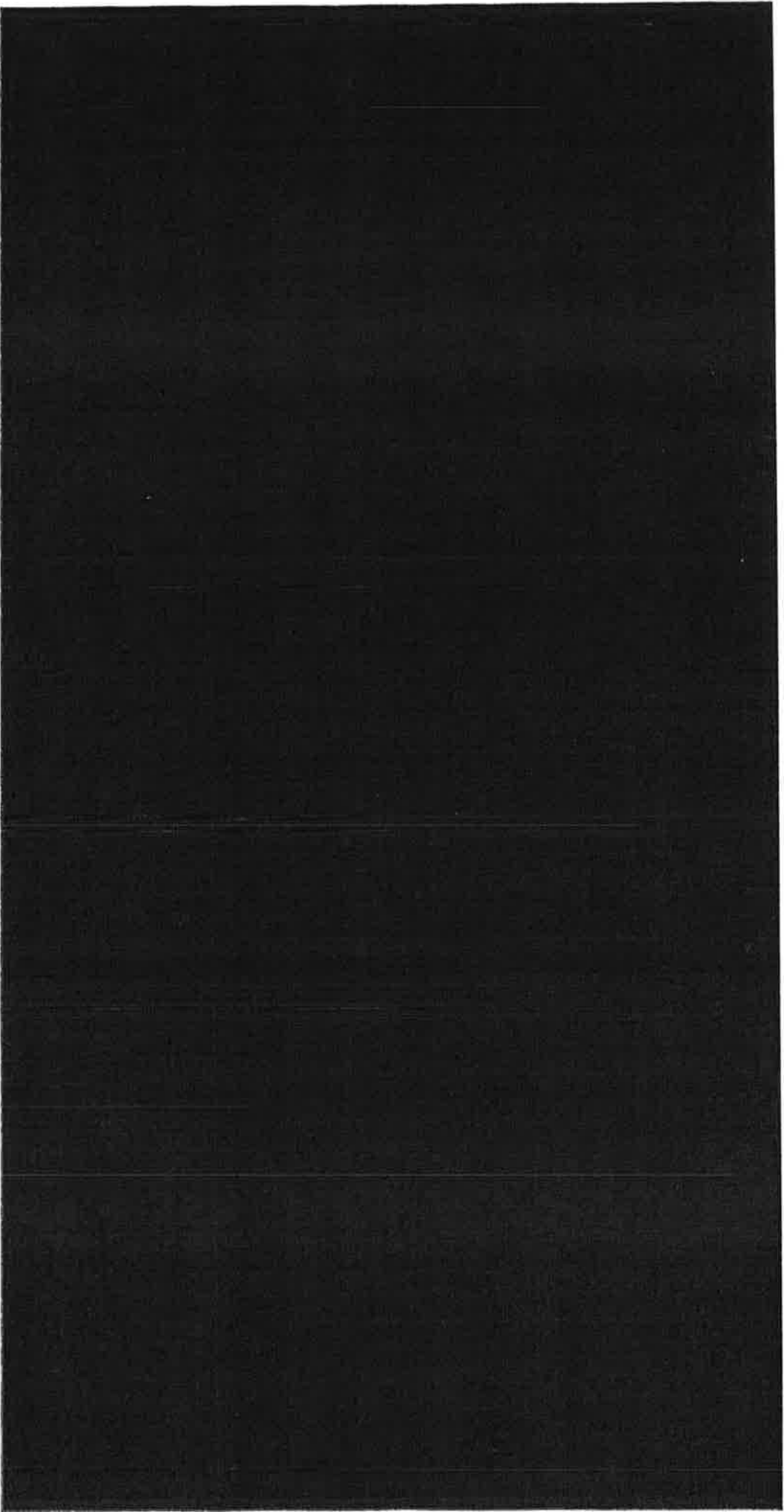
**Financial Investigation in relation to Drug Trafficking**

**08-12 October Prishtina Kosovo\***

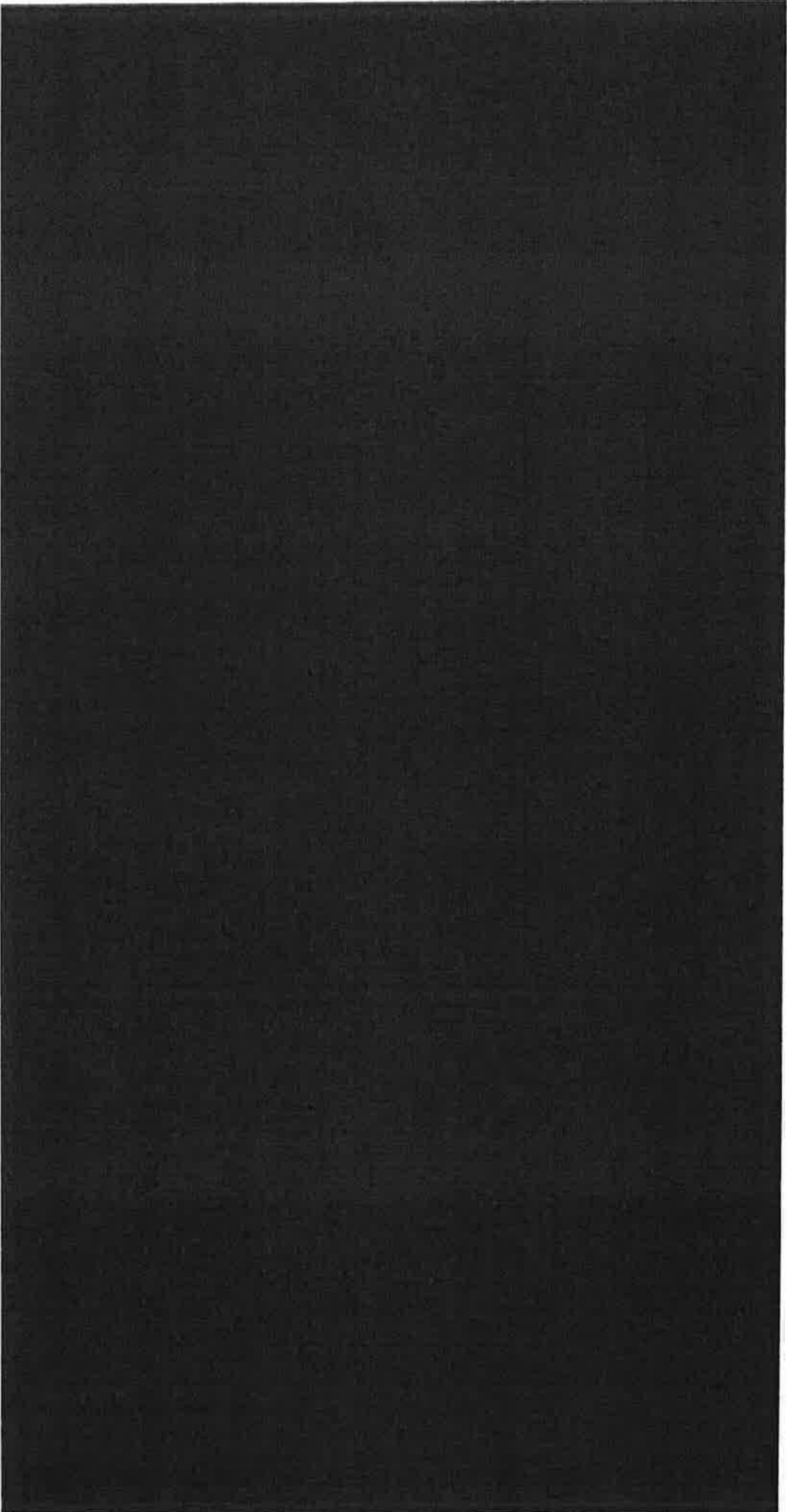
**Presence List of participants**



This project is funded  
by the European Union.



This project is funded  
by the European Union.



This project is funded  
by the European Union.

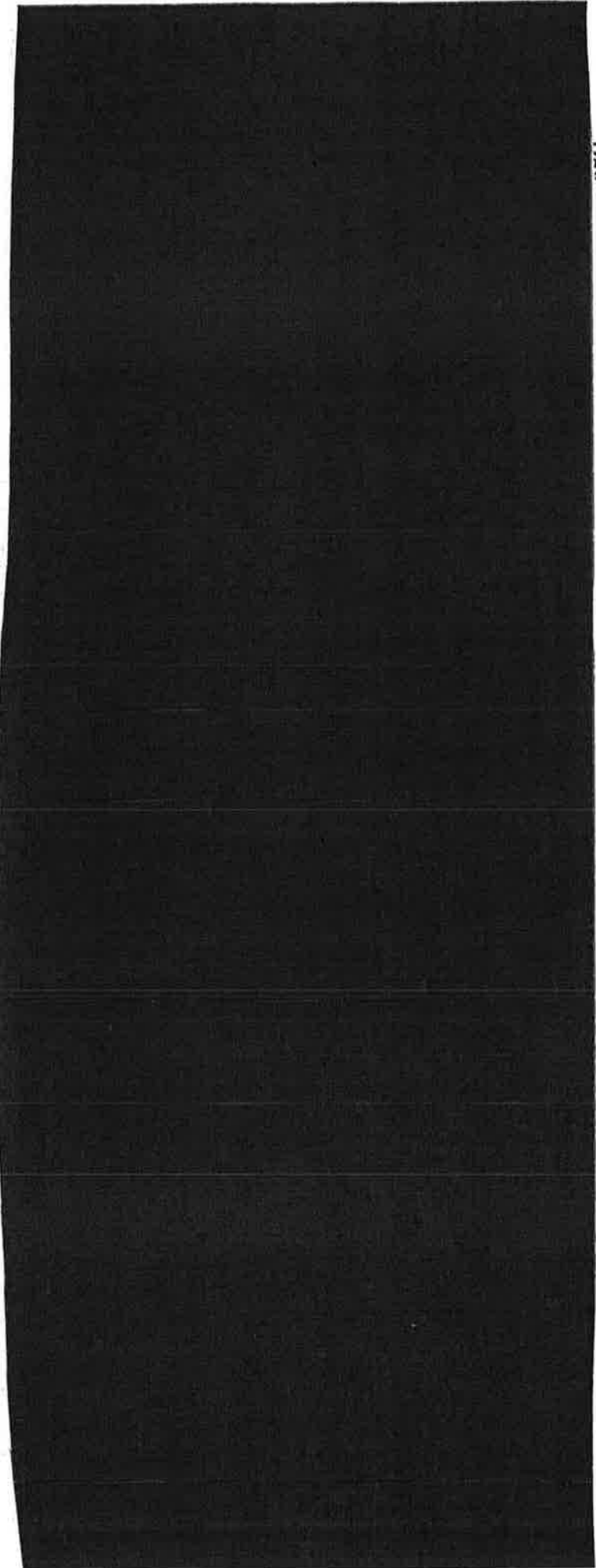


**Financial Investigation in relation to Drug Trafficking**

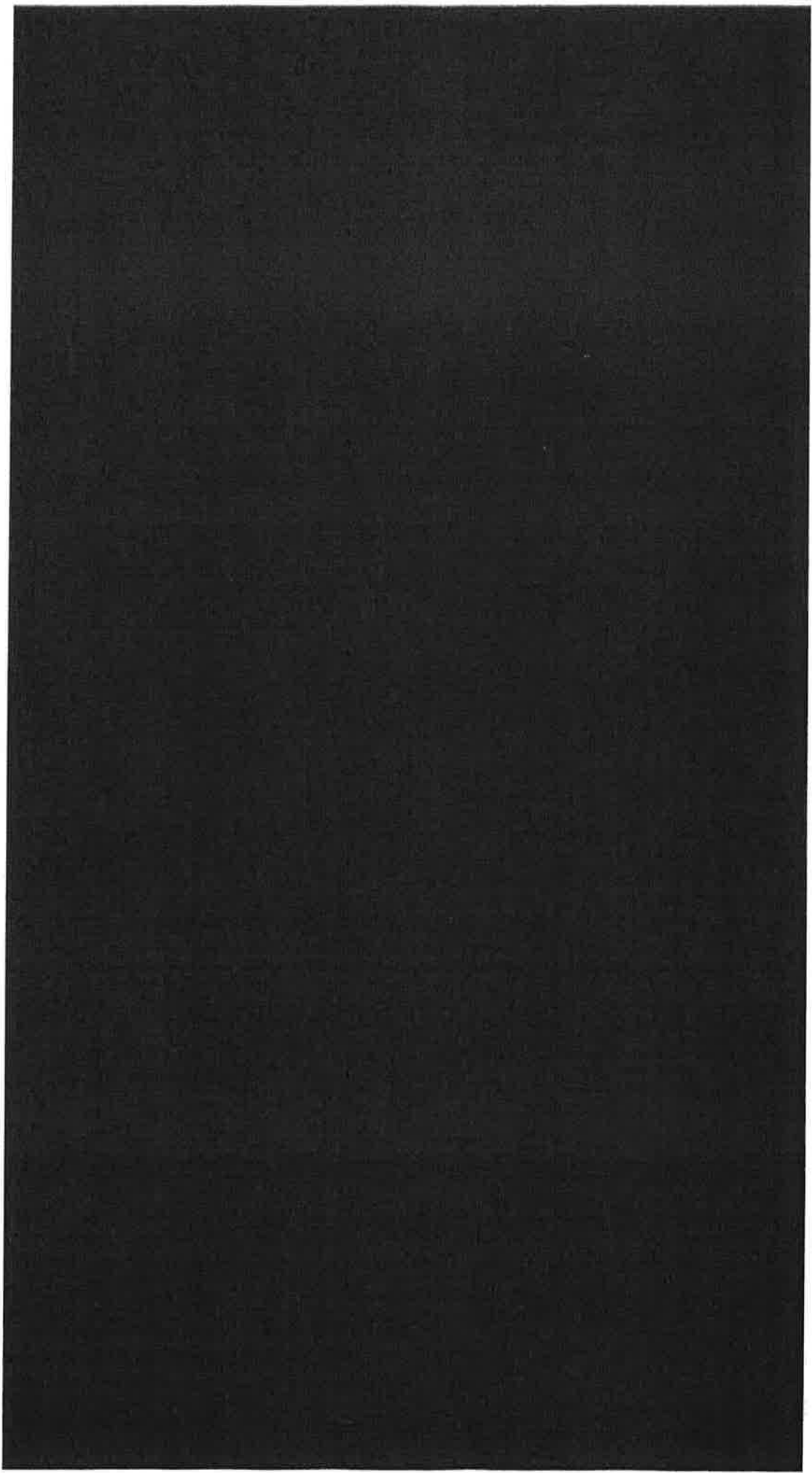
**08-12 October Prishtina Kosovo\***

**Presence List of participants**

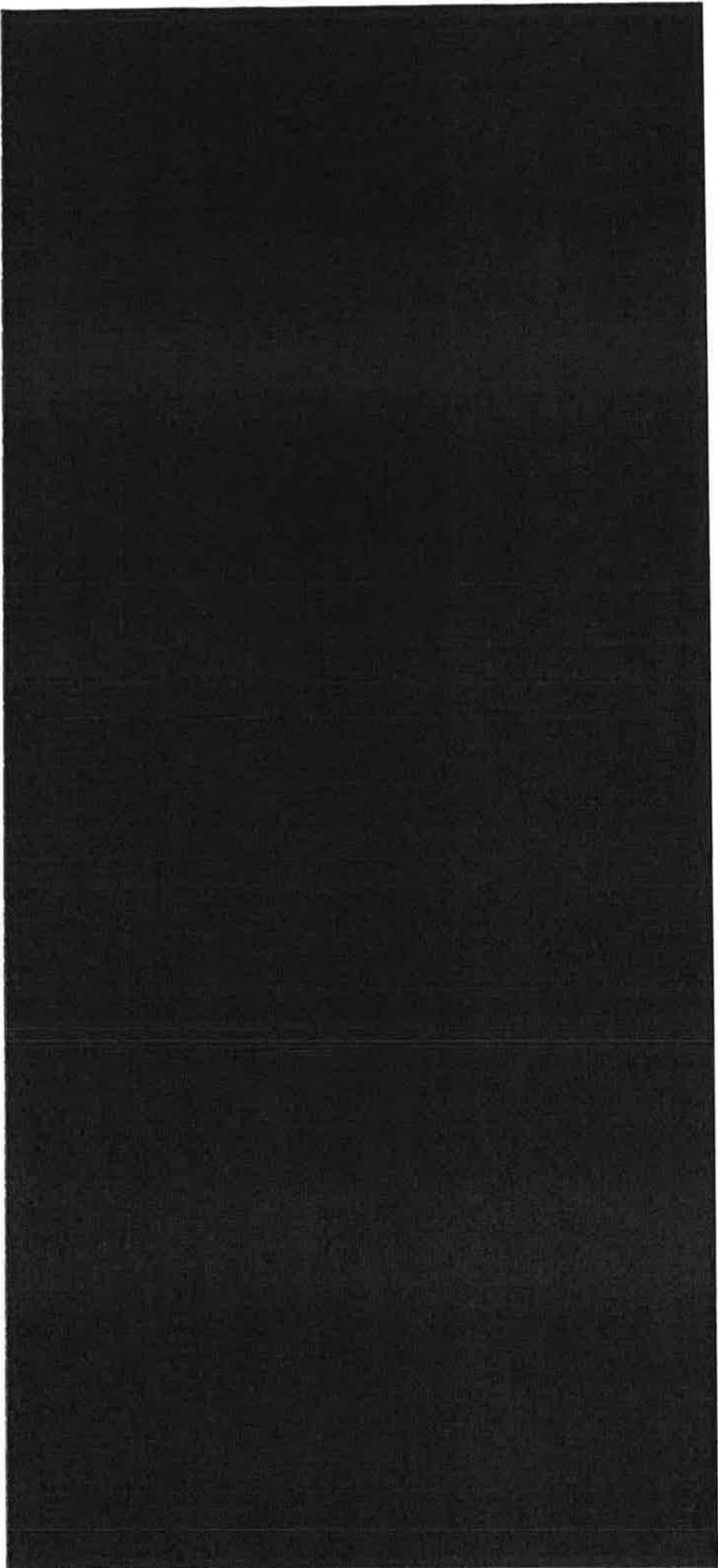
*Day. 03 Oct. 2018*



This project is funded  
by the European Union.



This project is funded  
by the European Union.



declaration of independence  
Provisional UN status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo



This project is funded  
by the European Union.





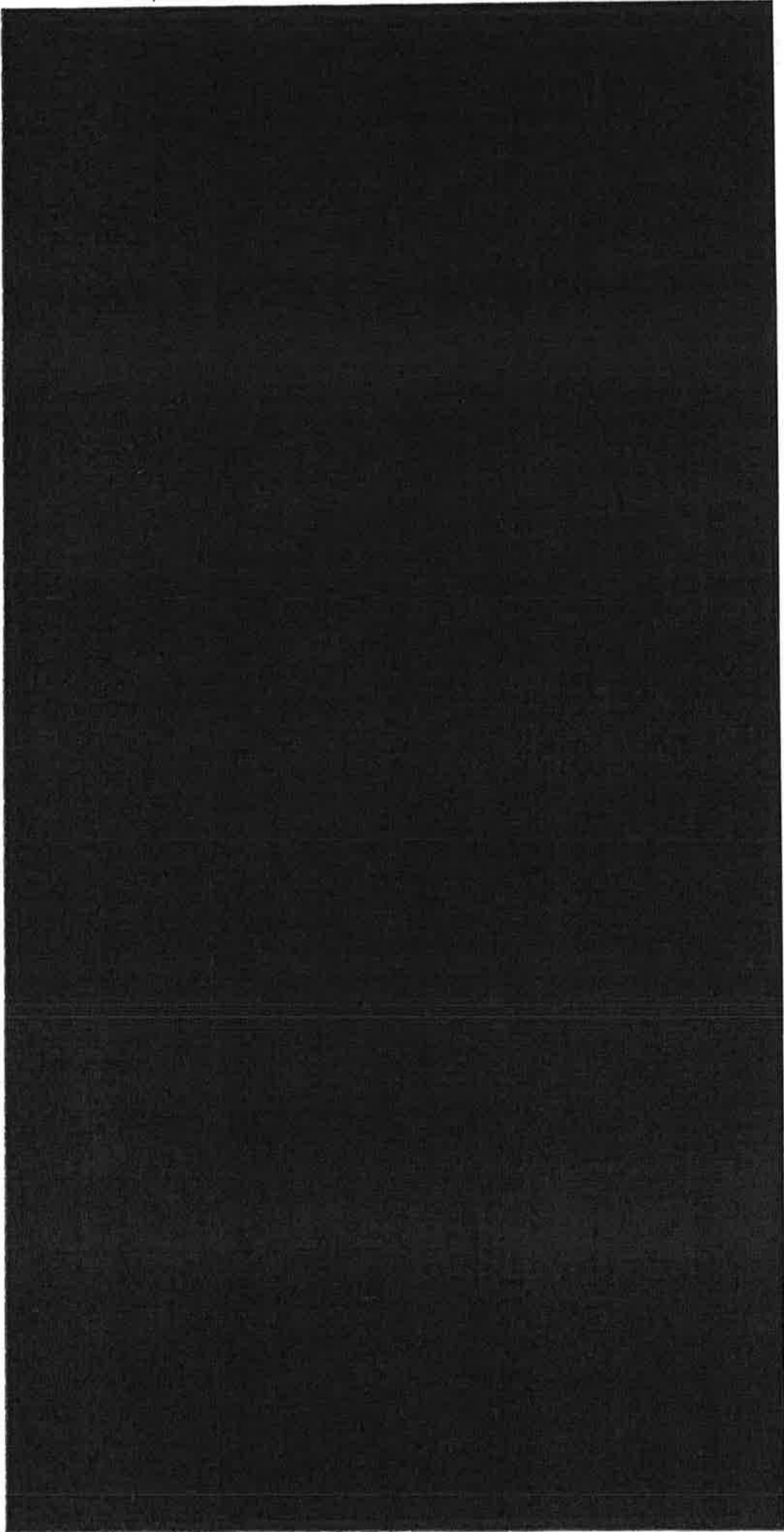
**Financial Investigation in relation to Drug Trafficking**

**08-12 October Prishtina Kosovo\***

**Presence List of participants**

**Day : 10 Oct. 2018**

by the European Union.



This project is funded  
by the European Union.

\*This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence



This project is funded  
by the European Union.

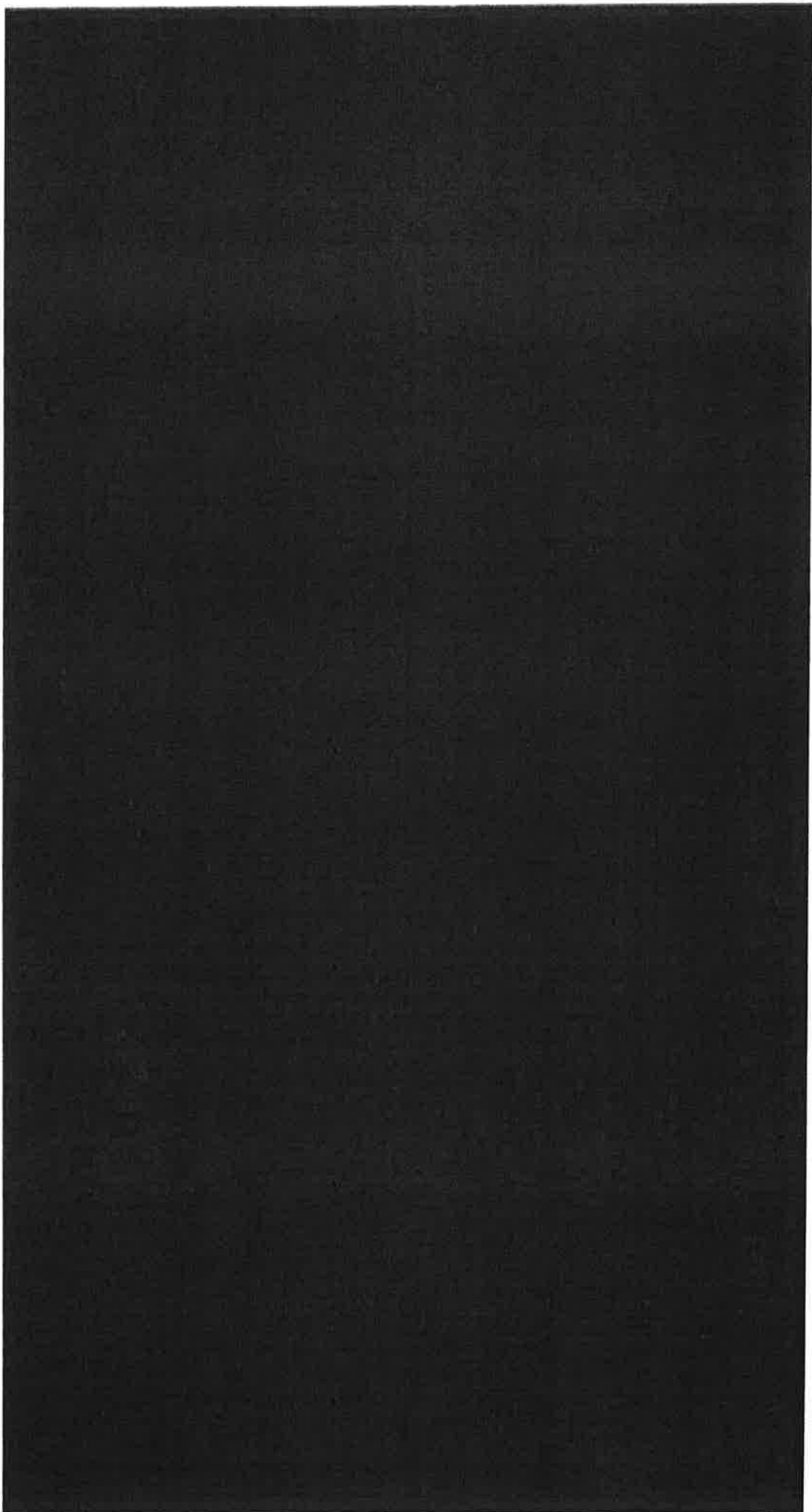


Financial Investigation in relation to Drug Trafficking

08-12 October Prishtina Kosovo\*

Presence List of participants

Day : 11 oct. 2018



This project is funded  
by the European Union.

\*This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence



This project is funded  
by the European Union.

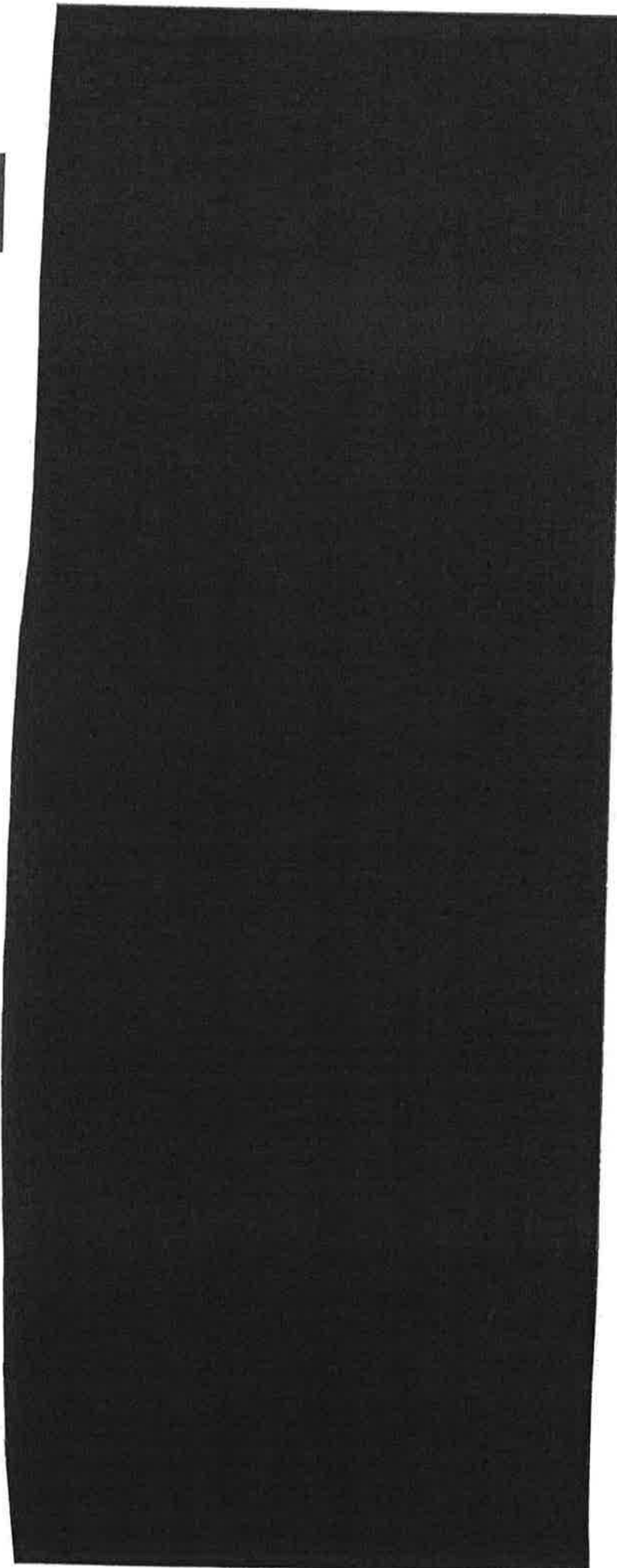


**Financial Investigation in relation to Drug Trafficking**

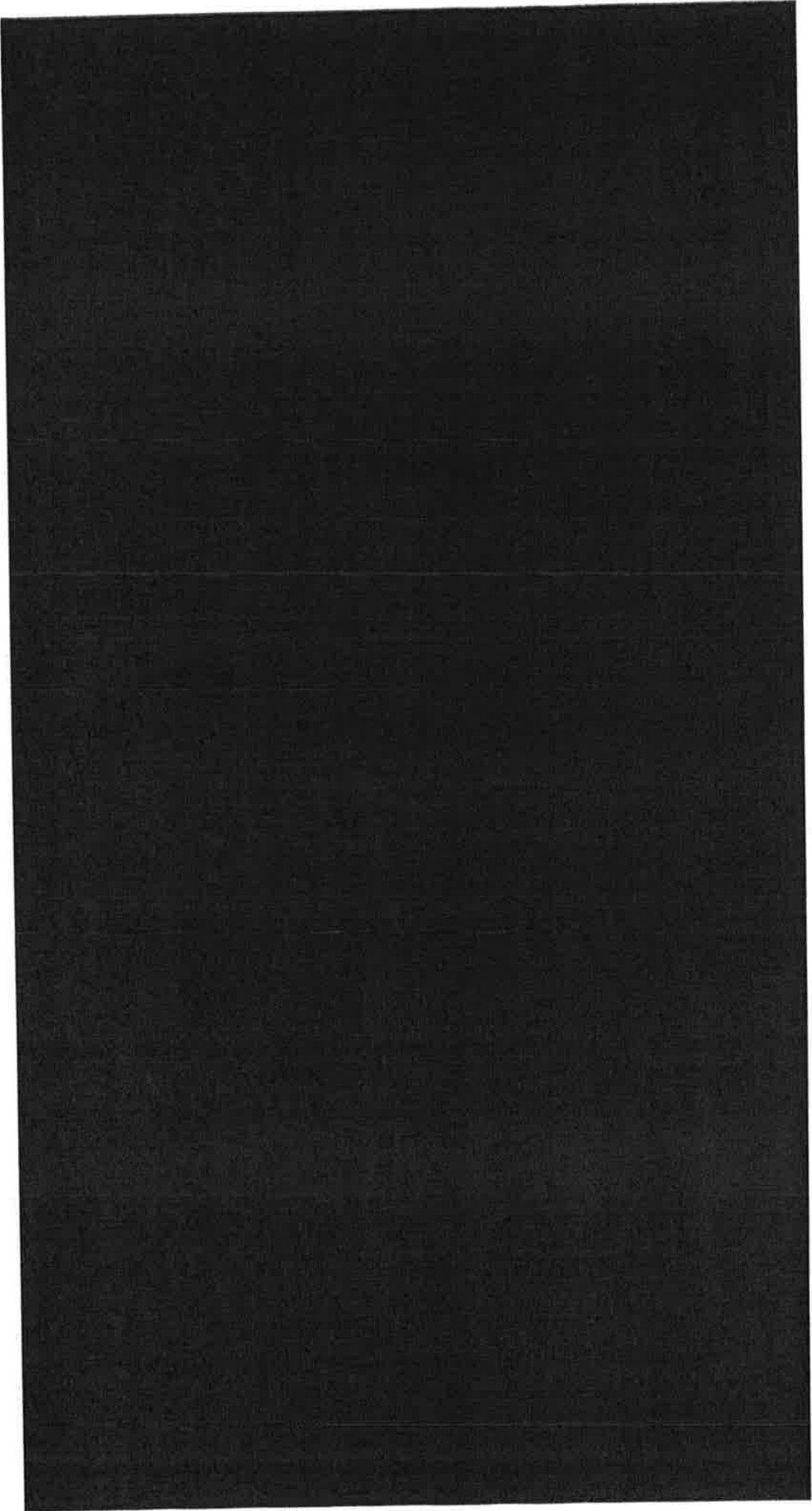
**08-12 October Prishtina Kosovo\***

**Presence List of participants**

12 OCT 2018



This project is funded  
by the European Union.



This project is funded  
by the European Union.



\*This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence



This project is funded  
by the European Union.





# Financial Investigation in relation to Drug Trafficking



8<sup>th</sup> to 12<sup>th</sup> October 2018

Prishtina, Kosovo



*'Albanian speaking organised crime in the EU and wider arena'*



1. Significance of the Kosovo War
2. Albanian speaking criminals in the EU
3. Albanian speaking organised crime
4. Cocaine market dominance



## Significance of the Kosovo War

Many of those who entered have since been identified as 'Albanian speakers', of Albanian origin.

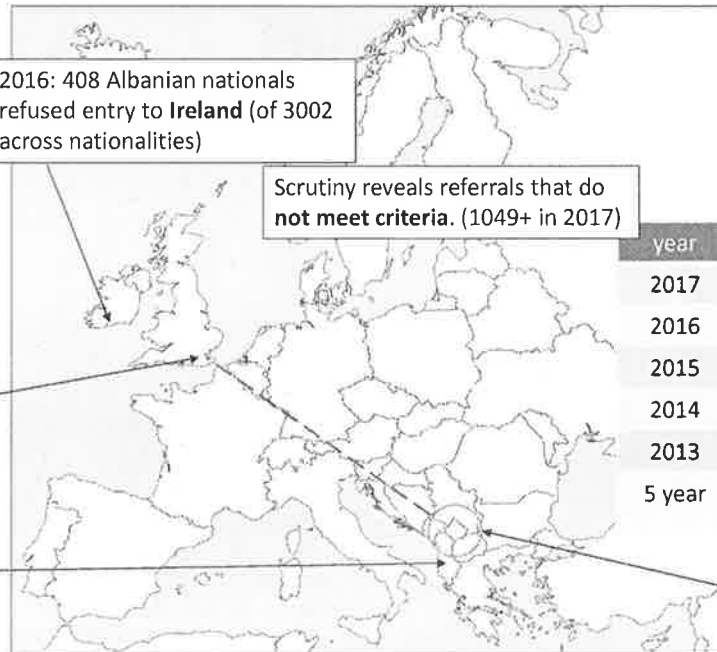
↑  
Leave to remain, followed by residence status was granted.

↑  
Entry into the UK as 'refugees fleeing conflict in Kosovo'.

↓  
No checks were made with the Albanian 'Civil Registry'.

2016: 408 Albanian nationals refused entry to **Ireland** (of 3002 across nationalities)

Scrutiny reveals referrals that do **not meet criteria**. (1049+ in 2017)



2009 UK introduces: **National Referral Mechanism**  
A framework for identifying victims of human trafficking and modern slavery, and ensuring they receive appropriate support.

year	total	Albania	Kosovo
2017	5145	777 (1)	4
2016	3804	699 (1)	4
2015	3261	600 (1)	2
2014	2339	449 (1)	3
2013	1745	268 (1)	0
5 year	16,294	2793 (17%)	13

1998 – 1999 significant migration, due to Kosovo War.

## Albanian Speaking organised criminals in the EU

3

Established and active presence of Albanian speaking organised crime.

Other organised crime nationalities involved with Albanian speaking OC. Transport / Logistics / Trafficking

Commonly claimed nationalities by Albanian speaking criminals.

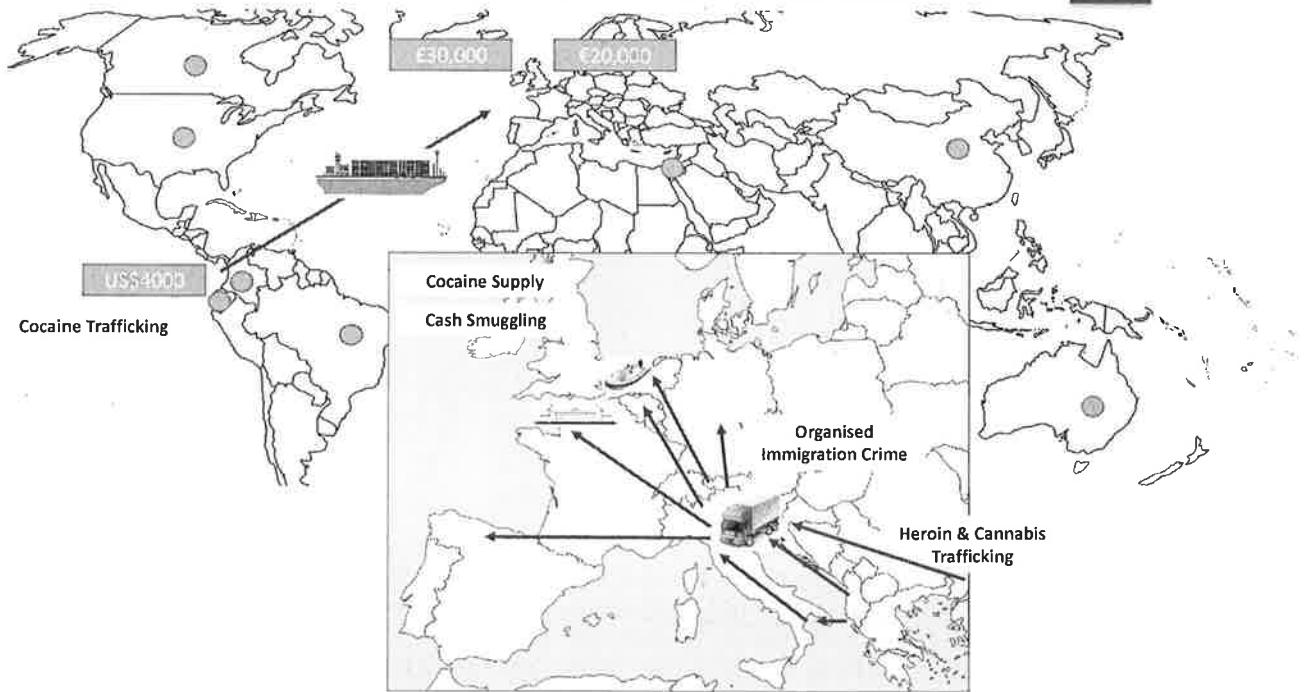


### Crime Types:

- Drug Trafficking
  - Cocaine
  - Heroin
  - Cannabis
- Human Trafficking & Organised Immigration Crime
- Modern Slavery & Sex Industry Exploitation
- Money Laundering & Cash Smuggling
- Firearms
- Violence
- Corruption & Border / Port Security Breaches

# Albanian Speaking Organised Crime

4



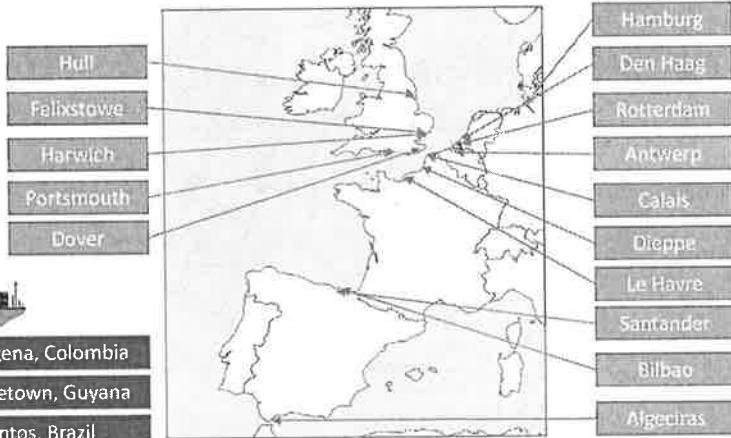


- Cartagena, Colombia
- Georgetown, Guyana
- Santos, Brazil
- Guayaquil, Ecuador
- Colon, Panama
- Caracas, Venezuela

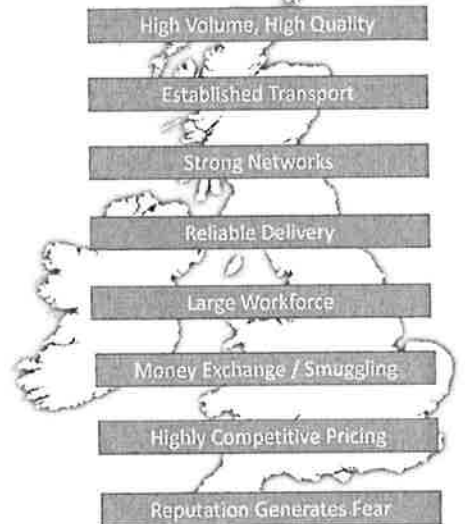
## Cocaine market dominance

1

### Significant Maritime Opportunity into Western Europe



### UK market control



### UK cocaine kilogram prices, since Albanian Speaking OC

2012	Albanian Speaking OC undercuts prices	2013	2014	2015	2016	2017	2018
£45,000		£40,000	£37,000	£35,000	£33,000	£30,000	£28,000





# Financial Investigation in relation to Drug Trafficking



8<sup>th</sup> to 12<sup>th</sup> October 2018

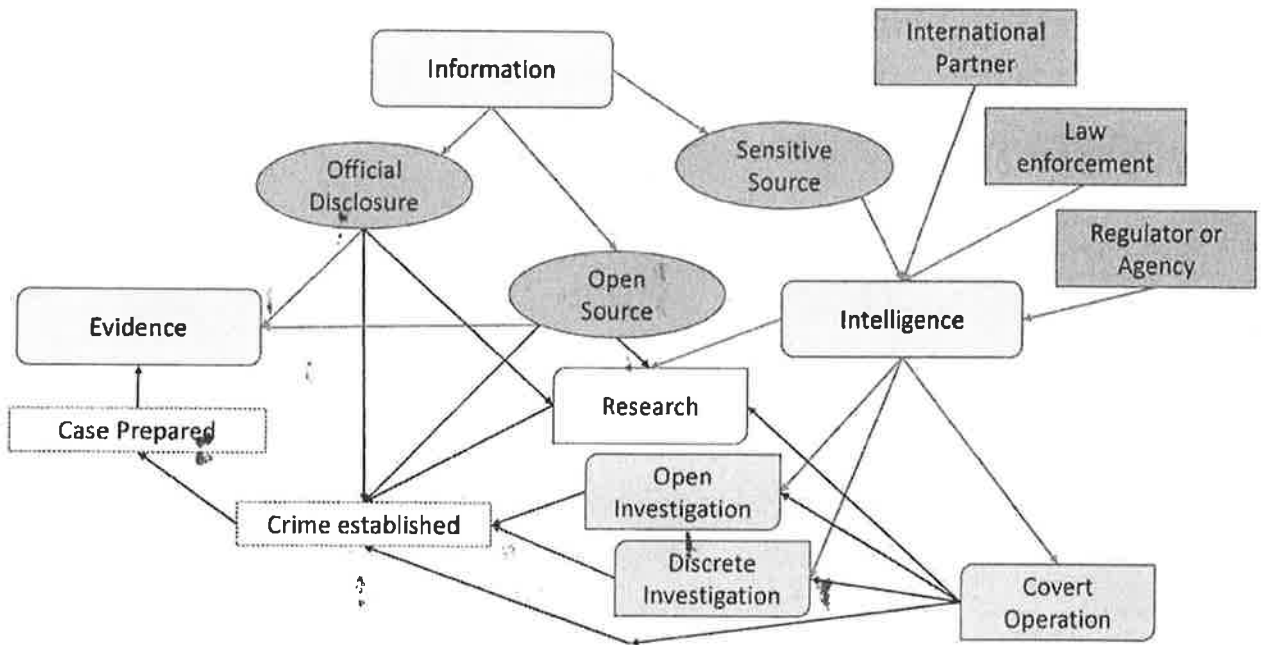
Prishtina, Kosovo



*'Intelligence led investigations'*

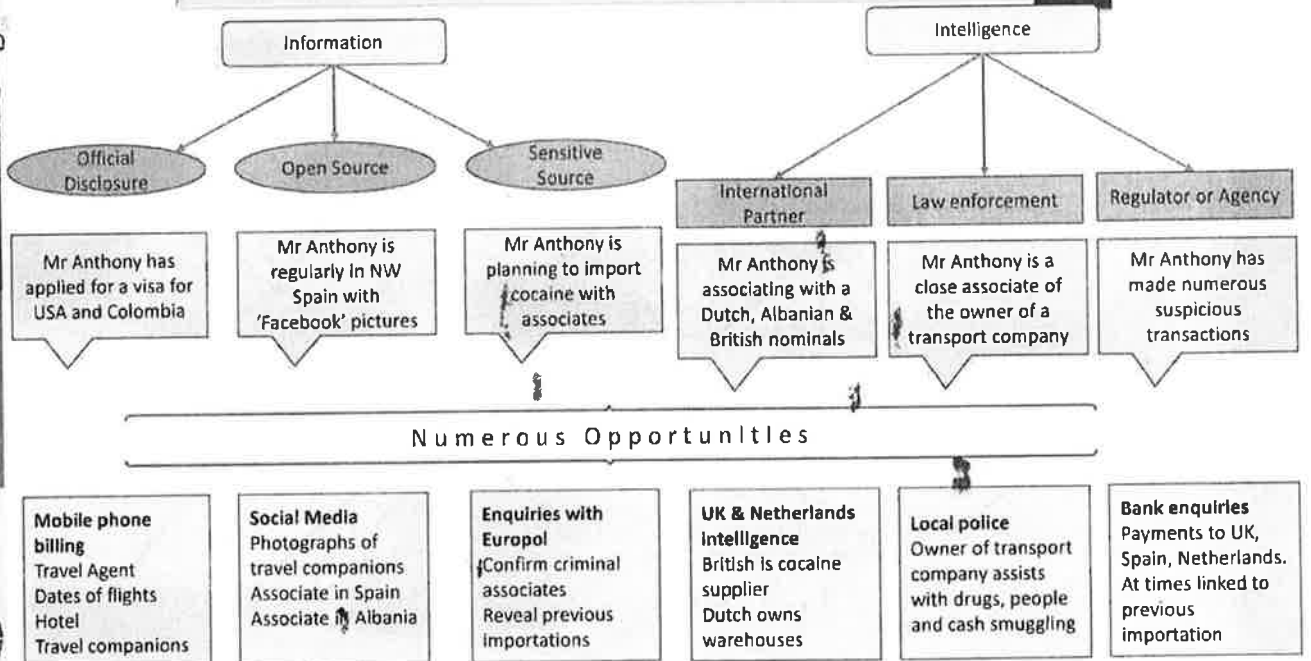


1. Information, Intelligence, Evidence...
2. Example of developing scenario
3. Discussion



### Example of developing scenario

3



**Mobile phone billing**  
Travel Agent  
Dates of flights  
Hotel  
Travel companions

**Social Media**  
Photographs of travel companions  
Associate in Spain  
Associate in Albania

**Enquiries with Europol**  
Confirm criminal associates  
Reveal previous importations

**UK & Netherlands intelligence**  
British is cocaine supplier  
Dutch owns warehouses

**Local police**  
Owner of transport company assists with drugs, people and cash smuggling

**Bank enquiries**  
Payments to UK, Spain, Netherlands.  
At times linked to previous importation

## Discussion

4



Question: Which intelligence sources are working well for you?

Question: Which intelligence sources could work better for you?

Contact

[REDACTED]



Threat, Risk & Harm  
Consultant

Strategic & Tactical  
Action Plan Design

Witness, Evidence &  
Investigation Courses

Drugs, Organised Crime &  
Safeguarding Advisor



# Financial Investigation in relation to Drug Trafficking



8<sup>th</sup> to 12<sup>th</sup> October 2018

Prishtina, Kosovo



*'From Money to Crime  
or vice versa with Drug Trafficking'*



content

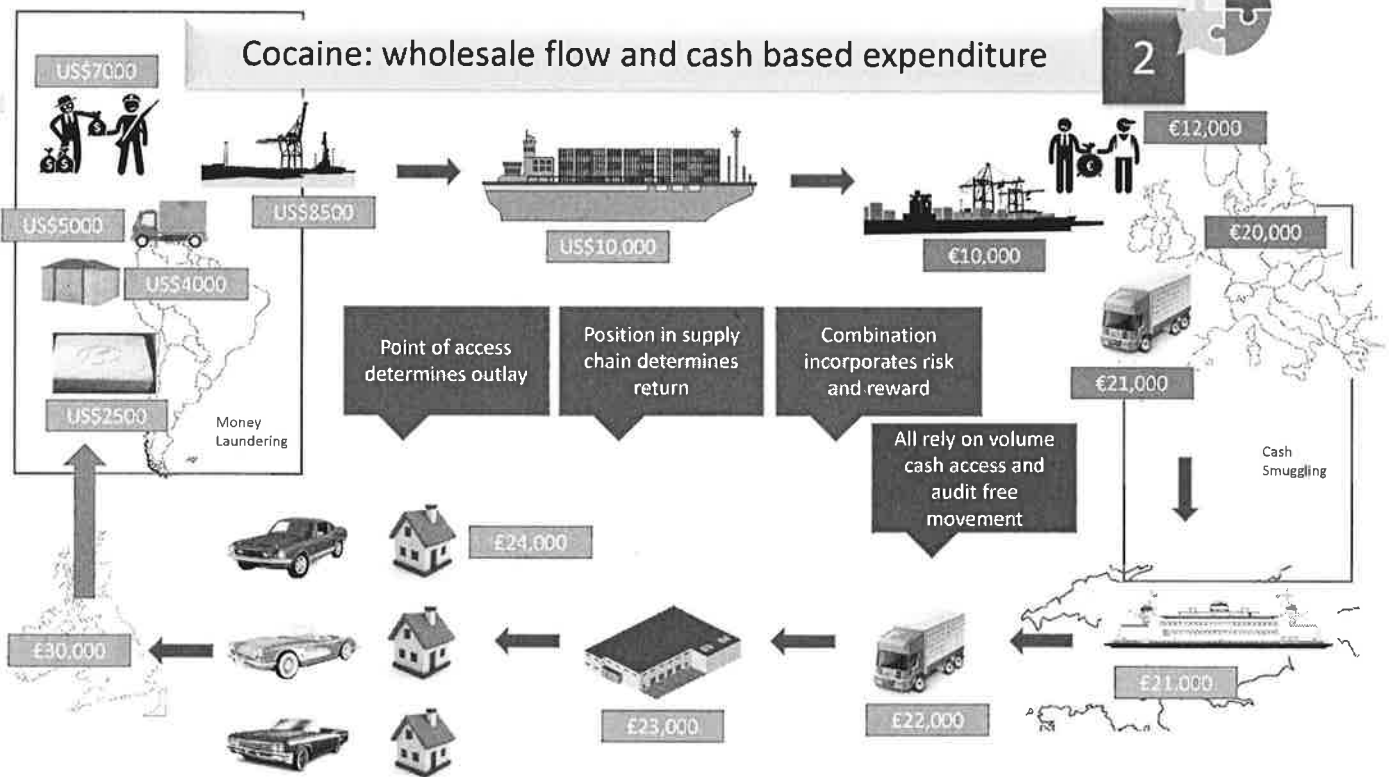
1

1. Cocaine: wholesale flow and cash based expenditure
2. Investment, overheads, diversification and reinvestment
3. Revenue and profit... UK example: 30 tons of cocaine



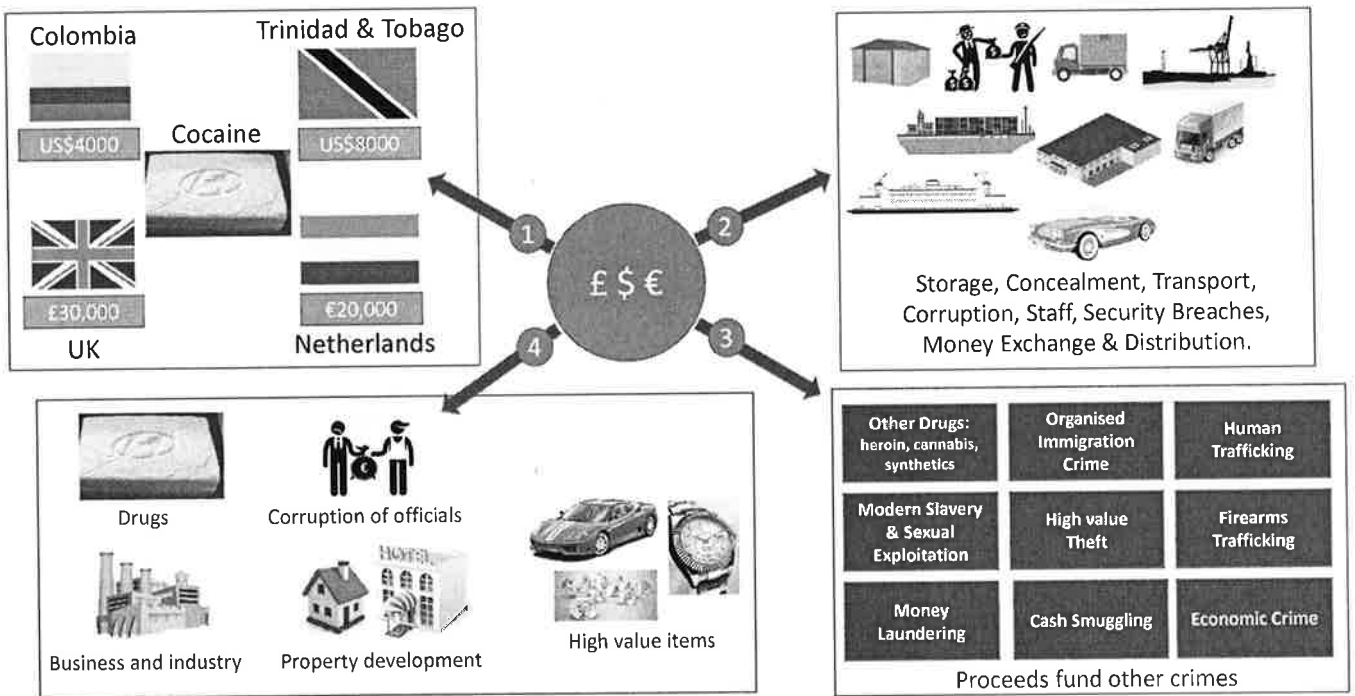
# Cocaine: wholesale flow and cash based expenditure

2



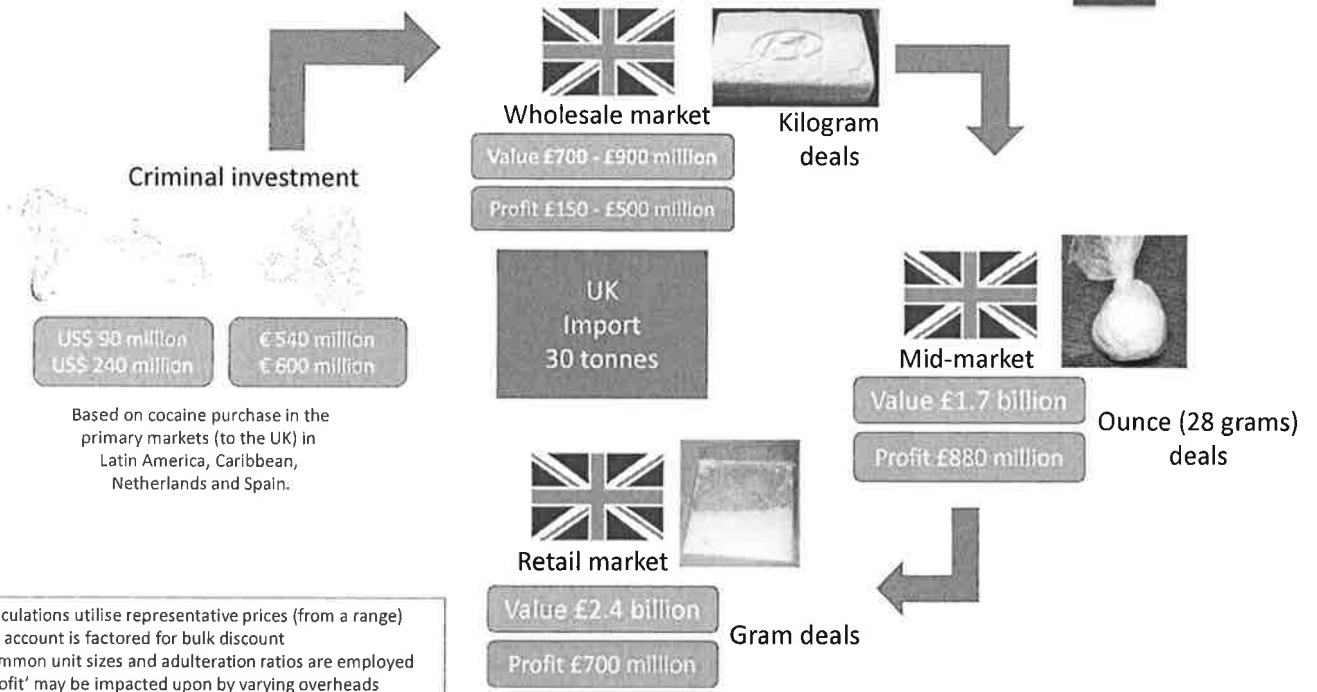
1 Investment 2 Overheads 3 Diversification 4 Reinvestment

3



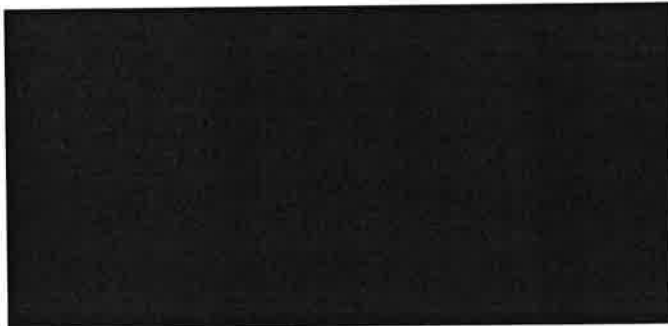
Revenue and profit... UK example: 30 tons of cocaine

4



Calculations utilise representative prices (from a range)  
 No account is factored for bulk discount  
 Common unit sizes and adulteration ratios are employed  
 'Profit' may be impacted upon by varying overheads

Contact



 Threat, Risk & Harm  
Consultant

Strategic & Tactical  
Action Plan Design

Witness, Evidence &  
Investigation Courses

Drugs, Organised Crime &  
Safeguarding Advisor



# Financial Investigation in relation to Drug Trafficking

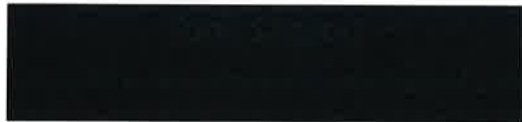


8<sup>th</sup> to 12<sup>th</sup> October 2018

Prishtina, Kosovo



*'Strategic Action Plans and National Drug Strategy example'*





1. Looking at the threat differently
2. Trafficking examples
3. Strategic Action planning
4. Single Vision
5. Tactical Response planning
6. Good practice for Strategic Action Plans



Looking at the Drugs Threat differently



Identify and Understand the Threat and Risks

Good quality intelligence and information

Relevant and focused analysis and research

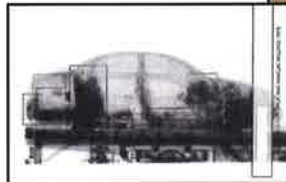
Accurate and unbiased reporting

Well informed and considered Strategy

Disrupt the Threat  
Mitigate the Risks  
Reduce the Harm

## Trafficking examples

3



This does not have to happen, it is a ruthless criminal choice to exploit other human beings





# Strategic Action Planning 4

**Risks**  
 Vulnerabilities  
 Exploitation  
 Opportunity  
**Harm**

Drivers  
**Enablers**  
 Logistics  
 Platforms

- Leadership
- Coordination
- Governance
- Communication

Strategic Action Plan

Threat

Single Vision

What do you want to achieve?

Strategic Objectives

International Trafficking

Importation  
(Ports and Borders)

National Distribution  
(organised crime)

Retail Supply  
(domestic crime)

Cross-cutting crime  
(links to other threats)

- International liaison
- Project participation
- Operational collaboration

- Multi-agency partnerships
- Combined policies
- Resource deconfliction



Single Vision: Example for Kosovo  5

“Through a well informed and coordinated response to the impact from the **Threat** of Drug Trafficking (and associated crimes) upon the security, integrity and well being of Kosovo; achieve mitigation of **Risks** and reduction in **Harm**”.

# Tactical Response Planning

## Strategic Objectives

### International Trafficking

- National criminal groups overseas
- Foreign criminal groups in country
- Transport and routes
- Origin and transit locations
- **Illicit funding and investment**
- Exploitation of legitimate trade and industry

### Importation

- Border & port security
- Corruption of officials & workers
- Aviation safety
- Maritime exploitation
- Concealment and cover loads
- Parcel and postal system
- **Import / export of illicit funds**

### National Distribution

- Organised Crime Groups
- Firearms and violent crime
- Domestic drug production
- Exploitation of illicit workforce
- Domestic networks and gangs
- **Cash aggregation & movement**

### Retail Supply

- Dangerous substances
- Internet / postal supply
- Domestic market dynamics
- 'Health' impact
- Public messaging & education
- Associated violence
- Young & vulnerable persons

### Cross-cutting crime

- **Money laundering**
- **Cash smuggling**
- High value theft
- Human Trafficking
- Modern Slavery
- Immigration crime
- Prison security and stability
- Corruption
- Cyber enabled supply
- **Economic Crime**

## Good Practice for Strategic Action Plans - CRAFT



- C** **Collaborative** Working with partners in country and internationally
- R** **Realistic** Establish objectives and deadlines that are achievable, not just aspirational
- A** **Adaptable** Be prepared to include new priorities and remove achieved objectives
- F** **Focused** Do not be distracted by an 'incident'. The strategy is a long term commitment
- T** **Transparent** Make actions clear, define outcomes to achieve, assign ownership and report performance, progress and barriers to success



Contact



Threat, Risk & Harm  
Consultant

Strategic & Tactical  
Action Plan Design

Witness, Evidence &  
Investigation Courses

Drugs, Organised Crime &  
Safeguarding Advisor



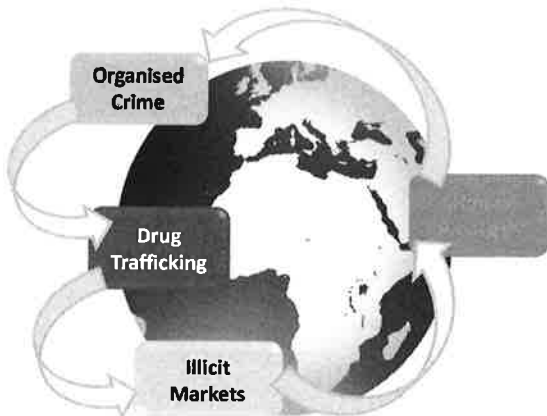


# Financial Investigation in relation to Drug Trafficking



8<sup>th</sup> to 12<sup>th</sup> October 2018

Prishtina, Kosovo



*'Drug markets on the Internet and Darknet'*



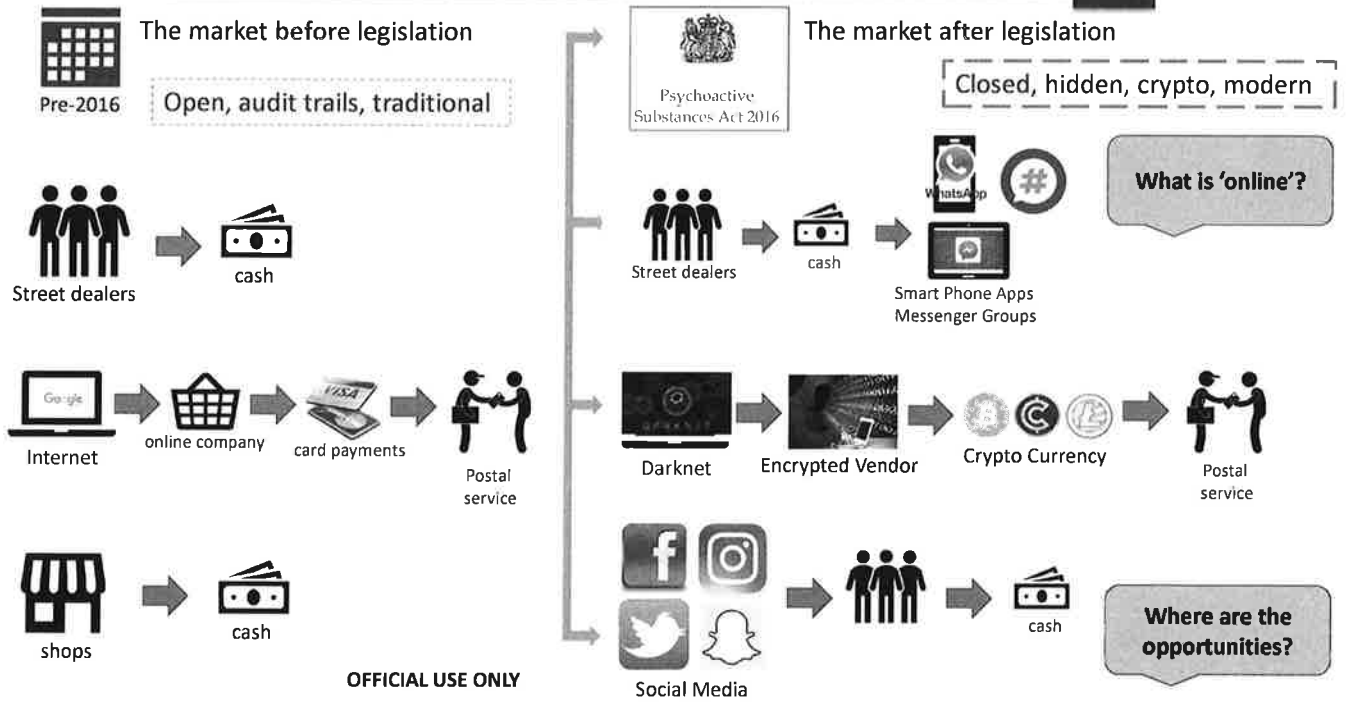


1. Disrupting and influencing the market
2. Importation, sale, distribution and purchase (UK example)
3. Substances of particular legal interest
4. High level vendors, markets and opportunities
5. Mechanisms for NPS and Internet sales control



# Disrupting & Influencing the Market

2



### Importation-Distribution-Sale-Purchase (UK)



OFFICIAL USE ONLY

Three substances of particular legal interest

4

**Mephedrone**



Already covered by the Misuse of Drugs Act 1971, together with other substances such as NBOM (an LSD type drug).

**Synthetic Cannabinoids**



Transferred to the Misuse of Drugs Act 1971, from the Psychoactive Substance Act 2016 – in 2017 (deemed too harmful not to be enhanced to higher legislation).

**Nitrous Oxide**



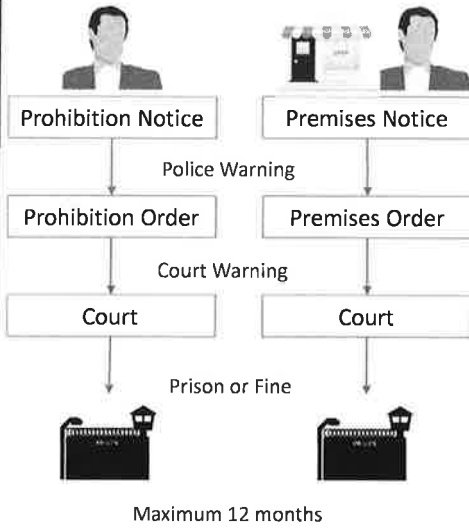
Legal challenge that Nitrous Oxide is a 'medicine' and exempt under the Psychoactive Substance Act 2016. Medicine if used as medicine, not abused.

OFFICIAL USE ONLY

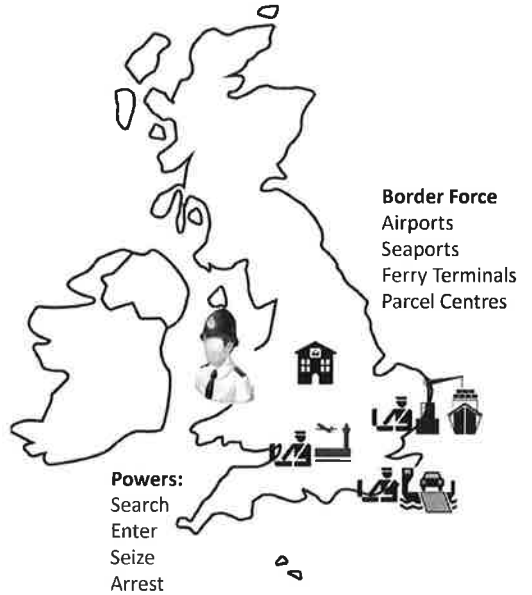
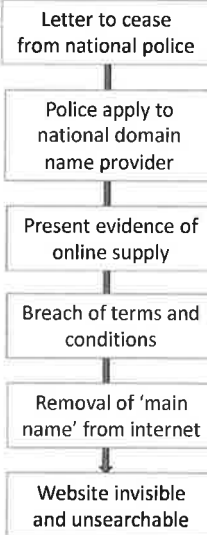


## Mechanisms for Control of NPS

6



Internet Trader



OFFICIAL USE ONLY

Contact



Threat, Risk & Harm  
Consultant

Witness, Evidence &  
Investigation Courses

Drugs, Organised Crime &  
Safeguarding Advisor



# Preliminary investigations and Prosecutor led Investigations

**CEPOL Western Balkan Financial Investigation In-  
Service Training**

**'Financial Investigations in relation to Drug Trafficking'**

**08-12 October 2018 in Prishtina, KOSOVO**

# Preliminary investigation



Once a crime has come to the attention of the police, a preliminary investigation is initiated;



The object is to find out who can be suspected of the crime and whether or not there is sufficient evidence to initiate an action;



The prosecutor leads the preliminary investigation from the point when a certain individual can be reasonably suspected of having committed the offence;



the police conduct the preliminary investigations from beginning to end.



As the person in charge of leading the investigation, the prosecutor is responsible for ensuring that the crime is investigated in the best way possible. The investigations are conducted by the police on the instructions of the prosecutor.

The prosecutor follows the investigations on a continuous basis and constantly determines which investigation measures and decisions are necessary. If the investigation concerns a serious and complicated crime, the prosecutor will often take part directly in the investigation in connection, for instance, with reconstructions of the crime or with important interrogations.

## Italian criminal procedure: generalities



Criminal procedure begins when a crime (in Italian "notizia di reato" = police report) is reported to the Public Prosecutor's office by the Judicial Police (Polizia Giudiziaria) or by any other means (citizens, press);



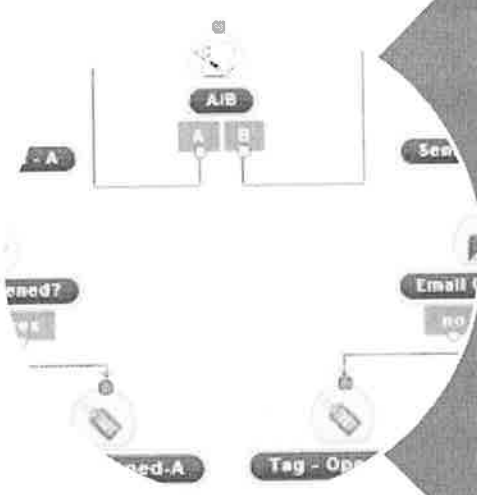
During the preliminaries investigations phase the Judicial Police and the Public Prosecutor carry out a detailed enquiry into the alleged crime. This phase ends with the request for filing in the archives or the initiation of penal action (art. 405 c.p.p.).

In this second case, a trial starts against a person alleged to have committed the crime. If the accused doesn't choose any special proceeding, he comes to Court to face the charges ( by the means of cross examination) or, if he prefers, he can remain in silence or choose not making any appearance in Court .In this case he is represented by his lawyer.The trial ends with the conviction or the acquittal of accused, depending on whether he is found guilty or not. Against the decision both the Public Prosecutor and the accused can bring an appeal to continue on enforcing their reasons.

## The preliminary investigations phase



Once the Public Prosecutor's office has received a crime report, he is obliged to start the preliminary investigations and he has got a maximum of six months to a year (depending on the nature of the crime) to carry out a systematic examination of the person who may have committed the crime and the questioning of witnesses.



The preliminary investigations may involve inspections, searches, seizures, monitoring of conversations or communications, securing sources of proofs, identifications of accused, summary report on person against whom investigation is conducted, other summary information from persons who can report circumstances useful for the purpose of the investigation and other similar procedures.

The enquiry is private and cannot be disclosed. The duration of preliminary investigations is dependent upon their complexity, so that the term for completing the investigations may vary between six to eighteen months and, in very complex cases, 2 years.

Only the Judge can grant requests to extend the term. Postponements and delays are very frequent. During this time the suspect can be held in custody in prison, or partially lose his personal freedom, if there are serious indications against him (art 272 c.p.p.) and at least one of the three precautionary requirements provided in art 274 c.p.p.



## Possible outcomes, after the investigation is completed

the Public Prosecutor can determine that there is not enough evidence to support the charge and for this reason, ask the Judge in charge for this stage (in Italian: “Giudice per le Indagini Preliminari”) to dismiss the case by a request for filing in the archives.

## Possible outcomes, after the investigation is completed #2

if the Public Prosecutor determines that there is sufficient evidence, he must notify the suspect and the defense counsel that the investigation is closed. At this point, within twenty days, the suspect may ask either to be questioned and/or to give evidence in his own defence. If this term expires or if he doesn't manage to demonstrate his innocence, the Public Prosecutor can ask the Judge to send the case to trial (proceeding with preliminary hearing) or he himself can send the case directly to trial (art. 33 e art. 550 c.p.p), that is without the necessity of a preliminary hearing, if the crime is considered by law less serious.

## End of preliminary investigations and preliminary hearing

According to the art. 415 bis c.p.p., the Public Prosecutor, before concluding the preliminary investigations, must notify to the person alleged to have committed a crime and also his lawyer, a notice which contains a statement of the alleged criminal act, the information that the documents are filed in the Public Prosecutor's secretary and an option to the same suspect to exercise, if he likes - within twenty days - some of his rights: asking to be interviewed, submitting statements and documents, asking the Public Prosecutor for further inquiries.

## End of preliminary investigations and preliminary hearing

the Public Prosecutor exercises the penal action, drafting the charges (art. 405 c.p.p.), that is through:

- decree of summons for trial (art. 33-550 c.p.p.) which introduces to a trial without a preliminary hearing;
- activation of a special proceeding (art. 438 and following) as an alternative to a traditional trial;
- request for trial, followed - in a short time - by a preliminary hearing.

# Investigative techniques

- Observation;
- Wire tapping;
- E-mail tracing;
- Financial analysis;
- Perquisition;
- Forensic analysis on e-devices;



Role of International cooperation  
Europol and Eurojust as key actors in the fight against crime



# Eurojust



Eurojust's mission is to "support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States or requiring a prosecution on common bases" (Art. 85 (1) TFEU). Eurojust is a 'facilitator' of judicial cooperation, which intervenes to smoothen the effective functioning of judicial cooperation instruments (such as the European Arrest Warrant), to resolve legal issues arising in complex cases (such as ne bis in idem issues or conflicts of jurisdiction) and/or to stimulate the coordination of judicial authorities.

# Europol

 **EUROPOL**

Europol's mission is to "support and strengthen action by the Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy" (Art. 88 (1) TFEU). Europol was set up to gather police and law enforcement information from national authorities and to provide strategic and/or operational analyses on the basis of this information. It has been compared to a 'mega-search engine'.<sup>7</sup> It also coordinates law enforcement authorities' actions, and may support operational activities with its mobile office, analysis in real-time of information gathered on actions days, forensic tools, etc.



## The Future: the European Prosecutor Public Office



On 8 June 2017, 20 EU Member States reached a political agreement on the establishment of a new European Public Prosecutor's Office (EPPO) under enhanced cooperation.

# EPPO

On 1 August 2018, the Commission confirmed the Netherlands as the 21st EU Member State in the enhanced cooperation on the establishment of the EPPO;

On 7 August 2018, the Commission confirmed Malta as the 22nd EU Member State in the enhanced cooperation on the establishment of the EPPO

## EPPO

Following a build-up phase of three years, the EPPO is envisaged to take up its functions by the end of 2020.

## EPPO

The EPPO will be an independent and decentralised prosecution office of the European Union, with the competence to investigate, prosecute and bring to judgment crimes against the EU budget, such as fraud, corruption or serious cross-border VAT fraud.

## EPPO

Currently, only national authorities can investigate and prosecute fraud against the EU budget. But their powers stop at national borders. Existing EU-bodies such as Eurojust, Europol and the EU's anti-fraud office (OLAF) lack the necessary powers to carry out criminal investigations and prosecutions.

# EPPO



The EPPO will operate as a single office across all participating Member States and will combine European and national law-enforcement efforts in a unified, seamless and efficient approach.

## EPPO

The EPPO will be built on two levels: the central and the national level.

## EPPO

The central level will consist of the European Chief Prosecutor, its two Deputies, 21 European Prosecutors (one per participating Member State), two of whom as Deputies for the European Chief Prosecutor and the Administrative Director.



## EPPO

The decentralised level will consist of European Delegated Prosecutors who will be located in the participating Member States.

## EPPO

The central level will supervise the investigations and prosecutions carried out at the national level. As a rule, it will be the European Delegated Prosecutors who will carry out the investigation and prosecution in their Member State.

## EPPO

The rights of the suspects and accused persons will be guaranteed by comprehensive procedural safeguards based on existing EU and national law. The EPPO will ensure that its activities respect the rights guaranteed by the Charter of fundamental rights of the EU, including the right to fair trial and the right to defence.

# EPPO

The procedural acts of the EPPO will be subject to judicial review by the national courts. The European Court of Justice – by way of preliminary rulings – has residual powers to ensure a consistent application of EU law.


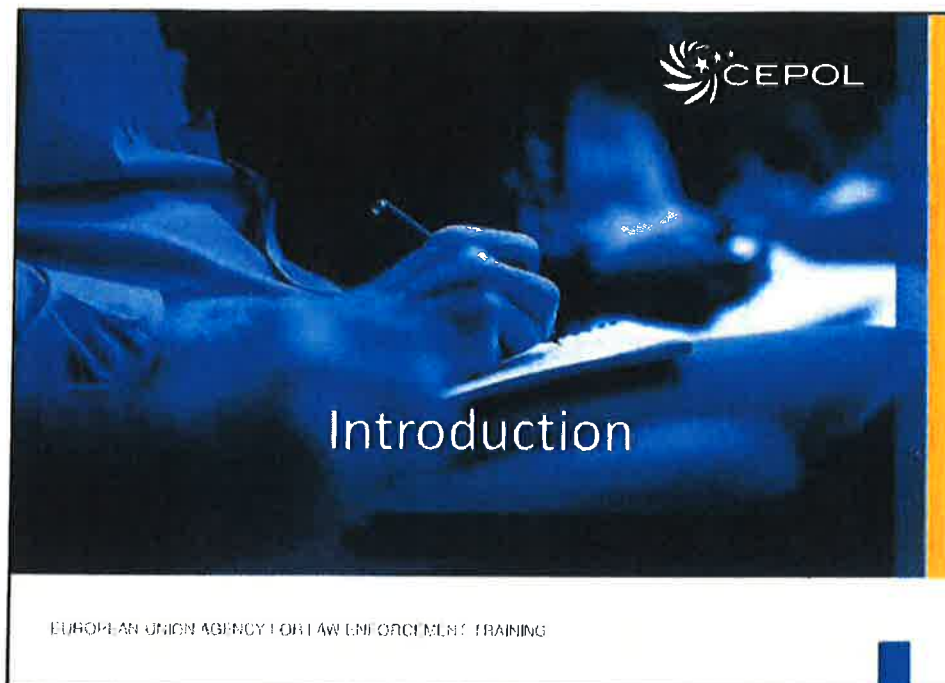
The EPPO will be the key actor to fight crimes against the EU budget, which is EU taxpayers' money.



**Thank you for your attention**








## OSINT Definition

### INTElligence

○ the collection and subsequent analysis of data from which to derive useful information to the process decision-making (military / civil / corporate), as well as the prevention of activities destabilizers of any nature





## Intelligence

- Intelligence is the tool that the state has it serves to collect, guard and disseminate to interested parties, be they public or private, information relevant to protection of the security of institutions, citizens and companies.
- Intelligence therefore plays a role fundamental and indispensable for which yes serves of professionalism from environments different that act according to peculiar procedures aimed at safeguarding the confidentiality of operators and their activities

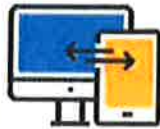


## OSINT

- *Open Source Intelligence*
- *Information gathering activities by consulting sources of public access*
  - Means of communication: newspapers, magazines, television, radio, institutional websites
  - Web & Social Media: Twitter, Facebook, Google+, Instagram, Pastebin, Forum, Blog, Chat Room, Web Archive ...
  - Open Data: government reports, financial plans, demographic data, legislative debates, press conferences, speeches, notices aeronautics, disease spread.
  - Direct observations: photographs of amateur pilots, listening to radio conversations and observation of photographs satellite.
  - Professionals and scholars: conferences, university lectures, professional associations and scientific publications
  - DeepWeb







## OSINT

- *GOAL and amplitude (in objectives and form) data sources + vastness (in quantity) of results = multi-disciplinarity*
  - Big Data (MapReduce / NoSQL / Horizontal Scaling / ...)
  - Semantic analysis engines
  - Data Mining
  - Scraping, Scripting, Networking



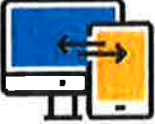
## Data-Information

- *Data = Knowledge not useful because incomplete or "raw"*
- *Information = Useful knowledge*
- *The three fundamental problems of computer science are:*
  - processing (transformation of data into information)
  - memorization (transfer over time)
  - communication (transfer to space).



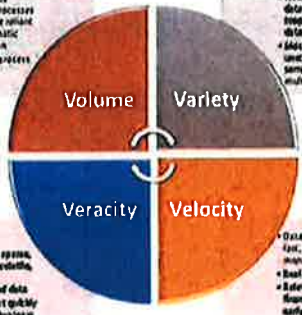
## Big Data

### Challenges With Big Data



- Data volume is growing so processes must be more reliant on programmatic administration
- Less people/process dependence

- Wider breadth of devices and sources in scope requires larger data capabilities
- Most of world's data is unstructured, semi-structured or multi-structured

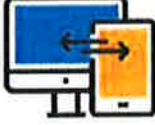


- Dealing with sparse, incomplete, volatile, and highly-manufactured data
- Able to adapt quickly to changing business

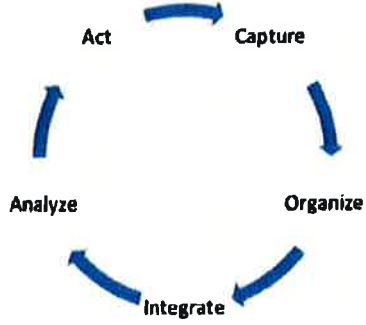
- Data is coming in so fast, how do we manage it?
- Real-time analytics
- Reference analytics, specialized servers, early warning signals

**CEPOL**

## Big-data functional requirements



Analytical process aimed at exploring the data in search of coherent schemes in order to establish a mathematical model that allows to predict phenomena of interest or to evaluate one been in place

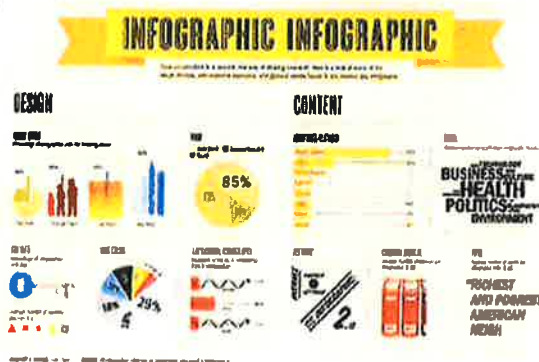


**CEPOL**



## Big data mining

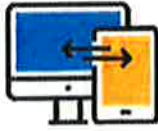
- Set of techniques and methodologies having as a goal the extraction of a knowledge or knowledge starting from large amounts of data (through automatic or semi-automatic methods) and scientific, industrial or operational use of this



## OSINT and REPUTATION

- The two disciplines are often confused, there are common points, but:
  - Different goals
    - The sources in the OSINT are very wider and heterogeneous
    - Many tools are in common, but in the OSINT techniques they are used more "flexible" techniques





## OSINT in place

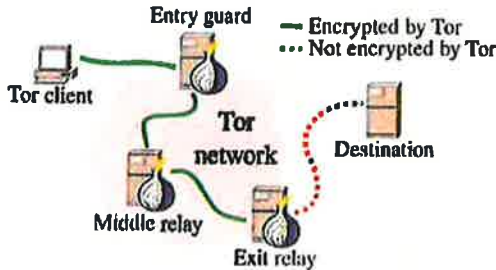
- *Dedicated servers*
- *H24 monitoring*
- *Continuous cataloging of targets*
- *Continuous study of variation of the targets*
- *Extrapolation and memorization some data*
- *Organization and analysis of data (automatic and human)*
- *Timely reaction to events (automatic and human)*




## OSINT



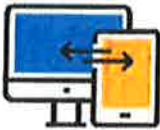
## Tor




- The onion routing
- <http://thehiddenwiki.org/>
- <http://kpvz7ki2v5agwt35.onion>

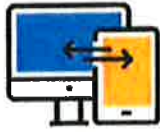


## Data extraction techniques



- Official Web APIs
- advantages
  - Ease
  - Rich documentation
- disadvantages
  - Structural limits





## Data extraction techniques

- *Web Scraping*
- *advantages*
  - no limitation
  - immediate results
  - extensive customization
  - sufficient costs (free tools)
- *disadvantages*
  - greater difficulty
  - less documentation

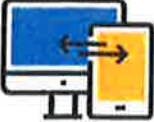
- Firebug
  - HTML, CSS, XPath
- Selenium / WebDriver (PhantomJS)
  - Greasemonkey
- Javascript + JQuery (PyQuery)
  - Python, Ruby, Perl



## Captchas


- *Turing test? Vicarious passed*
- <http://www.debasish.in/2014/04/attacking-audio-recaptcha-using-googles.html>






## Tools

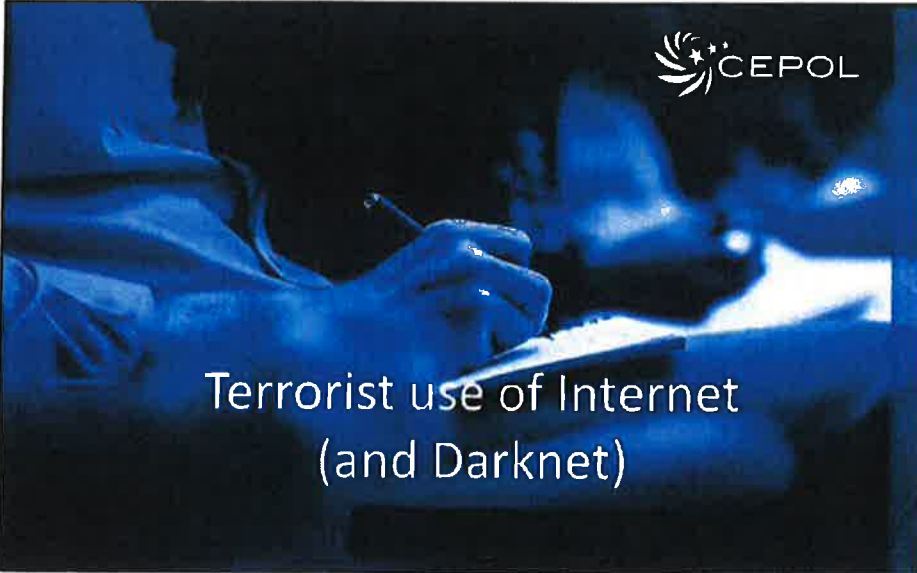
- OPEN SOURCE INTELLIGENCE TOOLS AND RESOURCES HANDBOOK




[https://www.i-intelligence.eu/wp-content/uploads/2018/06/OSINT\\_Handbook\\_June-2018\\_Final.pdf](https://www.i-intelligence.eu/wp-content/uploads/2018/06/OSINT_Handbook_June-2018_Final.pdf)



15





## Terrorist use of Internet (and Darknet)

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

16



## Research findings (2017)

- A small minority of individuals (9%) sought to recruit others online.
- Although a third of the sample prepared for some aspect of their attacks online, 9% specifically chose their target after conducting some online research.
- The analysis undertaken by police on one Jihadist-inspired plot showed that the plotters had used the Internet to research the English Defence League (EDL), their activists, and the locations of its leader for up to a month prior to the day of their planned bombing attack.


<http://onlinelibrary.wiley.com/doi/10.1111/1745-9133.12249/epdf>



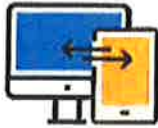
## radicalization

1. The Internet affords more prospects for radicalisation. For all 15 cases, the Internet was a "key source of information, communication and of propaganda for their extremist beliefs".
2. The Internet provides a "greater opportunity than offline interactions to confirm existing beliefs".
3. The Internet does not necessarily accelerate the process of radicalisation.
4. The Internet is "not a substitute for in-person meetings but, rather, complements in-person communication".
5. The Internet does not necessarily increase the opportunities for self-radicalisation; interactions, be they physical or virtual, are still crucial for radicalisation.



[www.rand.org/content/dam/rand/pubs/research\\_report/RRAC/RRAC111R](http://www.rand.org/content/dam/rand/pubs/research_report/RRAC/RRAC111R)





## radicalization

- Gill et al.'s (2014) study was perhaps the first. In a sample of 119 lone actor terrorists, they found that 35% of the sample virtually interacted with a wider network of political activists and that 46% learned aspects of their attack method through virtual sources.
- They also found that al-Qaeda inspired lone actors (65%) were significantly more likely to learn through virtual sources than their right-wing inspired (37%) or single-issue inspired (19%) counterparts.
- They also found that isolated dyads were significantly more likely to interact with co-ideologues online than those who committed their attacks alone.



## radicalization



1. The growth of the Internet did not correlate with a rise in lone-actor terrorist activity year-on-year from 1990 to 2011.
2. There is a growing trend amongst lone-actors to make use of the Internet. In other words, whilst the Internet has not caused a growth in numbers of lone actor terrorists, it has altered their means of radicalisation and attack learning. The Internet, therefore, acts as a substitute for other factors such as intelligence gathering and attack planning, not necessarily a force enabler.
3. Younger offenders were significantly more likely to engage in both virtual learning and virtual interaction than older offenders.



Gill, P. and Corner, E. (2015). "Lone-Actor Terrorist Use of the Internet and Behavioural Correlates", in *Terrorism Online: Politics, Law, Technology and Unconventional Violence*, L. Jarvis, S. Macdonald and T. Chen (eds.). London: Routledge.

## radicalization



4. *The non-US based offenders were significantly more likely to learn through virtual sources.*
5. *Offenders who interacted virtually with co-ideologues were significantly less likely to successfully carry out a violent attack.*
6. *Offenders who made use of online tools to prepare for an attack were significantly less likely to kill or injure (despite being significantly more likely to plot an attack against indiscriminate soft targets).*
7. *There was a significant positive correlation between those who virtually interacted with co-ideologues and who interacted with co-ideologues face-to-face. Radicalisation (at least for lone actors)*

Gill, P. and Corner, E. (2015). "Lone-Actor Terrorist Use of the Internet and Behavioural Correlates", in *Terrorism Online: Politics, Law, Technology and Unconventional Violence*, L. Jarvis, S. Macdonald and T. Chen (eds.). London: Routledge.



## radicalization



### facebook.

- *One frequent evidence of radicalization is the facebook profile photo history (and links, e.g. foreign fighters)*
- *4 phases:*
  1. *Not-anonymous facebook profile supporting terroristic organizations;*
  2. *Linking/friendship to other profiles with ideological affinity, participating to thematic groups;*
  3. *Strengthening relationships/friendships with radicalists, using private channels (e.g. chat);*
  4. *Planning attacks, communicating with private/underground tools*





## Financing

- Websites may also be used as online stores, offering books, audio and video recordings and other items to supporters.
- Online payment facilities offered through dedicated websites or communications platforms make it easy to transfer funds electronically between parties.
- Funds transfers are often made by electronic wire transfer, credit card or alternate payment facilities available via services such as PayPal or Skype.



## Financing

- Online payment facilities may also be exploited through fraudulent means such as identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes and auction fraud





**The Telegraph** HOME NEWS SPORT BUSINESS ALL SECTIONS

**News**

UK World Politics Science Education Health Retail Royals Investigations Mail Newsletters

News

### New York woman charged with sending \$85,000 in Bitcoin to support Isis

By **Timothy B. Shah**, New York Times Staff Writer

**A** New York woman has been charged with sending \$85,000 in Bitcoin to support the Islamic State.

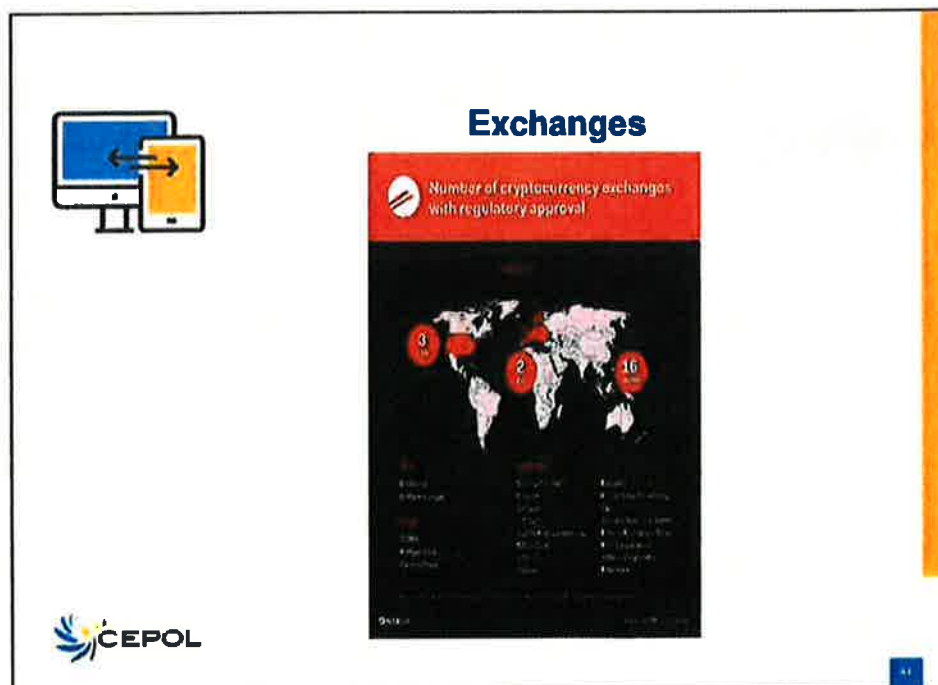
Zahra Shahnaz, a 27-year-old lab technician, was arrested at her home in Brentwood on Long Island on Wednesday night.

She appeared before Magistrate Judge Kathleen Tomblinson on Thursday afternoon and was remanded in custody to appear again in court in January.

**MORE STORIES**


- 1 Queen visits help of Duchess of Cambridge to host London Fashion Week event at Buckingham Palace
- 2 I had a cough - in a few days I'm told it is cancer and without treatment, I will be dead in three ...
- 3 Donald Trump targets in polls boosting Republican mid-term hopes
- 4 Brexit suits don't stack up? I agree entirely
- 5 Tight skirts and ruthless competition: the truth about being a female banker

FOLLOW TELEGRAPH NEWS

**Exchanges**

Number of cryptocurrency exchanges with regulatory approval

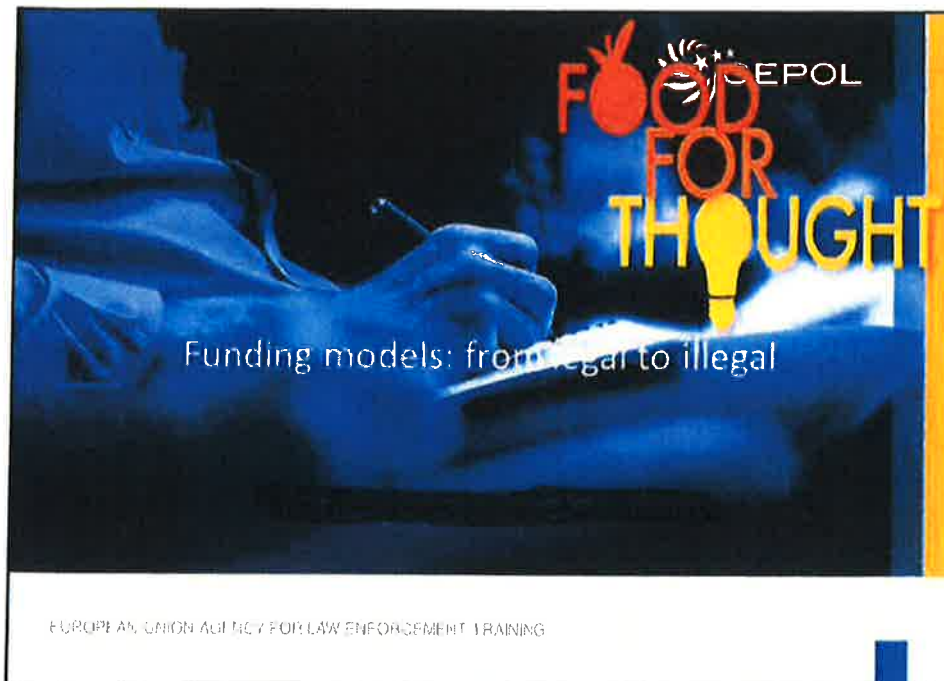


**3** North America

**2** Europe

**16** Asia

**CEPOL**



### The digital disruption supporting new criminal models




- Most popular media owner creates no content (**Facebook**)
- Fastest growing banks have no actual money (**SocietyOne**)
- Largest accommodation provider owns no real estates (**Airbnb**)
- Largest phone companies own no telco infra (**Skype, WeChat**)
- World's most valuable retailer has no inventory (**Alibaba**)
- World's largest movie house owns no cinemas (**Netflix**)
- Largest software vendors don't write the apps (**Apple & Google**)
- World's largest taxi company owns no taxis (**Uber**)

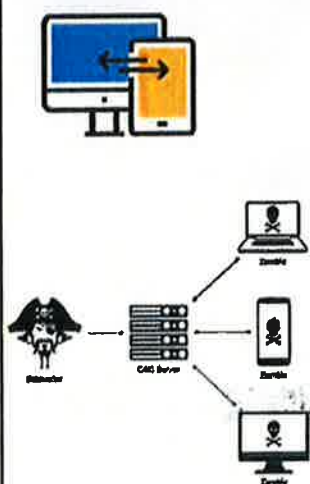
CEPOL

IT based crimes don't require IT sk

This slide contains a list of examples of digital disruption. It includes an icon of a computer monitor and a smartphone with bidirectional arrows. The CEPOL logo is in the bottom left, and the text 'IT based crimes don't require IT sk' is in red at the bottom right.





**funding – crime as a service**



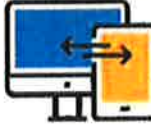
A Botnet is a network of infected computers (bots or zombies) completely managed by attackers (botmasters).

The botmasters control the activities of the entire structure giving orders to every single bot to achieve the purpose for which it has been composed.

The recent spread of botnets has increased due to various factors such as IoT, powerful connectivity, malware customization (e.g. Zeus), availability of ready-to-use vectors of infection (e.g. Blackhole), new business model (aaS model).

**funding – crime as a service**



**Blackhole pricing model**

Annual licence: \$ 1500  
 Hal-year licence: \$1000  
 3-month licence: \$700


Update cryptor \$ 50  
 Changing domain \$ 20 multidomain \$ 200 to license.  
 During the terms of the license all the updates are free.

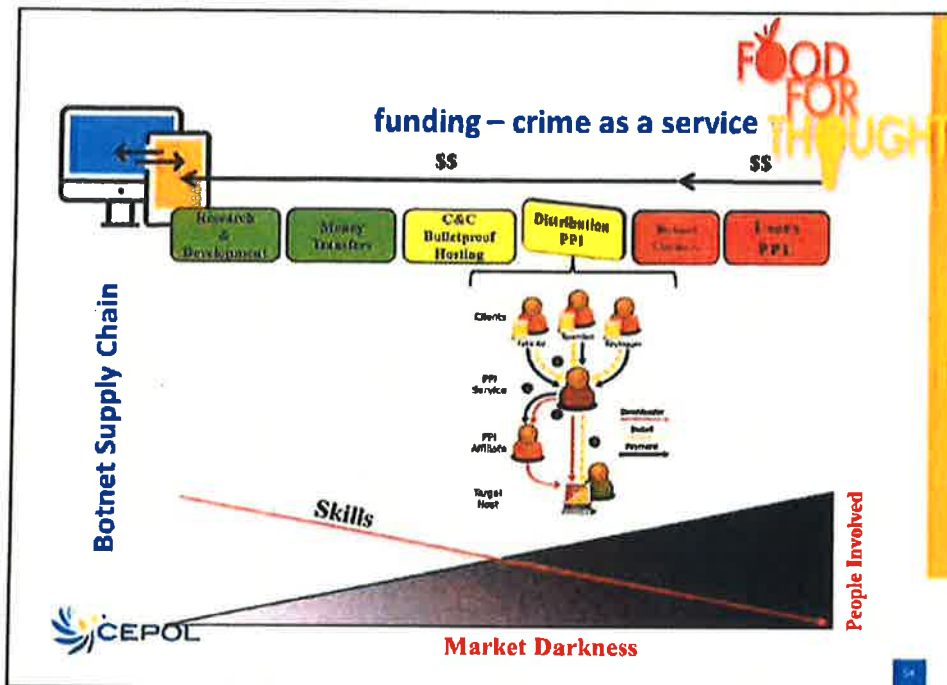
Rent on our server:

1 week (7 full days): \$ 200  
 2 weeks (14 full days): \$ 300  
 3 weeks (21 full days): \$ 400  
 4 weeks (31 full days): \$ 500  
 24-hour test: \$ 50

There is restriction on the volume of incoming traffic to a leasehold system, depending of the time of the contract.

Providing our proper domain included. The subsequent change of the domain: \$ 35



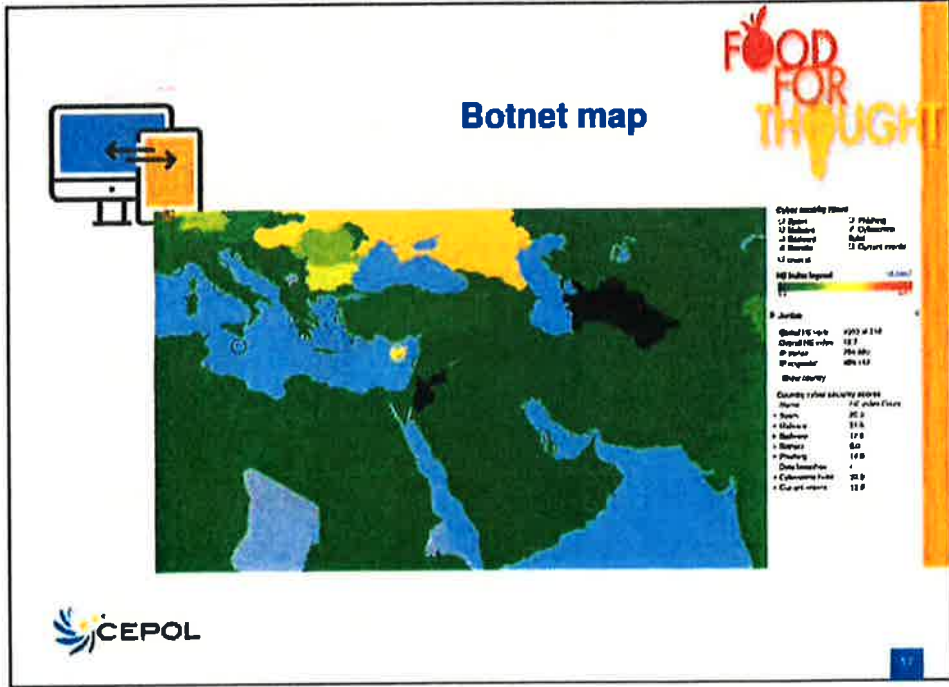
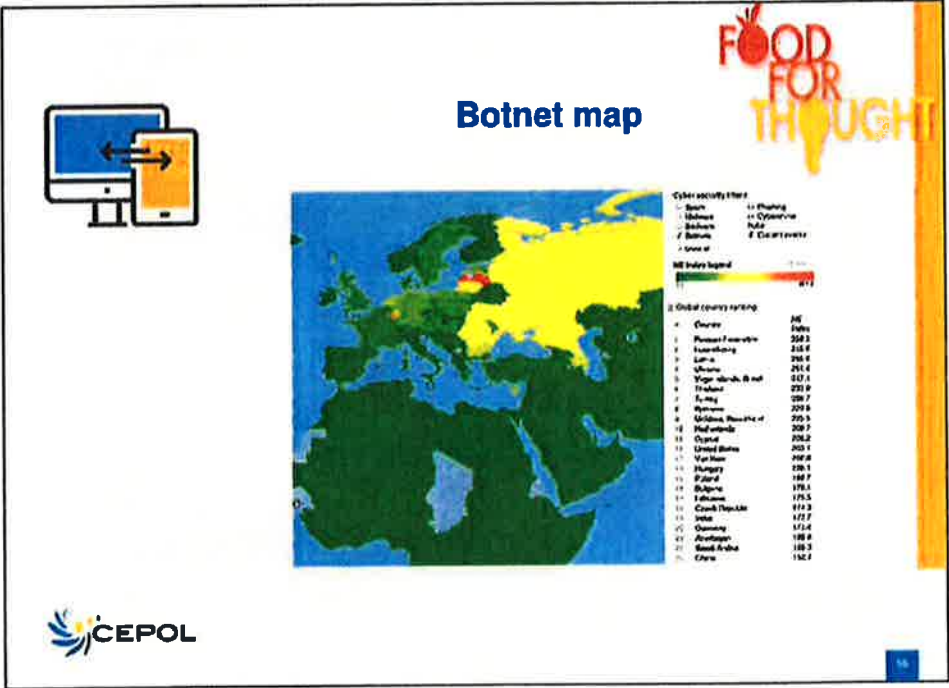


### Unfamous botnet usage


FDQN	IP
<a href="http://njrat7777.no-ip.biz/">http://njrat7777.no-ip.biz/</a>	91.235.160.103
<a href="http://asjad999.no-ip.biz/">http://asjad999.no-ip.biz/</a>	37.238.161.119
<a href="http://zakhacker.no-ip.org/">http://zakhacker.no-ip.org/</a>	37.236.204.157
<a href="http://hackerr0000.no-ip.biz/">http://hackerr0000.no-ip.biz/</a>	91.235.160.149
<a href="http://alihussain.no-ip.biz:9988">http://alihussain.no-ip.biz:9988</a>	37.239.248.37
<a href="http://hpyassin.no-ip.biz:81">http://hpyassin.no-ip.biz:81</a>	37.17.129.46
<a href="http://chrome-update.sytea.net">http://chrome-update.sytea.net</a>	37.238.176.71
<a href="http://safansalil.no-ip.biz">http://safansalil.no-ip.biz</a>	37.238.29.27
<a href="http://a7zaan.no-ip.biz">http://a7zaan.no-ip.biz</a>	37.236.76.68
<a href="http://younladeaaa.zapto.org/">http://younladeaaa.zapto.org/</a>	62.201.203.109
<a href="http://qaseem.zapto.org/">http://qaseem.zapto.org/</a>	37.239.64.193
<a href="http://hackid12.no-ip.biz/">http://hackid12.no-ip.biz/</a>	37.237.136.208

njRAT infections (Symantec)  
 the majority of the C&C server IP addresses were traced to ADSL lines used by home users Middle Eastern region.

No Data    0%    2%    10%    20%    30%    40%







## Domain generation algorithms (linguistic analysis)

**Meaningful Word Ratio (English dict)**

$d = \text{facebook.com}$

$$R(d) = \frac{|faco| + |book|}{|\text{facebook}|} = 1$$

likely non-DGA generated



$d = \text{pub03atr.info}$


$$R(d) = \frac{|\text{pub}|}{|\text{pub03atr}|} = 0.375.$$

likely DGA generated

**N-gram Popularity (English dict)**



$d = \text{facebook.com}$								$d = \text{saxrqv.com}$				
fa	ac	ca	ab	bo	oo	ak		sa	av	vr	rq	qv
108	343	438	29	116	114	45		4	45	17	0	0
mean: $S_1 = 170.8$								mean: $S_2 = 13.2$				
likely non-DGA generated								likely DGA generated				

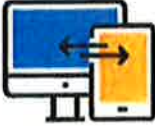





## Filtering

- A malicious domain does not become "Popular". We then filter by index of popularity (Alexa 1M whitelist)
- We filter the domains that refer to a CDN (names too "dirty" that could generate false positives)
- We filter for top level domains that they do not allow abusive registrations (.gov, .edu, .mil, ...)
- Filter for response times (TTL)
  - Filter by " $\Delta$  days" (`now () - registeredDate ()`)
- We filter for the domains that are found to have a reliable "Human" factor

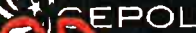
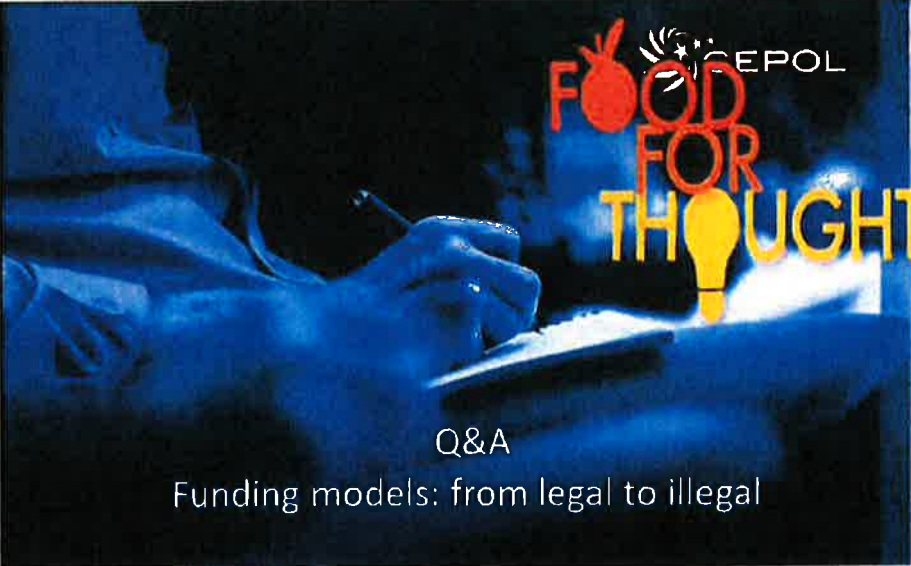







## Filtering

- Recap: ( 50.000 domains)
  - 20.000 TTL > 300 seconds
  - 19.000 non in "Alexa top 1M list"
  - 15.000 are not related to CDN
  - 800 have a DGA-Gen factor
  - 700 are not controlled domains (es: .gov)
  - **300 are younger than "A days"**


Suspects!

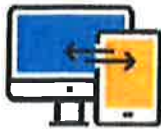


## FOOD FOR THOUGHT

Q&A

Funding models: from legal to illegal





## Research findings (2017)

○ A third of the sample (32%) prepared for their attacks by using online resources.

○ These included

- bomb-making instruction videos;
- poison manuals;
- downloaded copies of *Inspire* magazine;
- surveillance advice;
- an assassination guidebook;
- torture techniques;
- suicide vest production;
- body disposal;
- plans for the London Underground, Buckingham Palace, and other symbolic landmarks;
- military police voting records;
- terrorist training manuals.

 <http://onlinelibrary.wiley.com/doi/10.1111/1745-9133.12249/epdf>



## Research findings (2017)

TABLE 1

Observed Percentages for Individuals Who Used Online Learning (All Cases)

Variable	N <sup>a</sup> Values	Sig.	%	Odds
Online Learning (Extreme Right Wing)	5,952	0.015	78.3	3.190
Planned Attack	4,180	0.041	60.9	1.739
Government Target	4,319	0.036	83.3	4.505
Killed Others in Event	7,906	0.005	100.0	—
IED Attack	16,724	0.000	71.5	3.348
Armed Assault	5,995	0.015	85.7	5.505
Unarmed Assault	4,832	0.028	0.0	—
Acted Within a Cell	6,259	0.012	50.5	0.378
Attempts to Recruit Others	7,507	0.006	84.2	5.029
Nonvirtual Network Activity	17,487	0.000	79.2	4.398
Nonvirtual Place Interaction	13,747	0.000	73.1	3.176

Note. — = No odds calculated because of complete lack of variance.

<http://onlinelibrary.wiley.com/doi/10.1111/1745-9133.12249/epdf>

 CEPOL



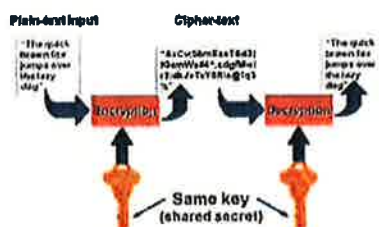
## Planning

- A recent case from France, *Public Prosecutor v. Hicheur*,<sup>15</sup> illustrates how different forms of Internet technology may be used to facilitate the preparation of acts of terrorism, including via thorough communications within and between organizations promoting violent extremism, as well as across borders.



## hidden communications-cryptography

- Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries)



- Use of encryption to instant messenger and mobile communications mediums;
- Tampered copies of "Asrar al-Mujahideen" that were deliberately infected with spyware





## hidden communications-cryptography

*The original Mujahideen Secrets (Asrar al-Mujahideen) encryption software launched in 2007, primarily for use with email. Asrar has had multiple releases over time and is distributed by the Global Islamic Media Front.*

*Amn al-Mujahid is an alternative encryption program released in December 2013. In this case from Al-Fajr Technical Committee (FTC) which is also a mainstream AQ outfit.*

*Asrar al-Dardashah, released by GIMF in February 2013, which is an encryption plugin for instant messaging based on the Pidgin platform – which connects to major US-based platforms.*

*Tashfeer al-Jawwal is a mobile encryption program, again from GIMF, released in September 2013, based on Symbian and Android.*


*Asrar al-Ghuraboo is yet another alternative encryption program, however importantly, released in November 2013 by Daesh, which coincides with Daesh breaking off from main AQ after a power struggle.*



## conclusions

- Today Daesh is more interested to play information warfare rather than to cyberattack
- Not clear the size of Daesh militant involved in cyber activity (SEA has 8 recognized guys)
- Cyber side of terrorism is more complicated to analyse due to anonymisation tools and trolls (complicating PSYOPS and information warfare techniques)
- Hacktivists alliances represent one of the phenomenon decoding keys
- Media focus attention on communication hacks and IW, helping propaganda
- LEAs can use effective monitoring tools
- Main severe risks are in the area of crime as a service (cyberattacks, hidden funding, use of technology to ease illegal activities as weapon traffick)
- Steganography and Cryptography! WW2 Enigma machine docet...





















## conclusions

**"A wealth of information  
creates a poverty of attention"**

*Herbert A. Simon*  
(1916 –2001, political scientist, economist)

 3,059,741,441 <small>Population of Europe</small>	 1,185,753,044 <small>Population of Africa</small>	 173,049,345,268 <small>Population of India</small>
 1,141,161,614 <small>Number of mobile phones</small>	 3,071,556 <small>Number of mobile phones</small>	 601,211,325 <small>Number of mobile phones</small>
 6,735,157,616 <small>Number of mobile phones in Africa</small>	 121,698,996 <small>Number of mobile phones in Africa</small>	 127,215,379 <small>Number of mobile phones in Africa</small>
 1,363,045,862 <small>Number of mobile phones</small>	 846,740,019 <small>Number of mobile phones</small>	 330,062,021 <small>Number of mobile phones</small>
 59,352,025 <small>Number of mobile phones</small>	 116,842,571 <small>Number of mobile phones</small>	 39,007 <small>Number of mobile phones</small>



<http://www.interninvestals.com/>




## Terrorist use of Internet

L'UNIONE FA LA FORZA. LA SICUREZZA È UNO DEI NOSTRI VALORI FONDAMENTALI.





### Market List With Up & Down




**Top Markets**


- Up / Online - Dream Market - 95.891 CF
- Up / Online - Point / Techna Free Market - 89.774 CF
- Up / Online - WallStreetMarket - 87.3011 CF

**Other Markets**


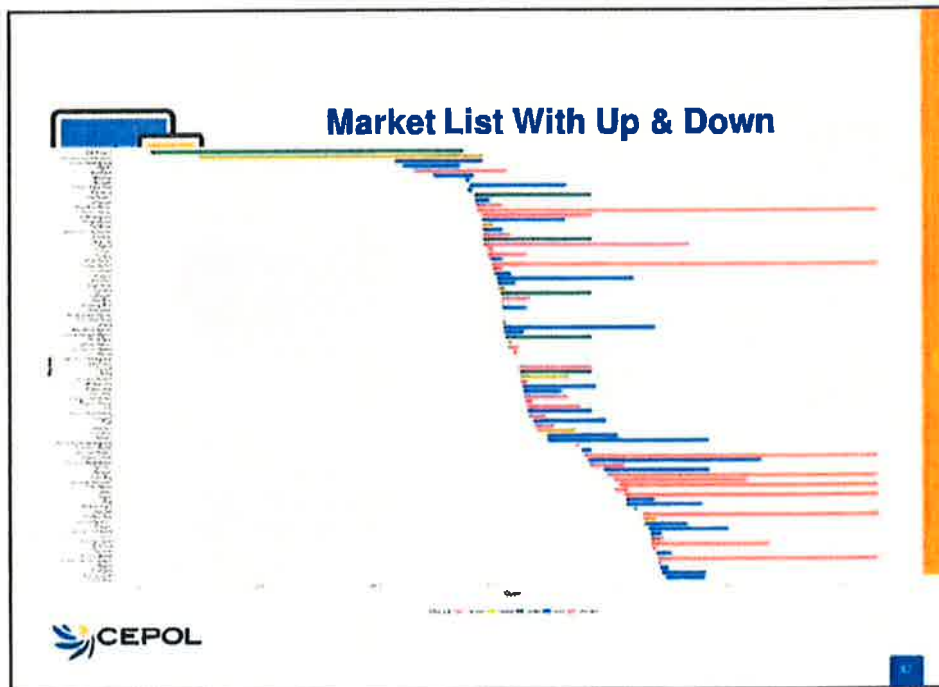
Up / Online - BitRise 2 - 83.500 CF
Up / Online - Empire Market CF
Down / Online - BitcoinMarket - 78.216 CF
Down / Online - SpruceBTC - 74.076 CF
Down / Online - TopMarket - 71.799 CF
Down / Online - BitcoinMarket - 70.676
Up / Online - Bitcoin - 68.426
Up / Online - BitCoin - 65.910 CF
Up / Online - Blockchain - 63.916
Up / Online - CMC - 61.826
Up / Online - ChainX - 61.826
Down / Online - DAX Future Market - 58.416
Up / Online - Bitcoin Market - 53.326 CF
Up / Online - Oxa - 56.316
Down / Online - Gem - 54.216 CF
Up / Online - Division TOR - 48.916
Up / Online - Dream Market (Bitcoin 1) - 41.826
Up / Online - Dream Market (Bitcoin 2) - 41.026



### Market List With Up & Down




Market	Total Lot(s)	Open Lot(s)	Market Status	New Order	Buy	Strategy	Commission	Vendor Bond	Bid	Period Vendor Pay	Created	Revised
• Eastern Market CE...	82509	29108	Open	✓	Open	4%	0.1 BTC	✓	✓	18.19.2018		
• SAH Road 212...	59800	14993	Open	✓	Open	✓	Nil (Liquid Vendor)	✓	✓	01.12.2018		
• Royal / Torka Free Market	8148	8421	Open	✓	Open	2.10%	✓	✓	✓	21.12.2019		
• Multiroom Market CE...	1948	3360	Open	✓	Open	0.0-0%	MS From the World	✓	✓	10.19.2018		
• East Market	3133	2183	Open	✓	Open	0-1%	0.1 BTC	✓	✓	11.10.2018		
• Royal Market	2025	2449	Open	✓	Open	4%	750	✓	✓	02.12.2018		
• Business Market	6472	3812	Open	✓	Open	1%	0.150	✓	✓	07.7.2017		
• The Market Order	✓	✓	Open	✓	Open	✓	Disposition Based Nil (Liquid Vendor)	✓	✓	01.12.2018		
• GOM 26 - 5th	548	437	Open	✓	Open	2-1%	85	✓	✓	26.7.2019		
• DSA Arampas CE...	Form	Form	Open	✓	Open	✓	✓	✓	✓	01.12.2018		
• Group and	Form	Form	Open	✓	Open	✓	✓	✓	✓			
• The Market Order	Form	Form	Open	✓	Open	✓	✓	✓	✓			



### Market List With Up & Down


Market	Total listings	Drug Listings	Market URL	User Guide	Reg	Holiday?	Commission	Vendor Seed	25% Pinned Vendor PDP	Created	Reviewed
• <a href="#">OpenMarket (EU) (Online)</a>	8334	8816		Click	Open	+	6%	0.1 BTC (201)	+	11-19-2015	🔗
• <a href="#">P&amp;H Road Trip (Online)</a>	5236	24093		Click	Open	+	?	Ref (Invited Vendors)	+	07.1.2011	🔗
• <a href="#">Penz / Techna Free Market (EU) (Online)</a>	9164	8811		Click	Open	+	1.14%	?	+	01-20-2018	🔗
• <a href="#">MultiVendor Market (EU) (Online)</a>	7049	1960		Click	Open	+	1.0-1%	500 Free For Trusted	+	10-18-2018	🔗
• <a href="#">EduMarket (EU) (Online)</a>	3122	2182		?	Open	+	1.5%	0.1 BTC	+	21-20-2016	🔗
• <a href="#">Hi Club Market (EU) (Online)</a>	5030	2449		?	Open	+	4%	200	+	07.11.2019	🔗
• <a href="#">MultiVendor Market (EU) (Online)</a>	6475	2033		?	Open	+	2%	0.55%	+	07.7.2017	🔗
• <a href="#">The Majestic Garden (EU) (Online)</a>	?	?		?	Ref	+	Discounts Given	Ref (Invited Vendors)	+	01-4-2014	🔗
• <a href="#">OMG (EU) (Online)</a>	849	492		?	Ref	+	1.1%	?	+	04.7.2016	🔗
• <a href="#">OMG (EU) (Online)</a>	Forum	Forum		?	Open	+	?	?	+	01.11.2015	🔗
• <a href="#">OpenMarket (EU) (Online)</a>	Forum	Forum		?	Open	?	?	?	?	?	🔗
• <a href="#">The Mark (EU) (Online)</a>	Forum	Forum	<a href="#">https://thehub24hours593.com/en/</a>	Click	Open	?	?	?	?	?	🔗




### Average prices

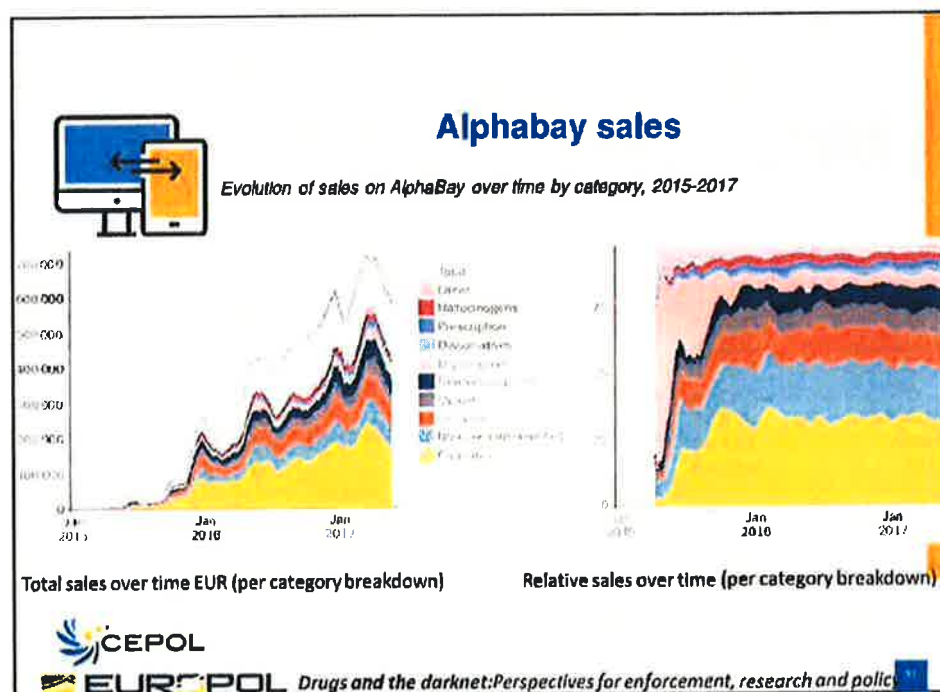
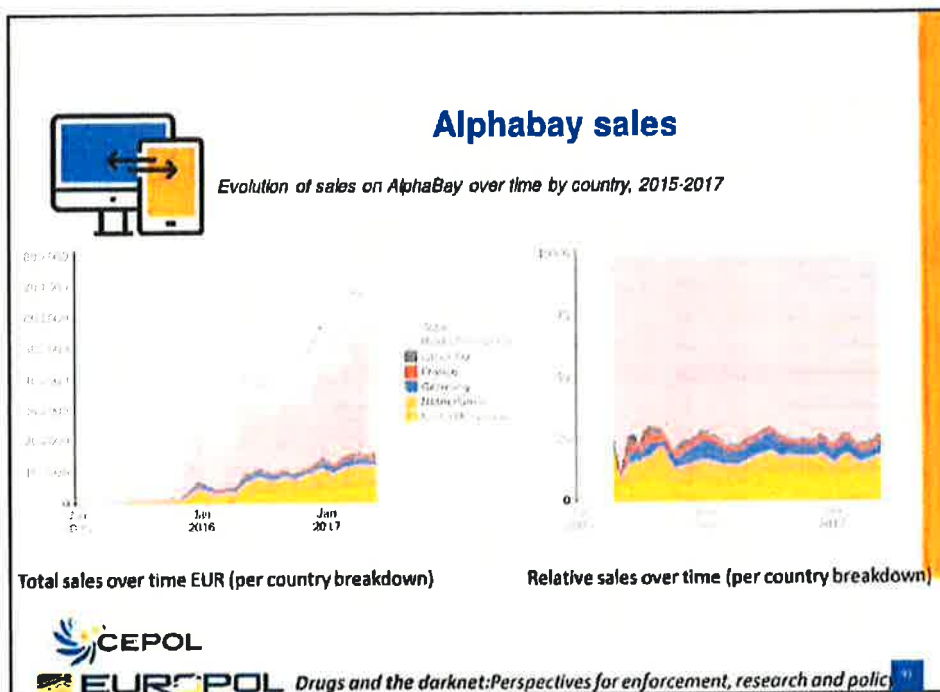
• Average prices (EUR) per drug unit (g/tablet/blotter); examples from five national darknet markets


Drug type/ market (country)	IOC 2.0 (Italy)	Flugsvamp 2.0 (Sweden)	Sipulikanava (Finland)	Silkkitie (Finland)	Hydra (Russia)
Price (EUR) (± SD) per drug unit (g/tablet/blotter)					
Herbal cannabis	11.7 (± 2.3)	10.3	20.0	20.0	17.2 (± 4.7)
Cannabis resin	7.7 (± 3.3)	8.2	NA	NA	13.6 (± 3.4)
Heroin	NA	102.8	NA	NA	64.5 (± 18.6)
Cocaine	95.8 (± 9.7)	72.0	140.0	150.0	160.0 (± 28.0)
Amphetamine	9.3 (± 5.5)	10.3	40.0	30.0	11.8 (± 3.8)
MDMA	5.2 (± 0.2)	6.2	NA	12.0	13.2 (± 4.0)
LSD	11.0 (± 4.7)	17.1	NA	NA	23.4 (± 4.5)




**EUROPOL** *Drugs and the darknet: Perspectives for enforcement, research and policy*












## Operation Bayonet




## Feedback

Rating	Date	Time	Content
👍	June 19, 2017	11:32	Forward Feedback upon our own Account product (Share in DC)
👍	June 18, 2017	23:48	Great! Great feedback!
👍	June 17, 2017	23:26	Let's get a full view of the product and get it on the page
👍	June 16, 2017	18:52	Let's get the product and get it on the page
👍	June 15, 2017	12:54	Let's get the product and get it on the page
👍	June 8, 2017	23:25	Let's get the product and get it on the page
👍	June 8, 2017	18:05	Let's get the product and get it on the page
👍	June 8, 2017	14:52	Let's get the product and get it on the page
👍	June 8, 2017	12:48	Let's get the product and get it on the page
👍	June 7, 2017	15:22	Let's get the product and get it on the page
👍	June 6, 2017	20:16	Let's get the product and get it on the page
👍	June 5, 2017	19:09	Let's get the product and get it on the page
👍	June 4, 2017	21:44	Let's get the product and get it on the page
👍	June 4, 2017	22:19	Let's get the product and get it on the page
👍	June 4, 2017	17:36	Let's get the product and get it on the page
👍	June 4, 2017	12:54	Let's get the product and get it on the page
👍	June 3, 2017	21:47	Let's get the product and get it on the page
👍	June 3, 2017	20:58	Let's get the product and get it on the page
👍	May 18, 2017	21:43	Let's get the product and get it on the page
👍	May 18, 2017	21:06	Let's get the product and get it on the page
👍	May 18, 2017	20:07	Let's get the product and get it on the page
👍	May 18, 2017	19:56	Let's get the product and get it on the page
👍	May 18, 2017	18:56	Let's get the product and get it on the page
👍	May 18, 2017	18:12	Let's get the product and get it on the page
👍	May 18, 2017	17:40	Let's get the product and get it on the page
👍	May 18, 2017	13:22	Let's get the product and get it on the page
👍	May 18, 2017	13:14	Let's get the product and get it on the page





## Drug data categories

Drug categories of primary interest	Other drugs	Non drugs
<p><b>Cannabis</b> all forms of cannabis products (herb, resin, oil, seeds)</p> <p><b>Opioids</b> heroin, opium, analgesics (e.g. oxycodone)</p> <p><b>Cocaine</b> all forms of cocaine products</p> <p><b>Synthetic stimulants</b> (meth)amphetamine, MDMA, MDA</p> <p><b>Dissociatives</b> ketamine, GHB, GBL</p> <p><b>Hallucinogens</b> LSD, PCP (excluding psychedelics)</p> <p><b>NPS</b></p> <ul style="list-style-type: none"> <li>● Cannabinoids: synthetic cannabinoids including spice, K2</li> <li>● Opioids: synthetic opioids including fentanyl, MF-45</li> <li>● Stimulants: methamphetamine, 4-fluorocamphetamine</li> <li>● Dissociatives: MKK, DXM</li> <li>● Hallucinogens: 25I-NBOMe, 4-AcO-DMT, 2C-B</li> </ul>	<p><b>Prescription drugs:</b> benzodiazepines, barbiturates, sildenafil and related products</p> <p><b>Psychedelics:</b> mushrooms and other</p> <p><b>Steroids:</b> steroid products</p>	<p><b>Drug paraphernalia:</b> bongas, pipes, scales</p> <p><b>Digital goods:</b> all forms of digital goods including forgeries, credit card numbers, e-books</p> <p><b>Electronics:</b> electronic items and components</p> <p><b>Tobacco:</b> tobacco products including e-cigarettes</p> <p><b>Weapons:</b> all sorts of illegal firearms</p> <p><b>Miscellaneous:</b> miscellaneous items not categorized in any other category</p>




## Surface Web




**USER**

Every computer on the Internet has a unique identity (IP number)




**SERVER**


When a user contacts a merchant on the Internet the identity can be traced back through the server

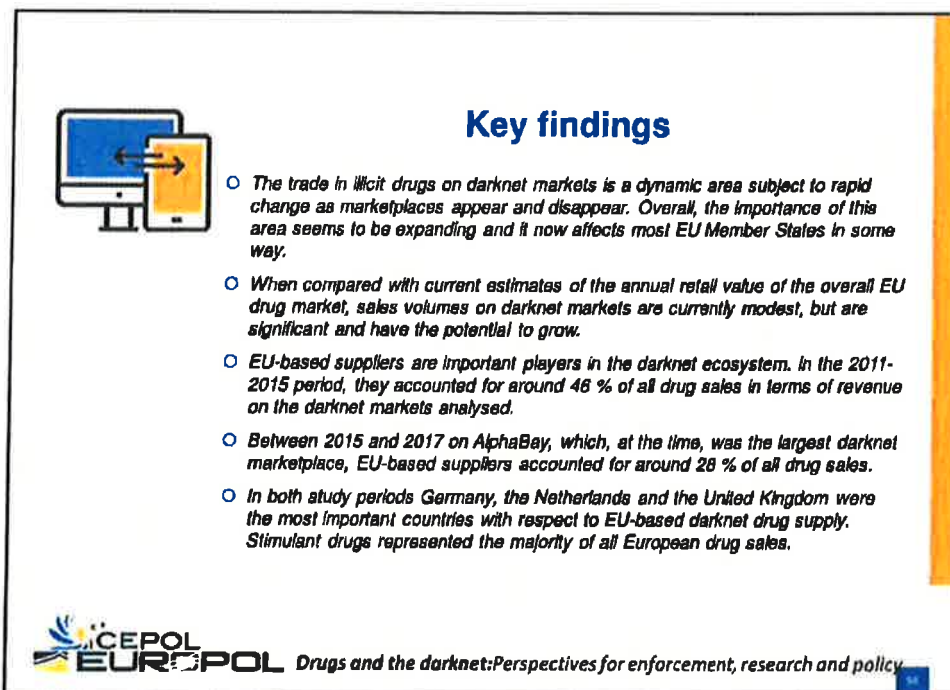
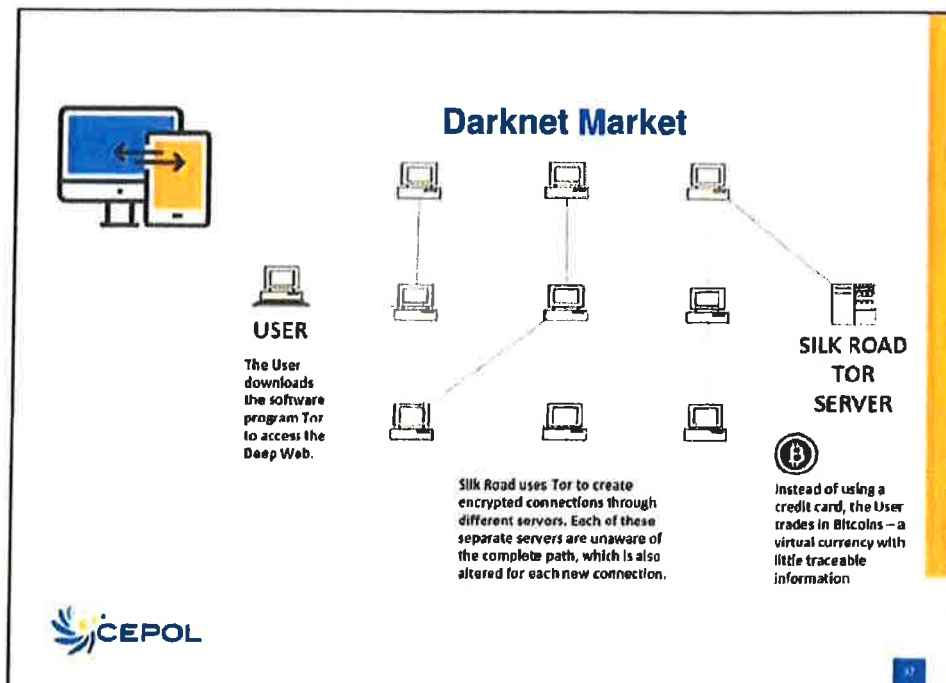


**MERCHANT**

The Merchant requires personal information (credit card and shipping details) from the User









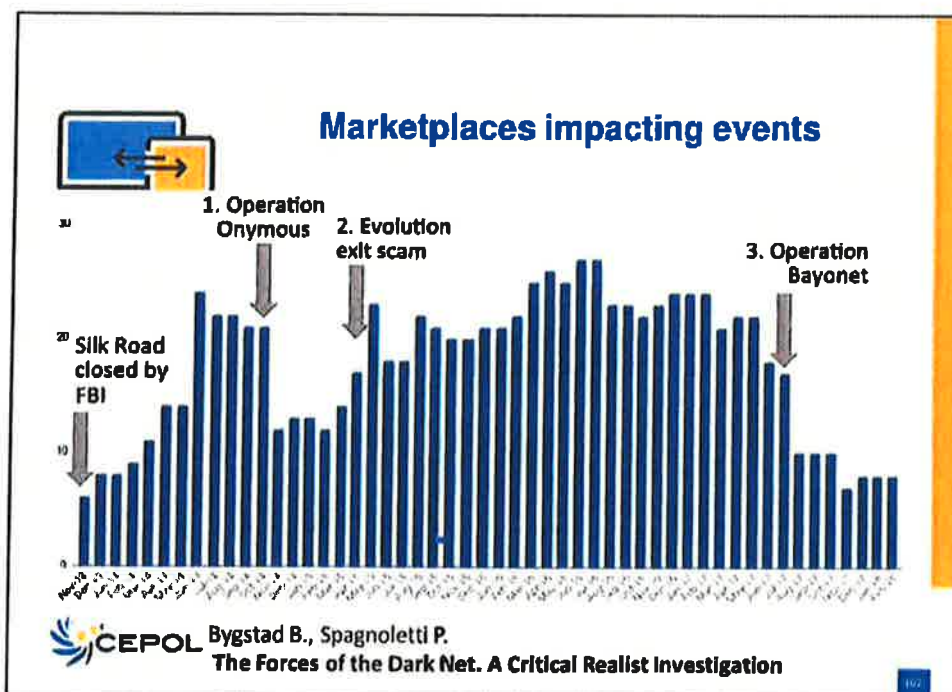
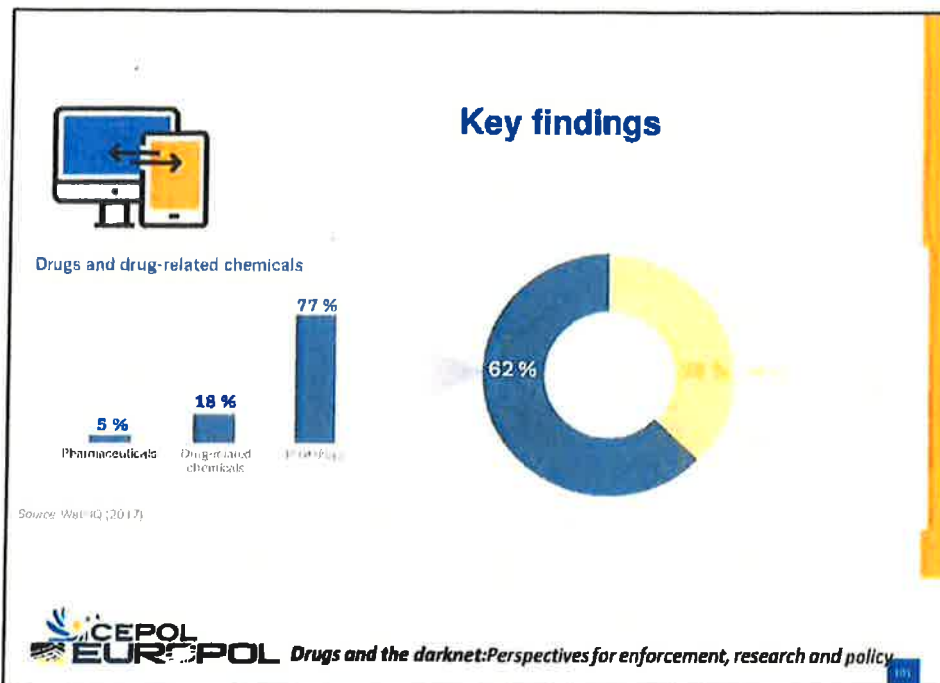
## Key findings

- New psychoactive substances (NPS) are less commonly sold than illicit drugs on the darknet market, probably reflecting the significant role played by surface web sales in this sector. The United Kingdom was the most frequently noted origin of NPS sales, which may reflect both patterns of demand and recent changes in legislation.
- The rationale underpinning darknet markets suggests that they will be most commonly used for mid- or low-volume market sales or sales directly to consumers. Large-volume sales (wholesale) are relatively uncommon.
- The highest market activity in terms of number of transactions was observed at the retail level, and retail sales values were greatest for cannabis and cocaine.
- The picture was different for MDMA and opioids, however, where mid-level sales represented a relatively large proportion of all sales (although still less in absolute terms), and the value of the mid-level sales was greater than the value of the retail sales.



## Key findings

- The picture was different for MDMA and opioids, however, where mid-level sales represented a relatively large proportion of all sales (although still less in absolute terms), and the value of the mid-level sales was greater than the value of the retail sales.
- This suggests that darknet markets may play a different role in the supply chain for these substances.
- Law enforcement interventions in the form of darknet market takedowns disrupt darknet markets, although the overall ecosystem appears to be fairly resilient with new markets quickly becoming established.
- Significant knowledge gaps exist with respect to the role of traditional organised crime groups (OCGs) in darknet markets. In particular, the extent to which OCGs are involved in the production, trafficking and distribution of drugs supplied on online markets is unclear.



### Lifetime of marketplaces

**Legend:**  
- First date  
- Still open  
- Closed type  
- Bold text only marks a place as bold

**Timeline Callouts:**  
- 2010: Desktop marketplaces...  
- 2011: Mobile marketplaces...  
- 2012: Desktop marketplaces...  
- 2013: Desktop marketplaces...  
- 2014: Desktop marketplaces...  
- 2015: Desktop marketplaces...

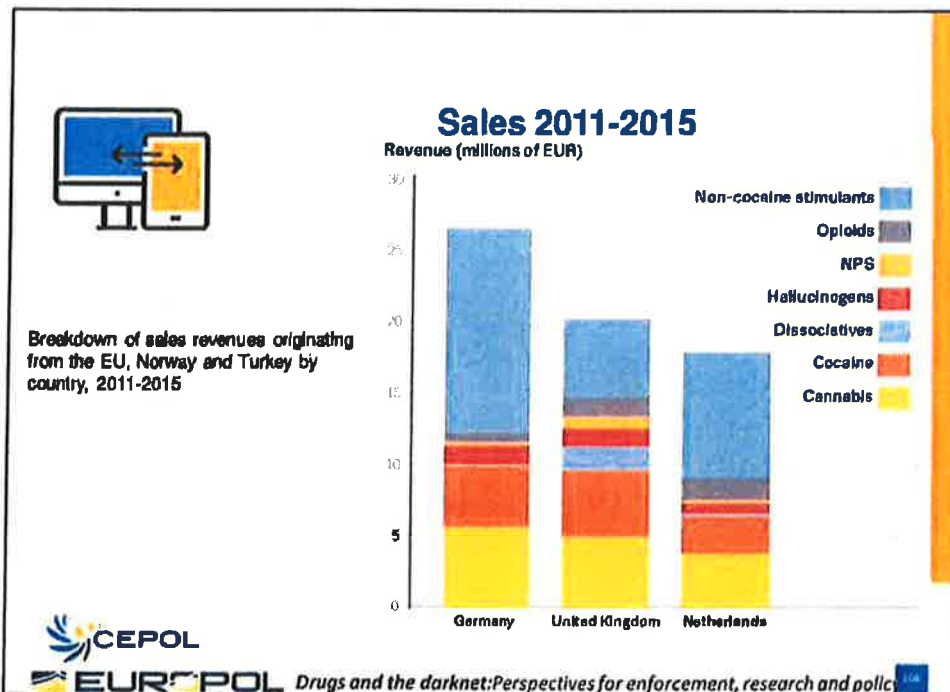
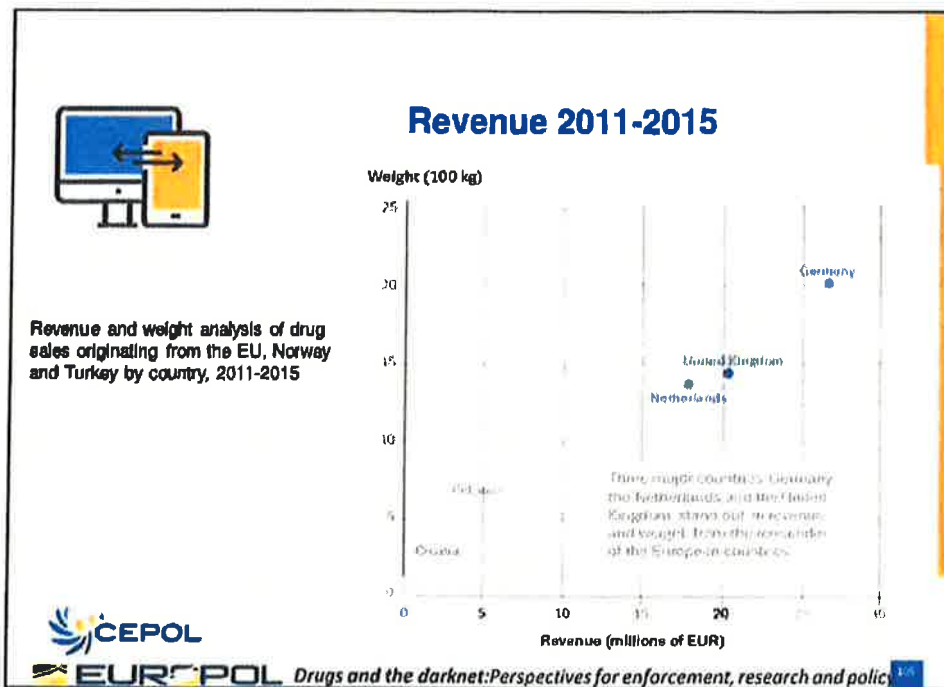
**CEP**  
**EURPOL** Drugs and the darknet: Perspectives for enforcement, research and policy 101

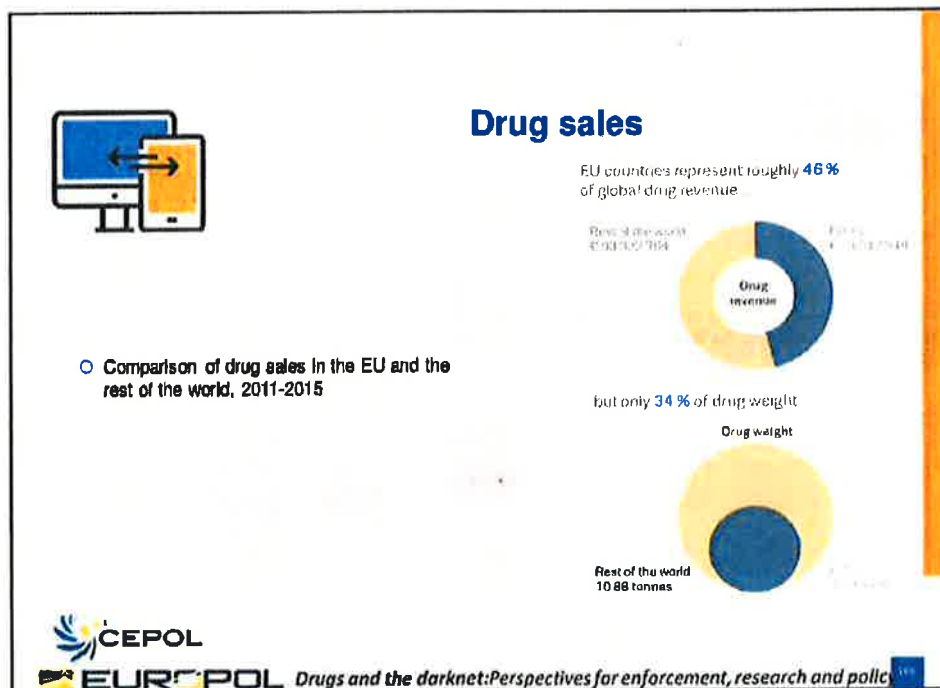
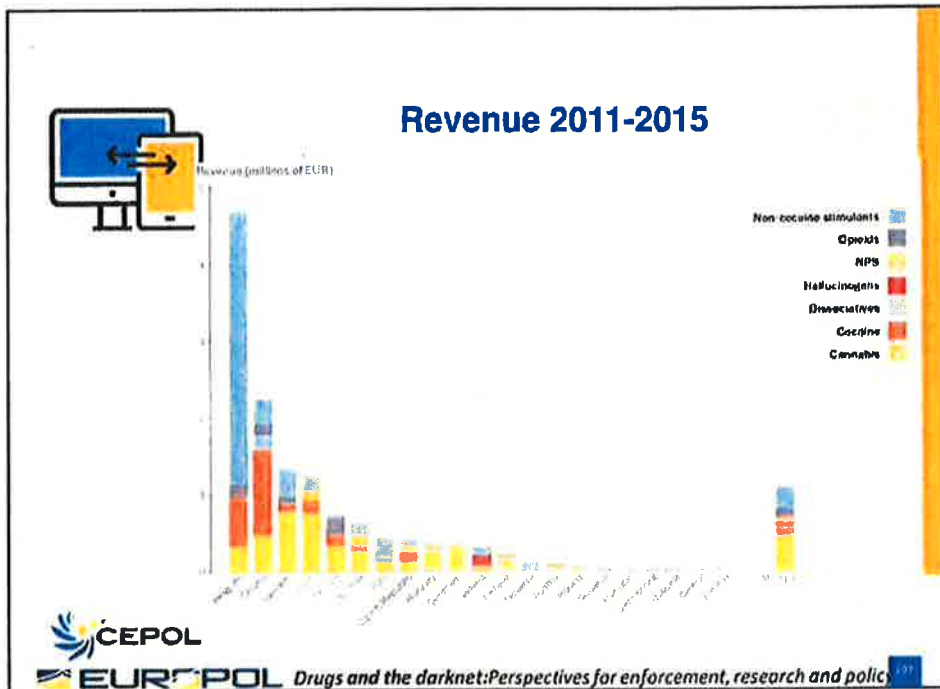
### Lifetime of marketplaces

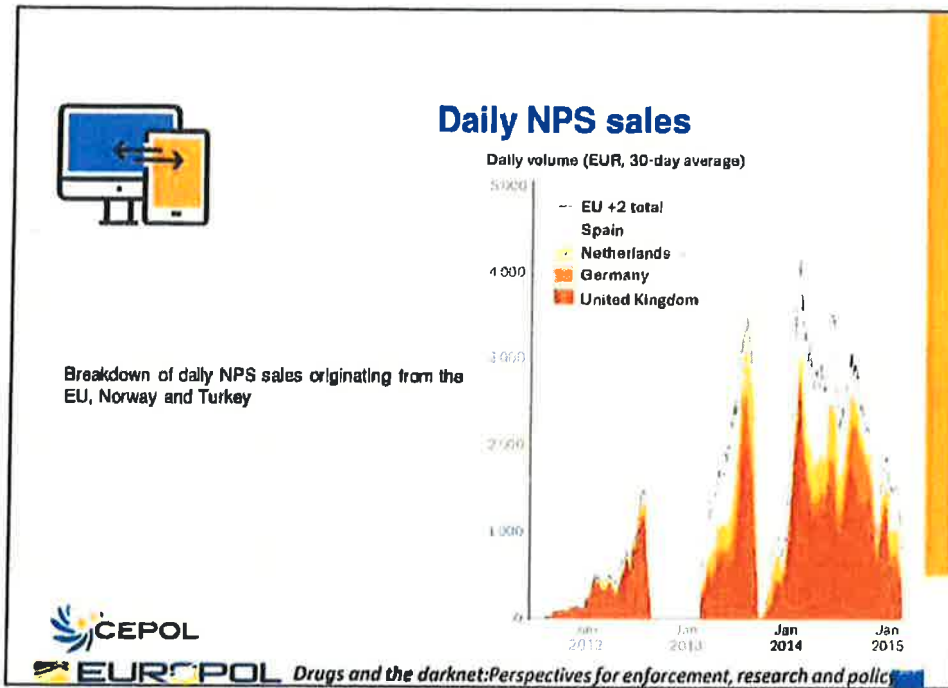
**Timeline Callouts:**  
- 2010: Desktop marketplaces...  
- 2011: Mobile marketplaces...  
- 2012: Desktop marketplaces...  
- 2013: Desktop marketplaces...  
- 2014: Desktop marketplaces...  
- 2015: Desktop marketplaces...

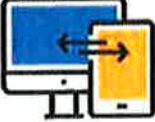
**CEPOL**  
**EURPOL** Drugs and the darknet: Perspectives for enforcement, research and policy 101









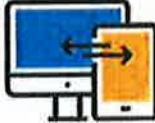


## Tor Marketplaces

**BLACK MARKETS** **ONLINE MARKETPLACES**

(Anonymous Net) Tor
Cryptocurrency
WOT based cryptography

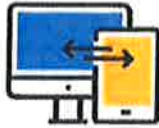
Anonymous enabling infrastructure



## IOCTA 2017

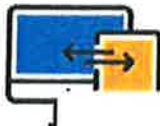
*Illicit online markets, both on the surface web and Darknet, provide criminal vendors the opportunity to purvey all manner of illicit commodities, with those of a more serious nature typically found deeper in the Darknet. Many of these illicit goods, such as cybercrime tools, fake documents, and enablers for further criminality.*

CEPOL



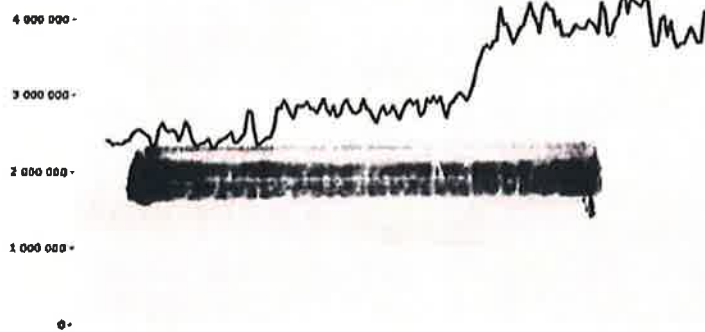
## IOCTA 2017

- Sale of illicit goods to dedicated criminal websites and markets hosted on anonymising networks such as Tor, I2P and Freenet, although such activity appears to be mainly concentrated on the Tor network
- As of June 2017, the Tor network had over 2.2 million directly connecting users, and hosted almost 60 000 unique .onion domains.
- What is difficult to quantify is the proportion of activity on these networks that is illicit, compared to its legitimate use by regular users to browse the web more securely.
- In one study however, almost 57% of active sites that could be classified related to some form of illicit activity



## Tor USERS

Directly connecting users

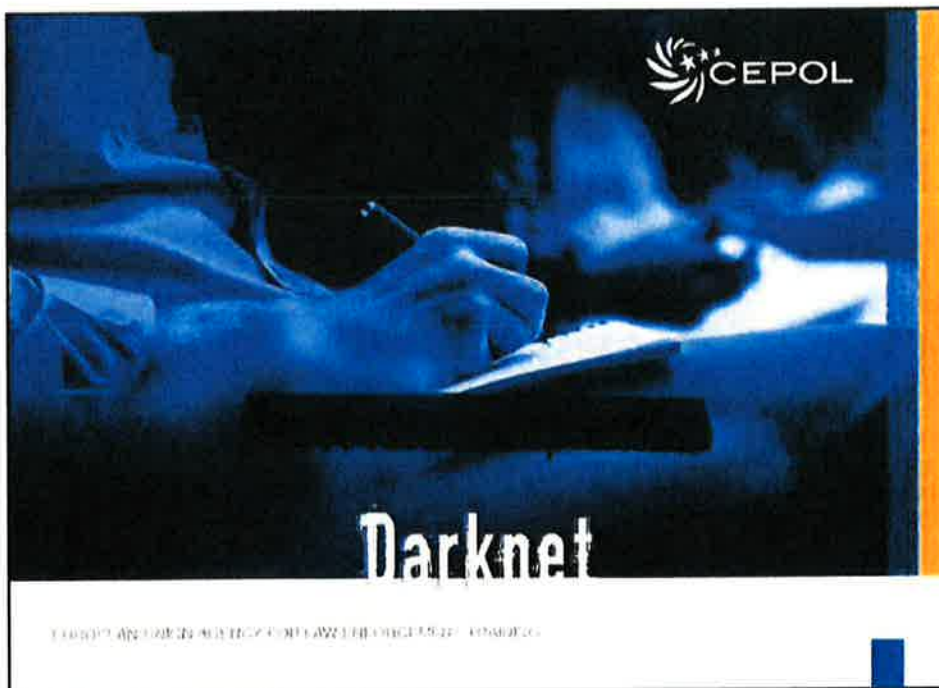
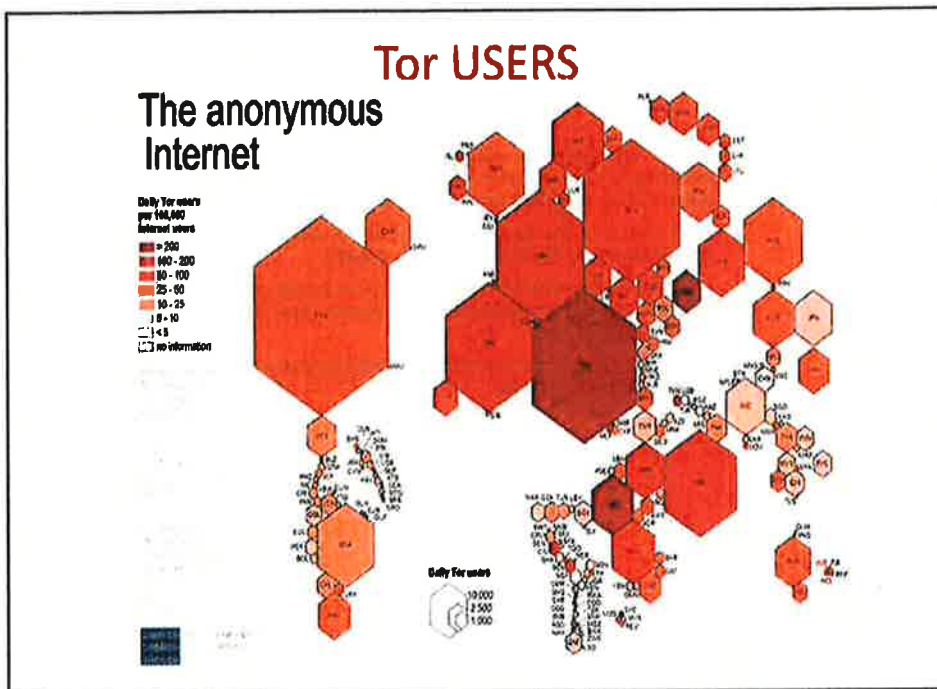


2017-10

2018-01

The Tor Project - <https://metrics.torproject.org/>







## Enabling Infrastructure

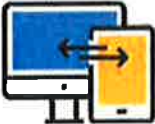
- TOR: anonymous network (your presented IP changes continuously)
- Cryptocurrency: Digital cash (BTC,XMR,ETH,LTC)
- VPN



## Introduction



- The marketplaces vendors/buyers settle up in bitcoin, a digital currency that can be exchanged for the old-fashioned sort and that offers near-anonymity during a deal.
- Almost all sales are via "cryptomarkets": dark websites that act as shop-fronts.
- These provide an escrow service, holding payments until customers agree to the bitcoin being released.
- Feedback systems like those on legitimate sites such as Amazon and eBay allow buyers to rate their purchases and to leave comments, helping other customers to choose a trustworthy supplier.
- The administrators take a 5-10% cut of each sale and set broad policy (for example, whether to allow the sale of guns). They pay moderators in bitcoin to run customer forums and handle complaints.






## Introduction

- **Forum Markets.** These are basically forums where vendors present their products, customers posting feedback and a community is discussing. These markets neither have an online shopping like interface nor a reputation or escrow system. Trusted members of the community may act as escrow agents.
- **Centralized Markets.** The original "Silkroad" was the first of this kind. Buyers and vendors have their bitcoins on an online wallet which is controlled by the markets admin and therefore rely totally on the good will of the markets admins. Several big scams happened in the past in which millions of \$ were stolen.
- **Multi-Signature Markets.** In this markets funds will be deposited in a multi-signature wallet. At three least three parties (usually: buyer, vendor, market admin) have the control over these wallets. Two of them have to agree to release the funds. The most elaborated marketplace of this kind was "The Marketplace". Second generation marketplace could not get some serious market share yet.
- **Decentralized Markets.** There are some projects which are currently developing software to host drug marketplaces in a distributed manner. Only Bitmarkets is fully functional, but none have yet been adopted by the darknet market community.

## Introduction

<b>Nucleus Market</b> Established: Nov 24, <a href="http://tixmebfx.onion">tixmebfx.onion</a>	<b>Dream Market</b> Established: Nov 15, 2013 <a href="http://txocahw4eruf5lu.onion">txocahw4eruf5lu.onion</a> -Invite (Required) -Forum	<b>AlphaBay</b> Established: Dec 22, 2014 <a href="http://gw-1gdwri.onion">gw-1gdwri.onion</a>
<b>Outlaw Market</b> Established: Dec 29, <a href="http://siwcztwbpd">siwcztwbpd</a>	<b>Agora Marketplace</b> Established: Dec 3, 2013 <a href="http://ggawayyfoe.onion">ggawayyfoe.onion</a> (Required)	<b>Abraxas Market</b> Established: Dec 13, 2014 <a href="http://usel.onion">usel.onion</a>
<b>East India Company</b> Established: Apr 28 2015 <a href="http://r4c35ipwifutacclv.onion">r4c35ipwifutacclv.onion</a>	<b>Market</b> Established: Dec 22, 2014 <a href="http://gxdn2zd.onion">gxdn2zd.onion</a>	<b>Babylon (Italian)</b> <a href="http://babylonxirtdyomy.onion">http://babylonxirtdyomy.onion</a>







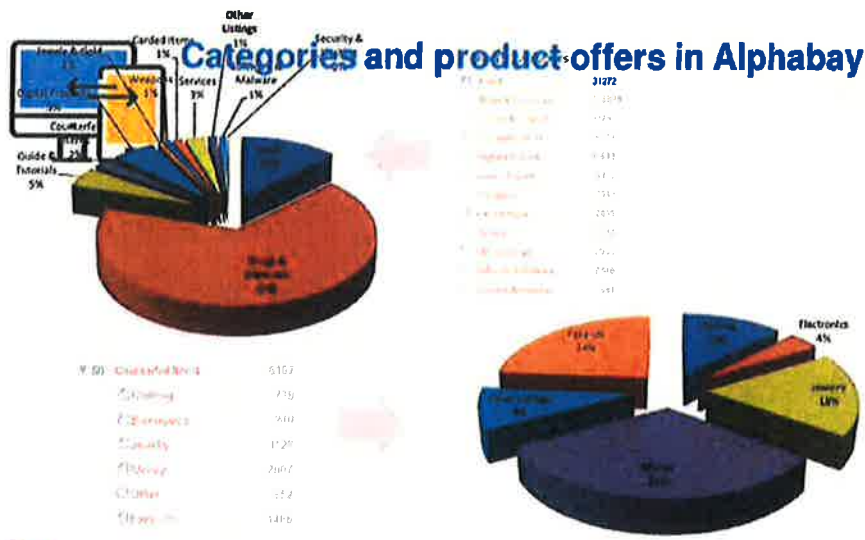
### Question (food for thoughts)

- Law enforcement agencies are far less effective at takedown than commercial firms, who get an awful lot more practice.
- the police must either raise their game, or subcontract the process.
- takedown is a career for specialists rather than a part-time activity for a single officer

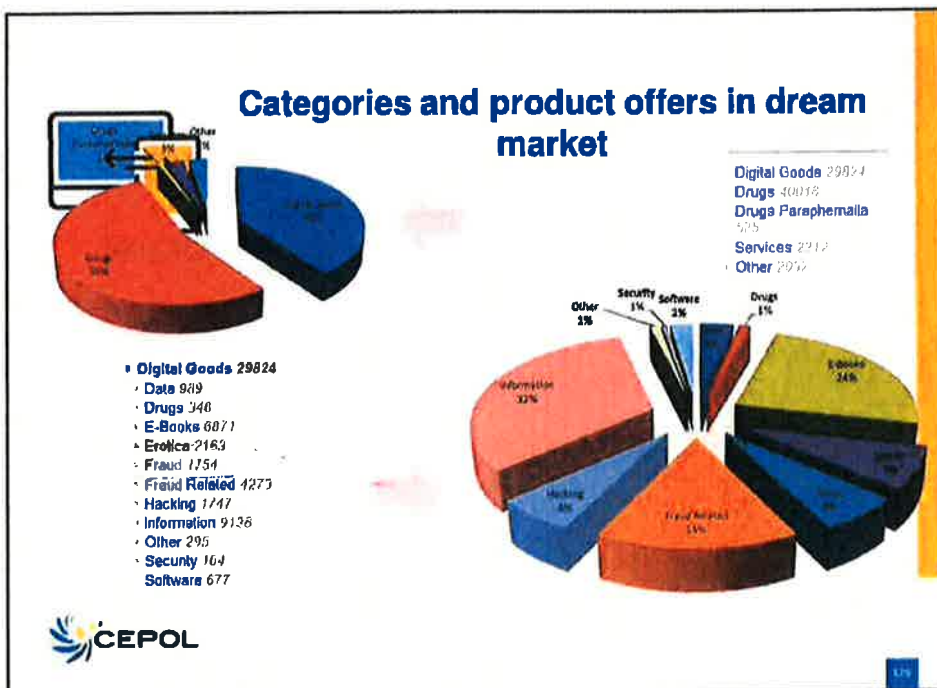
**Taking Down Websites to Prevent Crime**  
 Alice Hutchings, Richard Clayton and Ross Anderson



114



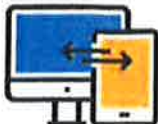
115



### The reputation problem

- While several characteristics of electronic markets serve to facilitate trade, online transactions also involve greater uncertainty and increased opportunities for fraud.
- Unlike buyers in traditional settings, online shoppers are often physically unable to inspect the products for sale and typically must rely on pictures and descriptions provided by the seller (information asymmetry)
- Any time buyers cannot determine the quality of a product until after the purchase has been made, sellers have less incentive to provide high quality products (e.g. lemon's market).
- One way that electronic marketplaces like eBay have attempted to reduce fraud and instill buyer trust is by allowing participants to post feedback about their experiences (signal)

**CEPOL**



## The reputation problem

- TOR Marketplaces are black online markets
  - High information asymmetry: illegal trade of goods/services reinforces information asymmetry, due to the poor reliability of the criminal activity of the vendor, increasing the fraud risk.
  - Online legal markets (e.g. Ebay) protect customers with signals like vendor reputation (feedback), which mechanisms do not completely protect from fraud
  - TOR Marketplaces replicate these mechanisms, reinforced offering the escrow service and, sometimes, by denying the "Finalized" status of the goods received.
- Many examples show that many vendors, even after very positive feedback, disappear after a period of fair trading. This is the well known phenomenon named "exit scam" (e.g. 9THWonder)



## The reputation problem

"I am sorry guys but I have scammed you. I am not going to try to justify it with my reasons, I am just a terrible person.

I am sorry for each and every person affected, I am ashamed about the way I have deceived so many people for my own personal gain.

For what it is worth the money is not going to stupid lifestyle enriching purposes.

Even though I could likely go on for a few more days, making fake promises and feedback I have reached my goal and will lock myself out of my account.

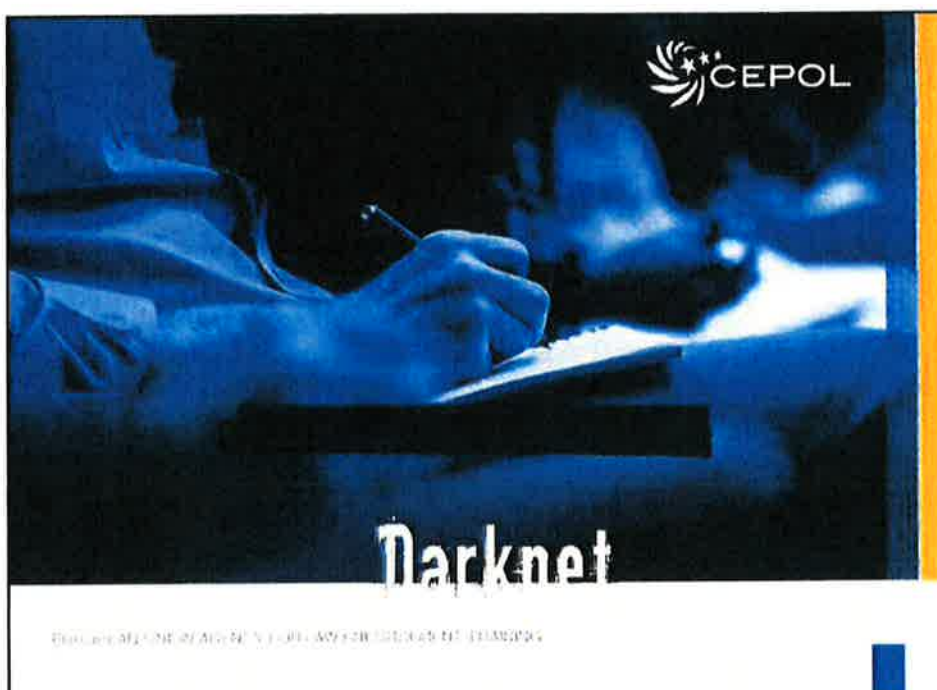
For anyone interested. This started on 19-22 December. After that I have not had a single gram of weed or hash in stock.

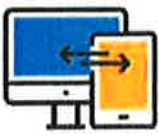
That is all I had to say. After this message I will destroy my PGP key which grants me access to Bitmessage, Lelantos and EVO

Goodbye

• Wonder"


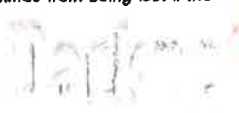






## A typical transaction

1. *Alice wants to purchase an item from Bob.*
2. *Instead of directly paying Bob, she pays the marketplace operator, Oscar.*
3. *Oscar then instructs Bob that he has received the payment, and that the item should be shipped.*
4. *After Alice confirms receipt of the item, Oscar releases the money held in escrow to Bob.*
5. *This allows the marketplace to adjudicate any dispute that could arise if Bob claims the item has been shipped, but Alice claims not to have received it.*
6. *Some marketplaces claim to support Bitcoin's recently standardized "multi-sig" feature which allows a transaction to be redeemed if, e.g., two out of three parties agree on its validity.*
7. *For instance, Alice and Bob could agree the funds be transferred without Oscar's explicit blessing, which prevents the escrow funds from being lost if the marketplace is seized or Oscar is incapacitated.*



## Drug sale on Tor

- *The drugs market is undoubtedly the largest criminal market on the Darknet, offering almost every class of drug for worldwide dispatch.*
- *As of June 2017, AlphaBay, one of the largest Darknet markets, had over 250 000 separate listings for drugs, accounting for almost 68% of all listings. 30% of the drugs listings related to Class A drugs.*
- *While it is assessed that the majority of vendors are lone offenders, dealing in small amounts, it is reported that many of the 'top sellers' are likely organised crime groups earning significant profits.*
- *Some studies suggest that the total monthly drugs revenue of the top eight Darknet markets ranges between EUR 10.6 million and EUR 18.7 million when prescription drugs, alcohol and tobacco are excluded*



## Drug sale on Tor

- *The Darknet is a key facilitator for various criminal activities **Including the trade in illicit drugs, illegal firearms and malware.** Darknet marketplaces are becoming increasingly decentralised.*





## Modus operandi

- *Once a deal is struck and payment is waiting in escrow, drugs are packed in a vacuum-sealed bag (e.g. often using latex gloves to avoid leaving fingerprints or traces of DNA, and dipped in bleach as a further precaution against leaving forensic traces).*
- *A label is printed (customs officials are suspicious of handwritten addresses on international packages).*
- *Smart sellers use several post offices, all far from their homes—and, preferably, not overlooked by CCTV cameras.*
- *Some offer to send empty packages to new customers, so they can check for signs of inspection.*
- *Smart buyers use the address of an inattentive or absent neighbour with an accessible postbox, and never sign for receipt.*
- *Judging by the reviews, around 80% of shipments get through*

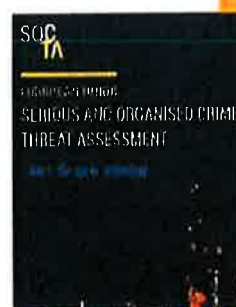


13

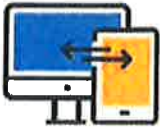


## Identity theft

- *The Introduction of forged documents*
- *Increasingly sophisticated security features protecting documents against forgery as well as improved technical control measures have compelled OCGs to improve the quality of fraudulent documents.*
- *Suppliers of raw materials now primarily rely on Darknet marketplaces to sell their products.*




**BLACK MARKET**

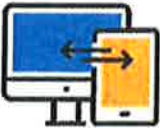


### Counterfeited goods (Iocta 2017)


- *Infringements of Intellectual property rights (IPR) are a widespread and ever-increasing worldwide phenomenon. In 2013, the international trade in counterfeit products represented up to 2.5% of world trade. The impact of counterfeiting is even higher in the European Union, with counterfeit and pirated products amounting to up to 5% of imports.\*<sup>2</sup> As discussed earlier, most counterfeit products can more readily be sold on the surface web, being presented as, or mixed with, genuine products.*
- *Consequently, counterfeit products only account for between 1.5% and 2.5% of listings on Darknet markets. Moreover, the most commonly listed counterfeit products are those which are obviously illegal - counterfeit bank notes and fake ID documents, which account for almost one third and almost one quarter of counterfeit listings respectively.*
- *The majority of reported law enforcement investigations in the EU relating to counterfeit goods on the Darknet relate to counterfeit bank notes.*


142

### Recurring Lemon's market



- *IRC cybercrime markets*
- *Markets run through Internet Relay Chats has been shown to be no different from the notorious market for lemons (Florencio)*
- *Darknet markets are different*
- *Why?*


143



## Counterterrorism on TOR

- Why Counterterrorism investigations passes through TOR?



## Conclusions

- Online markets still account for a small share of illicit drug sales, they are growing fast
- Sellers are competing on price and quality, and seeking to build reputable brands. Turnover has risen from an estimated \$15m-17m in 2012 to \$150m-180m in 2015.
- The share of American drug-takers who have got high with the help of a website jumped from 8% in 2014 to 15% this year, according to the Global Drug Survey, an online study.
- Online drug markets are part of the "dark web": sites only accessible through browsers such as Tor, which route communications via several computers and layers of encryption, making them almost impossible for law enforcement to track. Buyers and sellers make contact using
  - e-mail providers such as Sigaint, a secure dark-web service,
  - encryption software such as Pretty Good Privacy (PGP);
  - VPN software







## Darknet Marketplaces

- The common point between all the marketplaces is that they are *risk management* platforms for participants in (mostly illegal) transactions.
- Risk is mitigated on several levels:
  - First, by abolishing physical inter-actions between transacting parties, these marketplaces claim to reduce (or indeed, eliminate) the potential for physical violence during the transaction.
  - Second, by providing superior anonymity guarantees compared to the alternatives, online anonymous market-places shield – to some degree – transaction participants from law enforcement intervention.
  - Third, online anonymous marketplaces provide an escrow system to prevent financial risk. These systems are very similar in spirit to those developed by electronic commerce platforms such as eBay or the Amazon Marketplace.
  - Fourth, online anonymous marketplaces provide a feedback system to enforce quality control of the goods being sold. In marketplaces where feedback is mandatory, feedback is a good proxy to derive sales volume



CEPOL

# TOR Marketplaces

Q&A

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

