<table>
<thead>
<tr>
<th>Arrival of participants</th>
<th>Monday 08 October</th>
<th>Tuesday 09 October</th>
<th>Wednesday 10 October</th>
<th>Thursday 11 October</th>
<th>Friday 12 October</th>
</tr>
</thead>
<tbody>
<tr>
<td>09.00-10.00</td>
<td>Course opening and Introduction of CEPOL and the WB FI Project</td>
<td>09.00-10.00</td>
<td>Intelligence led Investigations</td>
<td>09.00-10.00</td>
<td>Economic crime</td>
</tr>
<tr>
<td>10.00-11.00</td>
<td>&quot;Family Photo&quot; and Introduction</td>
<td>10.00-11.00</td>
<td>Preliminary investigations and Prosecutor led investigations</td>
<td>10.00-11.00</td>
<td>Tax Crime</td>
</tr>
<tr>
<td>11.00-11.30</td>
<td>Coffee Break</td>
<td>11.00-11.30</td>
<td>Coffee Break</td>
<td>11.00-11.30</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>11.30-12.30</td>
<td>From Money to crime or vice versa with Drug Trafficking</td>
<td>11.30-12.30</td>
<td>Joint Investigation Team(s)</td>
<td>11.30-12.30</td>
<td>Albanian speaking organised crime in the EU and Transatlantic</td>
</tr>
<tr>
<td>Time</td>
<td>Monday 08</td>
<td>Tuesday 09</td>
<td>Wednesday 10</td>
<td>Thursday 11</td>
<td>Friday 12</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>13.30-14.30</td>
<td>Example of Successful Action Plans, including National Drug Strategies</td>
<td>13.30-14.30 Joint Investigation Team(s)</td>
<td>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</td>
<td>13.30-14.30 OSINT and Darknet Investigations</td>
<td>Departure of participants</td>
</tr>
<tr>
<td>14.30-15.00</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
</tr>
<tr>
<td>15.00-16.00</td>
<td>Various forms of money laundering in Drug Trafficking</td>
<td>15.00-16.00 JIT case study</td>
<td>15.00-16.00 EUROPOL</td>
<td>15.00-16.00 Drug Markets on the Internet and Darknet</td>
<td></td>
</tr>
<tr>
<td>16.00-17.00</td>
<td>Discussion / workshop</td>
<td>16.00-17.00 Challenges in asset recovery: Discussion</td>
<td>16.00-17.00 EUROPOL</td>
<td>16.00-17.00 Cross cutting multidisciplinary challenges – discussion</td>
<td></td>
</tr>
<tr>
<td>19.00</td>
<td>Dinner</td>
<td>Dinner</td>
<td>Dinner</td>
<td>Dinner</td>
<td>Dinner</td>
</tr>
</tbody>
</table>
declaration of independence
Presence List of Participants

08-12 October Pristina Kosovo
Financial Investigation in Relation to Drug Trafficking
declaration of independence
This decision is without prejudice to positions on status, and is in line with UN SCR 1244/1999 and the ICJ opinion on the Kosovo
This document is without prejudice to positions on stages and is in line with UNSCR 1244/1999 and the ICJ Opinion on Kosovo.
Presence List of Participants

08-12 October Prishtina, Kosovo

Financial Investigation in Relation to Drug Trafficking
This designation is without prejudice to positions on status, and is in line with UN Security Council Resolution 1244/1999 and the ICJ Opinion on Kosovo.
Financial Investigation in relation to Drug Trafficking
8th to 12th 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.

<table>
<thead>
<tr>
<th>year</th>
<th>total</th>
<th>Albania</th>
<th>Kosovo</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>5145</td>
<td>777 (1)</td>
<td>4</td>
</tr>
<tr>
<td>2016</td>
<td>3804</td>
<td>699 (1)</td>
<td>4</td>
</tr>
<tr>
<td>2015</td>
<td>3261</td>
<td>600 (1)</td>
<td>2</td>
</tr>
<tr>
<td>2014</td>
<td>2339</td>
<td>449 (1)</td>
<td>3</td>
</tr>
<tr>
<td>2013</td>
<td>1745</td>
<td>268 (1)</td>
<td>0</td>
</tr>
<tr>
<td>5 year</td>
<td>16,294</td>
<td>2793 (17%)</td>
<td>13</td>
</tr>
</tbody>
</table>

1998 – 1999 significant migration, due to Kosovo War.
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.

Albanian Speaking organised criminals in the EU

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

Cocaine Supply
Cash Smuggling

Organised Immigration Crime

Heroin & Cannabis Trafficking
Cocaine market dominance

Significant Maritime Opportunity into Western Europe

UK market control

High Volume, High Quality
Established Transport
Strong Networks
Reliable Delivery
Large Workforce
Money Exchange / Smuggling
Highly Competitive Pricing
Reputation Generates Fear

UK cocaine kilogram prices, since Albanian Speaking OC

<table>
<thead>
<tr>
<th>Year</th>
<th>Albanian Speaking OC underside prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>£45,000</td>
</tr>
<tr>
<td>2013</td>
<td>£40,000</td>
</tr>
<tr>
<td>2014</td>
<td>£37,000</td>
</tr>
<tr>
<td>2015</td>
<td>£35,000</td>
</tr>
<tr>
<td>2016</td>
<td>£33,000</td>
</tr>
<tr>
<td>2017</td>
<td>£30,000</td>
</tr>
<tr>
<td>2018</td>
<td>£28,000</td>
</tr>
</tbody>
</table>
Financial Investigation in relation to Drug Trafficking

8th to 12th October 2018

Prishtina, Kosovo

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

Information
- Official Disclosure
  - Mr Anthony has applied for a visa for USA and Colombia
- Open Source
  - Mr Anthony is regularly in NW Spain with 'Facebook' pictures
- Sensitive Source
  - Mr Anthony is planning to import cocaine with associates

Intelligence
- International Partner
  - Mr Anthony is associating with a Dutch, Albanian & British Nominals
- Law enforcement
  - Mr Anthony is a close associate of the owner of a transport company
- Regulator or Agency
  - Mr Anthony has made numerous suspicious transactions

Numerous Opportunities
- Mobile phone billing
- Travel Agent
- Dates of Flights
- Hotel
- Travel companions
- Social Media
  - Photographs of travel companions in Spain
  - 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
Question: Which intelligence sources are working well for you?

Question: Which intelligence sources could work better for you?
Financial Investigation in relation to Drug Trafficking

8th to 12th October 2018

Prishtina, Kosovo

‘From Money to Crime or vice versa with Drug Trafficking’
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

Point of access determines outlay
Position in supply chain determines return
Combination incorporates risk and reward
All rely on volume cash access and audit free movement
Revenue and profit... UK example: 30 tons of cocaine

Criminal investment

Based on cocaine purchase in the primary markets (to the UK) in Latin America, Caribbean, Netherlands and Spain.

US$ 50 million
US$ 230 million
€ 540 million
€ 690 million

Wholesale market

Value £700 - £900 million
Profit £150 - £500 million

Kilogram deals

Mid-market

Value £1.7 billion
Profit £880 million

UK Import
30 tonnes

Retail market

Value £2.4 billion
Profit £700 million

Gram deals

Ounce (28 grams) deals

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
Financial Investigation in relation to Drug Trafficking
8th to 12th 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
This does not have to happen, it is a ruthless criminal choice to exploit other human beings.
“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”.
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
Financial Investigation in relation to Drug Trafficking

8th to 12th 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

The market before legislation: Open, audit trails, traditional

Pre-2016

Street dealers → cash

Internet → online company → card payments → Postal service

Shops → cash

The market after legislation: Closed, hidden, crypto, modern

Psychotropic Substances Act 2016

Street dealers → cash

Smart Phone Apps Messenger Groups

Darknet → Encrypted Vendor → Crypto Currency → Postal service

Social Media

What is 'online'? Where are the opportunities?
Three substances of particular legal interest

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.
High Level Vendors, Markets & Opportunities

Oppunities:
1. Identify high profile ‘cult status’ vendors and target their high frequency/volume activity.
2. Locate their ‘crypto wallet’. At some stage their crypto currency will be accessed and converted to conventional proceeds.
3. Conduct mail scanning (with dogs) and profiling, at hubs identified as servicing customer hotspot areas.
4. Monitor and engage in online forums, to understand the market.

Challenges:
1. The drug market forms a part of the Darknet platform and NPS only a part of that market. This is initially a Cyber enabled, not drugs challenge.
2. Messages between vendor and customers are becoming increasingly encrypted.
Mechanisms for Control of NPS

Psychotropic Substances Act 2016

Prohibition Notice
- Police Warning
- Prohibition Order
- Court Warning
- Court
- Prison or Fine
- Maximum 12 months

Premises Notice
- Premises Order
- Court

Internet Trader
- Letter to cease from national police
- Police apply to national domain name provider
- Present evidence of online supply
- Breach of terms and conditions
- Removal of 'main name' from internet
- Website invisible and unsearchable

Powers:
- Search
- Enter
- Seize
- Arrest

Border Force
- Airports
- Seaports
- Ferry Terminals
- Parcel Centres

OFFICIAL USE ONLY
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
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.
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.
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.
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’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'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'. 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.
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.
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.
Following a build-up phase of three years, the EPPO is envisaged to take up its functions by the end of 2020.
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.
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.
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.
The EPPO will be built on two levels: the central and the national level.
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.
The decentralised level will consist of European Delegated Prosecutors who will be located in the participating Member States.
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.
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.
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 to serve 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

Volume

Variety

Veracity

Velocity

Data volume is growing at present; need to evaluate.

Data variety is a key factor.

Data is veracity is under consideration.

Data is velocity is high.

Data is veracity is still a problem.

Data is velocity is high.

Data is variety is high.

Data is volume is growing.


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.
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

INFographic INFographic

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
- 24/7 monitoring
- Continuous cataloging of targets
- Continuous study of variation of the targets
- Extrapolation and memorization of data
- Organization and analysis of data (automatic and human)
- Timely reaction to events (automatic and human)
Tor
- The onion routing
- http://thetorproject.org/
- http://hpz27id2v5sigw36.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
Tools

- OPEN SOURCE INTELLIGENCE TOOLS AND RESOURCES HANDBOOK


CEPOL

Terrorist use of Internet (and Darknet)
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 activities, and the locations of its leader for up to a month prior to the day of their planned bombing attack.


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_reports/RR4420R
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.

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)


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 terrorist organizations;
  2. Linking/friendship to other profiles with ideological affinity, participating to thematic groups;
  3. Strengthening relationships/friendships with radicals, 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.
New York woman charged with sending $85,000 in Bitcoin to support ISIL

By Becky Anderson

A New York woman has been charged with sending $85,000 in Bitcoin to support ISIL.

Zahra Shahira, 52, was arrested after a ten-month investigation by the New York Police Department. She is accused of violating the USA PATRIOT Act.

The investigation began after a tip-off to the Federal Bureau of Investigation (FBI) about Shahira's activities.

She is due to appear before a magistrate judge in Brooklyn on Thursday.

The arrest is the latest in a series of arrests of people suspected of supporting or affiliating with ISIL.

FBI agents said Shahira used Bitcoin to send money to ISIL supporters in Syria.

1. Got a call from my bank to check my account.
2. 2. I used to buy drugs, but now I buy drugs.
3. Donald Trump says in rally speech on national referendum in Britain.
4. Syrian men don't stand up! I will never leave.
5. Fighting against the US crime in Syria, and against the American occupation.
The digital disruption supporting new criminal models

- Most popular media owner creates no content (Facebook)
- Fastest growing banks have no actual money (SocieteOne)
- Largest accommodation provider owns no real estate (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)

IT based crimes don't require IT sk
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
Half-year licence: $800
3-month licence: $700

Update domain: $50
Changing domain: $20 multi-domain $200 to license.
During the terms of the license all the updates are free.

Rent on our server:

1 week (7 full days): $100
2 weeks (14 full days): $300
3 weeks (21 full days): $600
4 weeks (28 full days): $800
24-hour test: $50

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

Providing our proper domain included. The subsequent change of the domain: $95
Unfamous botnet usage

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

IP
- 91.225.158.103
- 37.238.161.115
- 37.235.304.157
- 37.239.348.27
- 37.17.128.64
- 37.230.176.71
- 37.238.29.27
- 37.239.76.68
- 62.201.202.109
- 37.239.84.193
- 37.237.136.208
Domain generation algorithms (linguistic analysis)

Meaningful Word Ratio (English dict)

\[ R(d) = \frac{|\text{facebook}|}{|\text{facebook}|} = 1 \quad R(d) = \frac{|\text{pub}|}{|\text{pub3ast1}|} = 0.375. \]

likely non-DGA generated    likely DGA generated    N-gram Popularity (English dict)

Filtering

- A malicious domain does not become "Popular". We then filter by index of popularity (Alexa 1M white list)
- We filter the domains that refer to a CDN (names too "dirty" that could generate false positives)
- We filter for tcp level domains that have not allow abusive registrations (.gov, .edu, .mil, ...)
- Filter for response times (TTL)
  + Filter by "d delay" (now (i - registered Date (i))
- 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 CON
  - 800 have a DGA-Gan factor
  - 700 are not controlled domains (e.g., gov)
  - 300 are younger than "A days"

Suspects!

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;
  - poleon 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.


Research findings (2017)

<table>
<thead>
<tr>
<th>Variable</th>
<th>p-Wala</th>
<th>Sig.</th>
<th>%</th>
<th>Odds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Learning (Extreme Right)</td>
<td>5.952</td>
<td>0.015</td>
<td>78.1</td>
<td>3.390</td>
</tr>
<tr>
<td>Planted Attack</td>
<td>4.308</td>
<td>0.041</td>
<td>69.9</td>
<td>2.719</td>
</tr>
<tr>
<td>Government Support</td>
<td>4.309</td>
<td>0.038</td>
<td>81.3</td>
<td>4.506</td>
</tr>
<tr>
<td>Global Economic Event</td>
<td>7.806</td>
<td>0.005</td>
<td>100.0</td>
<td>—</td>
</tr>
<tr>
<td>RDD Attack</td>
<td>16.724</td>
<td>0.000</td>
<td>71.5</td>
<td>3.148</td>
</tr>
<tr>
<td>Armed Assault</td>
<td>5.095</td>
<td>0.015</td>
<td>63.7</td>
<td>5.085</td>
</tr>
<tr>
<td>Unarmed Assault</td>
<td>4.952</td>
<td>0.018</td>
<td>4.0</td>
<td>—</td>
</tr>
<tr>
<td>Acted With a Cell</td>
<td>6.209</td>
<td>0.012</td>
<td>50.5</td>
<td>1.287</td>
</tr>
<tr>
<td>Attempts to Recruit Others</td>
<td>7.907</td>
<td>0.006</td>
<td>84.2</td>
<td>6.029</td>
</tr>
<tr>
<td>Reduction of Network Activity</td>
<td>17.487</td>
<td>0.000</td>
<td>79.2</td>
<td>4.100</td>
</tr>
<tr>
<td>Residual/Fish Interaction</td>
<td>13.747</td>
<td>0.000</td>
<td>22.1</td>
<td>3.116</td>
</tr>
</tbody>
</table>

Note. — = Odds calculated because of complete lack of variance.

Planning

- A recent case from France, Public Prosecutor v. Hicheur, 15 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 Muhajideen Secrets (Aesar al-Muhajideen) encryption software launched in 2007, primarily for use with email. Aesar has had multiple releases over time and is distributed by the Global Islamic Media Front.

Anea 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.

Aesar al-Arsadah, released by GIMF in February 2018, which is an encryption plugin for instant messaging based on the Plugin platform – which connects to major US-based platforms.

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

Aesar al-QamarBay is yet another alternative encryption program, however importantly, released in November 2018 by Daesh, which coincides with Daesh breaking off from main AQ after a power struggle.

conclusions

- Today Daesh is more interested in play Information warfare rather than to cyberattack
- Not clear the size of Daesh militant involved in cyber activity (ISB has 6 recognized guys)
- Cyber side of terrorism is more complicated to analyze due to anonymity tools and trolls (complicating PSYOPS and Information warfare techniques)
- Hacktivist alliances represent one of the phenomenon decoding keys
- Media focus attention on communication hacks en 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 traffic)
- Steganography and Cryptography WW2 Enigma machine docat....
**conclusions**

“A wealth of information creates a poverty of attention”

Herbert Simon

(1916–2001, political scientist, economist)

| 1,000,449,461 | 1,000,449,461 |
| 1,000,449,461 | 1,000,449,461 |
| 1,000,449,461 | 1,000,449,461 |
| 1,000,449,461 | 1,000,449,461 |
| 1,000,449,461 | 1,000,449,461 |
| 1,000,449,461 | 1,000,449,461 |
| 1,000,449,461 | 1,000,449,461 |

http://www.internetresearch.net/
Tor & Marketplaces statistics

Market List With Up & Down

Top Markets
- Up / Online: Dream Market 28,393.2
- Up / Online: Points / Free Market - 89.771.6
- Up / Online: Heartbound Market - 89.019.4

Other Markets
- Up / Online: Dream Market 28,393.2
- Down / Online: Points / Free Market - 89.771.6
- Down / Online: Heartbound Market - 89.019.4

Other Markets
- Up / Online: Dream Market 28,393.2
- Down / Online: Points / Free Market - 89.771.6
- Down / Online: Heartbound Market - 89.019.4

- Up / Online: Dream Market 28,393.2
- Down / Online: Points / Free Market - 89.771.6
- Down / Online: Heartbound Market - 89.019.4
### Market List With Up & Down

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Company Name</th>
<th>Sector</th>
<th>Type</th>
<th>Size</th>
<th>Price Change</th>
<th>% Change</th>
<th>Bid</th>
<th>Ask</th>
<th>Spread</th>
<th>urnor</th>
<th>Year</th>
<th>Date</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC</td>
<td>ACME Corp</td>
<td>Tech</td>
<td>Equity</td>
<td>1000</td>
<td>10.50</td>
<td>1.0%</td>
<td>10.20</td>
<td>10.70</td>
<td>0.50</td>
<td>Inc.</td>
<td>2020</td>
<td>02/12/2019</td>
<td>Note</td>
</tr>
<tr>
<td>XYZ</td>
<td>BRAVO Group</td>
<td>Retail</td>
<td>Equity</td>
<td>5000</td>
<td>25.80</td>
<td>0.5%</td>
<td>25.60</td>
<td>26.00</td>
<td>0.40</td>
<td>Inc.</td>
<td>2018</td>
<td>01/30/2018</td>
<td>Note</td>
</tr>
<tr>
<td>GIK</td>
<td>DELTA Systems</td>
<td>Energy</td>
<td>Equity</td>
<td>8000</td>
<td>35.75</td>
<td>2.5%</td>
<td>34.75</td>
<td>36.00</td>
<td>1.25</td>
<td>Yes</td>
<td>2019</td>
<td>03/15/2019</td>
<td>Note</td>
</tr>
<tr>
<td>JKL</td>
<td>LUMINA Corp</td>
<td>Finance</td>
<td>Equity</td>
<td>3000</td>
<td>18.25</td>
<td>1.0%</td>
<td>18.00</td>
<td>18.50</td>
<td>0.50</td>
<td>Inc.</td>
<td>2017</td>
<td>05/10/2017</td>
<td>Note</td>
</tr>
</tbody>
</table>

**CEPOL**

---

### Market List With Up & Down

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Company Name</th>
<th>Sector</th>
<th>Type</th>
<th>Size</th>
<th>Price Change</th>
<th>% Change</th>
<th>Bid</th>
<th>Ask</th>
<th>Spread</th>
<th>urnor</th>
<th>Year</th>
<th>Date</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNO</td>
<td>OMEGA Corp</td>
<td>Health</td>
<td>Equity</td>
<td>4000</td>
<td>12.50</td>
<td>0.0%</td>
<td>12.40</td>
<td>12.60</td>
<td>0.20</td>
<td>Inc.</td>
<td>2020</td>
<td>02/12/2019</td>
<td>Note</td>
</tr>
<tr>
<td>PQR</td>
<td>QUANTUM Corp</td>
<td>Energy</td>
<td>Equity</td>
<td>7000</td>
<td>22.75</td>
<td>1.5%</td>
<td>22.50</td>
<td>23.00</td>
<td>0.50</td>
<td>Yes</td>
<td>2018</td>
<td>01/30/2018</td>
<td>Note</td>
</tr>
<tr>
<td>RST</td>
<td>SOLAR Corp</td>
<td>Tech</td>
<td>Equity</td>
<td>6000</td>
<td>30.50</td>
<td>2.0%</td>
<td>30.25</td>
<td>30.75</td>
<td>0.50</td>
<td>Inc.</td>
<td>2019</td>
<td>03/15/2019</td>
<td>Note</td>
</tr>
<tr>
<td>TUV</td>
<td>NODA Corp</td>
<td>Finance</td>
<td>Equity</td>
<td>3500</td>
<td>15.25</td>
<td>0.0%</td>
<td>15.20</td>
<td>15.30</td>
<td>0.10</td>
<td>Inc.</td>
<td>2017</td>
<td>05/10/2017</td>
<td>Note</td>
</tr>
</tbody>
</table>

**CEPOL**

---

26
Market List With Up & Down

Average prices

<table>
<thead>
<tr>
<th>Drug</th>
<th>Average prices (EUR) per drug unit (g/tablet)</th>
<th>Examples from five national darknet markets</th>
</tr>
</thead>
<tbody>
<tr>
<td>THC 2.0 (Ind)</td>
<td>10.3</td>
<td>30.00</td>
</tr>
<tr>
<td>20.00</td>
<td>17.7 (4.7)</td>
<td></td>
</tr>
<tr>
<td>Caffeine</td>
<td>7.7 (3.3)</td>
<td>8.2</td>
</tr>
<tr>
<td>Heroin</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Cocaine</td>
<td>85.0 (6.7)</td>
<td>22.0</td>
</tr>
<tr>
<td>Amphetamine</td>
<td>60.0 (5.5)</td>
<td>10.0</td>
</tr>
<tr>
<td>MDMA</td>
<td>52.0 (4.0)</td>
<td>5.2</td>
</tr>
<tr>
<td>LSD</td>
<td>110.0 (4.7)</td>
<td>17.1</td>
</tr>
</tbody>
</table>
### Drug data categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannabis, heroin, cocaine products (e.g., resin, extract, crystals)</td>
<td>Drug paraphernalia, drug related goods, airmail and seized products, counterfeit products, and other</td>
</tr>
<tr>
<td>Quaaludes, ketamine, amphetamine</td>
<td>Substance use issues (prescription, overuse) and related goods, airmail and seized products, and other</td>
</tr>
<tr>
<td>Marijuana, synthetic cannabinoids, and related goods</td>
<td>Substance use issues (prescription, overuse) and related goods, airmail and seized products, and other</td>
</tr>
<tr>
<td>Ecstasy, MDMA</td>
<td>Substance use issues (prescription, overuse) and related goods, airmail and seized products, and other</td>
</tr>
<tr>
<td>Hallucinogens (e.g., PCP)</td>
<td>Substance use issues (prescription, overuse) and related goods, airmail and seized products, and other</td>
</tr>
<tr>
<td>NPS</td>
<td>Substance use issues (prescription, overuse) and related goods, airmail and seized products, and other</td>
</tr>
</tbody>
</table>

### 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

![CEPOL Logo]
Key findings

- The trade in illicit drugs on darknet markets is a dynamic area subject to rapid change as marketplaces appear and disappear. Overall, the importance of this area seems to be expanding and it now affects most EU Member States in some way.
- When compared with current estimates of the annual retail value of the overall EU drug market, sales volumes on darknet markets are currently modest, but are significant and have the potential to grow.
- EU-based suppliers are important players in the darknet ecosystem. In the 2011-2015 period, they accounted for around 48% of all drug sales in terms of revenue on the darknet markets analysed.
- Between 2015 and 2017 on AlphaBay, which, at the time, was the largest darknet marketplace, EU-based suppliers accounted for around 28% of all drug sales.
- In both study periods Germany, the Netherlands and the United Kingdom were the most important countries with respect to EU-based darknet drug supply. Stimulant drugs represented the majority of all European drug sales.
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.
Revenue 2011-2015

Revenue and weight analysis of drug sales originating from the EU, Norway and Turkey by country, 2011-2015

Sales 2011-2015

Breakdown of sales revenues originating from the EU, Norway and Turkey by country, 2011-2015
Revenue 2011-2015

Drug sales

Comparison of drug sales in the EU and the rest of the world, 2011-2015
Breakdown of daily NPS sales originating from the EU, Norway and Turkey.
Tor Marketplaces

BLACK MARKETS
ONLINE MARKETPLACES

(Anonymous Net) Tor | Cryptocurrency | WOT based cryptography

Anonymous/Relaying 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, counterfeit documents, and components for further criminality.
**IOCTA 2017**

- Sale of illicit goods to dedicated criminal websites and markets hosted on anonymizing 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

![Graph showing Tor users over time](https://tormetrics.torproject.org/)
Tor USERS
The anonymous Internet

Darknet
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.
- Most of 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 interface nor a reputation or escrow system. Trusted members of the community may act as escrow agents.

- **Centralized Markets.** The original "Silroad" 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 heists 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 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.

<table>
<thead>
<tr>
<th>Nucleus Market</th>
<th>Dream Market</th>
<th>AlphaBay</th>
</tr>
</thead>
<tbody>
<tr>
<td>marketrepo.onion</td>
<td>Lacebikers5ly.onion</td>
<td>Invite (Required)</td>
</tr>
<tr>
<td>Forum</td>
<td>Forum</td>
<td>Forum</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outlaw Market</th>
<th>Agora Marketplace</th>
<th>Abraxas Market</th>
</tr>
</thead>
<tbody>
<tr>
<td>twistweb</td>
<td>twistweb</td>
<td>smallonion</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>East India Company Market</th>
<th>Babylon (Italian)</th>
</tr>
</thead>
<tbody>
<tr>
<td>marketrepo.onion</td>
<td>Invited 2nd onion</td>
</tr>
</tbody>
</table>
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

Categories and product offers in Alphabay
Categories and product offers in dream market

- Digital Goods 29824
  - Data 909
  - Drugs 340
  - E-Books 667
  - Software 2146
  - Fraud 1754
  - Fraud Related 227
  - Hacking 144
  - Information 9126
  - Other 216
  - Security 164
  - Software 617

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 (signals).
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 declaring the "Finalized
    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., 8THWonder)

"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 enhancing 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,
Lolnet 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 drug revenue of the top eight Darknet markets ranges between EUR 10.6 million and EUR 19.7 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 90% of shipments get through.

Identity theft

- The introduction of forged documents.
- Increasingly sophisticated security features protecting documents against forgery as well as improved technical control measures have compelled CCAs to improve the quality of fraudulent documents.
- Suppliers of raw materials now primarily rely on Darknet marketplaces to sell their products.
Counterfeited goods (Iocta 2017)

- Infringements of intellectual property rights (IPR) are a widespread and ever-increasing worldwide phenomenon. In 2015, 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.* 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.

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?
Counterterrorism on TOR

- Why Counterterrorism investigations pass through TOR?

BOTNET AD FRAUD WILL NET CRIMINALS $7.2 BILLION IN 2016

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 $10m-17m in 2012 to $150m-160m in 2015.
- The share of American drug-takers who have got high with the help of a website jumped from 6% 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 marketplaces 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.