Questions - Responses et fin de session.
16:00
14:15
14:00
13:45
13:00
12:00
11:15
11:00
10:45
10:30
09:00
08:00
Prière en charge de la délégation CEPOL et des experts à leur hôtel.

Lundi 22 Avril

Questions - Responses et fin de session.
16:00
14:15
14:00
13:45
13:00
12:00
11:15
11:00
10:45
10:30
09:00
08:00
Prière en charge de la délégation CEPOL et des experts à leur hôtel.

Dimanche 21 Avril

Arrive de la délégation des experts CEPOL, suivant différents lignes de horaires.

Samedi 20 Avril

Expects:

CEPOL:

Fondamentaux

Le contenu du cas sessions a ete developpe dans le respect de la loi et des droits

Dimanche 21 Avril - Jeudi 25 Avril 2019

ZerEDI/Alger. Algérie
École Supérieure de la Gendarmerie Nationale
"OSINT, DIA, EITI, et technicues d'investigation"
Activité Restitutive
EU/Algérie - Partenariat Constance-Terrorisme

This project is funded by the European Union
nos hôtels-agences.

Départ de la délégation des experts vers l'aéroport (à organiser au cas par cas avec

Vendredi 26 Avril

16:00 Fin de la visite résidentielle.
15:00 Déjeuner du déjeuner - Remise des certificats.
14:00 Évaluation de la visite résidentielle.
13:00 Réception des Professionnels sur Internet.
12:00 Repas de midi.
11:00 Évaluation des Professionnels sur Internet.
10:45 Break le ou café.
09:00 Évaluation des Professionnels sur Internet.
08:00 Pique-nique et change de la délégation CEPO et des experts à leur hôtel.

Jeudi 25 Avril

16:00 Questions - Réponses et fin de session.
14:15 Danse IV.
14:00 Break le ou café.
13:00 Danse III.
12:00 Repas de midi.
11:00 Danse II.
10:45 Break le ou café.
09:00 Danse I.
08:00 Pique-nique et change de la délégation CEPO et des experts à leur hôtel.

Mercredi 24 Avril

16:00 Questions - Réponses et fin de session.
14:15 Animé CDR et la grande échelle commune, j'illustretr mobile IV.
14:00 Break le ou café.
13:00 Animation CDR et la grande échelle commune, j'illustretr mobile III.
12:00 Repas de midi.
11:00 Animation CDR et la grande échelle commune, j'illustretr mobile II.
10:45 Break le ou café.
09:00 Animation CDR et la grande échelle commune, j'illustretr mobile I.
08:00 Pique-nique et change de la délégation CEPO et des experts à leur hôtel.

Mardi 23 Avril
| N°  | Nom & Prénom | Grade  | Lieutenant | Commandant | Commandant | Commandant | Commandant | Commandant | Commandant | Commandant | Commandant | Lt/Colonel | Lt/Colonel | Lt/Colonel | Lt/Colonel |
|-----|--------------|--------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|
| 20  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 19  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 18  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 17  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 16  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 15  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 14  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 13  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 12  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 11  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 10  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 09  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 08  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 07  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 06  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 05  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 04  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 03  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 02  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
| 01  |              |        |            |            |            |            |            |            |            |            |            |            |            |            |            |
OSINT Stream

1. Information (photo) validation
2. Technical OSINT (SHODAN/Censys)
3. Technical OSINT (Wigle)
4. Instagram OSINT
5. Airport OSINT (using Instagram)
6. Social media gathering
Photo validation

How to verify pictures/photo’s.

How to get started?

Make sure you use good tools or add-ons

A lot of false information involves old images taken out of context.

Start with a reverse image search. Insert the picture in one or several search engines to see if it has previously appeared online.
The RevEye browser extension is interesting to use. This gives you the choice of image search engines like Google, Yandex, Bing, TinEye and Baidu.

Images or videos alone are never proof of a statement.

Via:
https://whopostedwhat.com/
you can look for posts on Facebook at a certain date or specific keyword.
Investigating videos

Fake video news debunker by InVID

This Chrome extension is used to cut a video in separate thumbnails and then reverse image search.

Wayback

Via the wayback machine you can go back in time. And look at content at a specific date. You can also debunk information with the help of the wayback machine.
Where is this?

- This is one of the terrorists who drove into the crowd with a van in Sweden.
- A friend of him made this picture and posted it via social media online.
- When looking with reverse image search it came back at a Facebook profile.
- He didn’t tag it and also didn’t gave it geo information.

- Probably C, D and E looks like a airport.
- The bear is yellow. And because searching via uploading the picture wasn’t bringing us further, we did something different.
We needed to tell Google very clearly what we see. A airport, a yellow bear and of course we needed to tell Google that the photo must be yellow.

Shodan tutorial

Het vliegveld is in Doha, Qatar
What is Shodan?

Shodan is a search engine for finding specific devices, and device types that exist online. The most popular searches are for things like webcam, linksys, cisco, netgear, SCADA, etc.

It works by scanning the entire internet and parsing the banners that are returned by various devices. Using that information Shodan can tell you things like what web server (and version) is most popular, or how many anonymous FTP servers exist in a particular location, and what make and model the device may be.

Basics

You start by going to the main page. Then entering into the search field, like you would any other search engine.

For this search, I looked for "VNC"
From there you can pivot to a few key areas in the results. Starting on the left sidebar, we see a good amount of summary data:

- Results map
- Top services (Ports)
- Top organizations (ISP's)
- Top operating systems
- Top products (Software name)

Then in the main section we get the full results list, including:

- IP address
- Hostname
- ISP
- When the entry was added to the database
- The country it's located in
- The banner itself
Then, for even more information you can click details, which takes you into that host itself.

Here you see the data about the host on the left, the list of ports that were found at the top right, and then the individual port details and banners from each port as you go down the page. It's a clean layout.

Filters
As with any search engine, Shodan works well with basic, single-term searches, but the real power comes with customized queries.

Here are the basic search filters you can use:

- city: find devices in a particular city
- country: find devices in a particular country
- geo: you can pass it coordinates
- hostname: find values that match the hostname
- net: search based on an IP or CIDR
- os: search based on operating system
Find GWS (Google Web Server) servers:
  "Server: gws" hostname:"google"

Find Nginx servers in Germany:
  nginx country:"DE"

Find Cisco devices on a particular subnet:
  cisco net:"216.219.143.0/24"

Find Apache servers in San Francisco:
  apache city:"San Francisco"

So you basically have some sort of base search term you're looking for (shown in orange) and then you narrow down your search using the filters like we see above.

Use cases

You can use the "Explore" button on the main Shodan site to look at common searches and results, which are illuminating. You'll find things like:

1. Webcams
2. SCADA
3. Traffic lights
4. Routers
5. Default passwords
Combining filters

To combine filters, simply keep adding them on. You can also do this by clicking filters in the left sidebar for a given result set. So if you want to search for **Nginx** servers in **San Francisco**, that are running on **port 8080**, that are also running **Tomcat**, **Apache** or **Shindigo** port **8080** product **Apache Tomcat/Coyote JSP engine**.
OSINT techniques
Let's take a deep(er) dive into different techniques and tools used to make your OSINT work worthwhile.

Wigle
Let's take a deep(er) dive into different techniques and tools used to make your OSINT work worthwhile.
Wigle

Who already know’s Wigle and uses it??

WIFI Threats

Our machines are probing all day long where we are. This is a dangerous thing. Let's take a look at your probing phone as a hotspot.
Tracking via WIFI

Some explanations:
MAC = unique address from a device which identifies itself in this way
SSID = the network name (Service Set identifier)
BSSID = the MAC address from the access point (Basic Service Set Identifier)
WiGLE zoomed in

WiGLE WIFI test
**WiGLe test**

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Primary Key</th>
<th>Frequency</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property 1</td>
<td>Type 1</td>
<td>Primary Key 1</td>
<td>Frequency 1</td>
<td>Value 1</td>
</tr>
<tr>
<td>Property 2</td>
<td>Type 2</td>
<td>Primary Key 2</td>
<td>Frequency 2</td>
<td>Value 2</td>
</tr>
<tr>
<td>Property 3</td>
<td>Type 3</td>
<td>Primary Key 3</td>
<td>Frequency 3</td>
<td>Value 3</td>
</tr>
</tbody>
</table>

**Map Diagram:**

- Den Haag location

---

**Strategic Contra**
Instagram

Part of Facebook and Whatsapp. Very popular in Europe.

In Algeria Instagram is becoming more popular also. And in Algeria there is also a la are showing their message

Instagram

Instagram is used by a lot of people. And also criminals.

In Europe we see a vast amount of criminal activities...
Let's get over to my PDF from the case..
Social media gathering

GOOGLE DORK

DEEP WEB
What is Google Dorks?

Let’s start with definition of “dorks”

A Google dork is an employee who unknowingly exposes sensitive corporate information on the Internet. The word dork is slang for a slow-witted or in-apt person.

Margaret Rouse
Director, WhatIs.com at TechTarget
@WhatIsDotCom
THE PURPOSE OF DORKS QUERIES

WHAT
Google dorks is a powerful advanced search, an instrument to perform queries on Google search engine.

HOW
That queries allow the user to find detailed information over the internet, such files, hidden pages, sensitive documents and so on.

WHY
But...dork queries are considered by many an "hacking technique". Because of his nature, the dorks can be used for different purposes, often bad purpose and we shall then see...

Dorks queries
Queries syntax, special characters and operators.
**SPECIAL CHARACTERS**

- **Star (**)**: Substitution with any other word in the query.
- **Tilde (~)**: Also research synonyms of that word.
- **Minus (-)**: Remove that word from the research.

**OPERATORS**

- **inurl**: Find that word or sentences in the URL.
- **intitle**: Find that word or sentences in the title of a website.
- **related**: Find that related websites.
- **site**: Specify to a specific site.
- **filetype**: Research by file type.
### Other Operators from Wikipedia

<table>
<thead>
<tr>
<th>Operator</th>
<th>Purpose</th>
<th>Mixes with Other Operators?</th>
<th>Can be used Alone?</th>
<th>Web</th>
<th>Images</th>
<th>Groups</th>
<th>News</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>site</code></td>
<td>Search page site</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><code>allsite</code></td>
<td>Search page site</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><code>intitle</code></td>
<td>Search title</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><code>allintitle</code></td>
<td>Search title</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><code>inurl</code></td>
<td>Search URL</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><code>allinurl</code></td>
<td>Search URL</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td><code>intext</code></td>
<td>Search text of page only</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><code>allintext</code></td>
<td>Search text of page</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><code>intitle</code></td>
<td>Search specific site</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td><code>allintitle</code></td>
<td>Search specific site</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><code>link</code></td>
<td>Search for links to pages</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td><code>manchur</code></td>
<td>Search link anchor text</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><code>numrange</code></td>
<td>Locate number</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><code>daterange</code></td>
<td>Search in date range</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td><code>author</code></td>
<td>Group author search</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td><code>group</code></td>
<td>Group name search</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><code>subject</code></td>
<td>Group subject search</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>like</td>
<td>like</td>
<td>like</td>
</tr>
<tr>
<td><code>msgid</code></td>
<td>Group msgid search</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>not really</td>
<td>not really</td>
<td>yes</td>
</tr>
</tbody>
</table>

**Queries examples**
This presentation is meant for educational purposes only.
Google Hacking Database - Exploit Database

The Exploit Database is maintained by Offensive Security, an information security training company that provides various Information Security Certifications as well as high end penetration testing services. Categories of dork queries by GHDB:

- Footholds
- Files Containing
  - Usernames
- Sensitive Directories
- Web Server Detection
- Vulnerable Files
- Vulnerable Servers
- Error Messages
- Let's see those underlined...

- Files Containing Juicy Info
- Files Containing Passwords
- Sensitive Online Shopping Info
- Network or Vulnerability Data
- Pages Containing Login Portals
- Various Online Devices
- Advisories and Vulnerabilities

List of pastes (username and password). Check your email status on haveibeenpwned.com by Troy Hunt.
In this case, the **star character** have been changed with "fc" and "it" domain in the first one, and "tn" and "it" for the second one.

comune means municipality, district.
Sensitive directory example

Google

The following folders probably contains sensitive data:

- Index of /admin/uploads
- Index of /media
- Index of /uploads
- Contact/
Conclusion

Actually the best way to protect us against Google hacking, is to test our website to figure out what could harm us, then patch/fix/remove the problem if possible.

As we can see, it's not difficult to find sensitive folders or file over the network. Because of his simplicity, security skills are not required to steal information.

Be careful and protect your data!

How to find usernames rapidly?

https://github.com/sherlock-project/sherlock
Thank you for your attention!
Who am i?

OSINT ANALYST
- CEH (Certified Ethical Hacker)
- OSINT Pathfinder, Bellingcat, Dutch Police Academy
- "Lives" OSINT
- Trainer (OSINT, digital awareness)
OSINT stream today
1. Introduction
2. Operational security (opsec)
3. Documenting
4. Preparation of the workplace
5. OSINT Techniques part 1
6. CTF lab
7. OSINT Techniques part 2
8. CTF lab
9. Questions
As of October 2018, there are more than 1.9 billion websites on the Internet.

Did you know?
Welcome to the Netherlands
sometimes called SOCOMINT for SOCIAL Media INTELLIGENCE

- social media

"CIA: information does not have to be secret to be valuable"

- open:
  - refers to open, publicly available sources (as opposed to covert or clandestine sources)
  - one of many forms of 'INT' (SIGINT, HUMINT, etc)

requirement

exploration and reporting to address a specific intelligence need

from publicly available information that is collected

WHAT IS OSINT?
What is OSINT?

But basically, EVERYONE

• Authors
• Businesses
• Law Enforcement
• Private Investigators
• Information Security

Where professionals can leverage OSINT data?
- Verification of information you've collected
- Spies only tell secrets, you do not (most of the time) need secrets
- Over information and accessible for everyone

Why does LE use OSINT?

Robert Steele

Time

being on guard, open, all the intelligence information and turning over citizen info on...

Ultimately OSINT is about networks

entire power and communications and water individuals each capable of shutting down

more and more social disconnection

loss about state on the military power and is in relation to the new reality that war is another area where OSINT is fundamental
The OSINT process | 6 categories

1. Media: Print newspapers, magazines, radio and television.
2. Internet: Online publications, blogs, discussion groups, social media.
3. Public government data: Chamber of commerce, bankruptcy data.
4. Professional and academic publications: Academic papers.
5. Commercial data: Commercial imagery, databases, financial assessments.
Types of OSINT

1. Non-technical: basically making use of the internet and other open sources without difficult technical knowledge.

2. Social media OSINT

3. Technical OSINT: doing reconnaissance and search for IP addresses, DNS information, port scanning etc.
1. Tools: what tools are needed?
2. Sources: what sources am I going to use?
3. Research machine: what research machine am I going to use?
4. Adversary: who is my adversary?

Operational Security (Opsec)
1. Adjust activities to threat level
2. Residential Internet or 4G/LTE?
3. Proxy/VPN or TOR?
4. Referrer on/off?
5. User agents
6. Tracking blockers?
7. Do not log in with a (fake) account in Google, Yahoo etc..
8. What is the risk if an account gets compromised? (connection with other accounts?)

Fingerprint by correlation
1. Browser fingerprinting
2. IP fingerprinting
3. Time online or timezone settings
4. Choice of words
5. Behavior (browser habits/patterns)
Think before you act

1. No linking (in anyway possible) to your personal identity. Work and private 100% separated.
2. Stay away from your private environment
3. No office WIFI / ethernet
4. No office terminal for online research
5. No connecting or linking to your private devices

Blend in

- Study how you should manifest on a certain platform
- What is your story? (alibi)
- Look Alive!
- When online, prevent 9-5 hours
- Language settings
- Time zone
- Choice of words (slang, professional)
But what if someone is listening...
Man in the middle - the theory

What can we detect?
Man in the Middle
Man in the Middle with SSL
Man in the Middle with SSL

dashboard (for skiddies)
Password manager

Do you use a password manager?
- Easy to use
- Different passwords for accounts
- Cloud availability

Fingerprinting

Go to http://webkay.robinlinus.com/
What does your browser reveal about the system you are using? Or go to: https://www.whoer.net
Considerations

- Weeks? Months? Hours?
- Time frames for collection
- Duplicate data (same phone, multiple people)
- Sensitive data

Types of OSINT Data

- Text
- Web pages
- Downloads
- Videos
- Images

Tool output
- Command Line
- Dates/Times
- URLs
- Analyses
Considerations

- Cloud storage versus local storage/intranet
- Multi user Apps versus single...

Number of team members

- How many people will contribute?
- Just you?
- Team, geographical spread
- Enterprise?
Who do you want to be? => VPN/Proxy etc.
Are you making use of smartphones to do research?
What kind of distribution do you want to use?
Do you want to work with a virtual machine?
What kind of machine do you use? Windows, Linux, MacOS?

Preparing your workplace
Some are multi-user
Embed images and documents
Visual note-taking

Mindmaps

Let's focus!

Easiest to use
Most complete features
Most flexible
Hunchly
- Passively extracts data
- Automated recording of browsing
- Time-lining
- Hashing of images
- Downloaded files included
- Google Chrome extension
- Not expensive \$130/year

Mindmap con's
- Not always easy to look back in time
- Exporting the data isn't easy, especially with free mode
- Manual data entry process
So, if you know
What kind of software do you use?

- Excel
- R
- Python
- Spreadsheets (open source applications)
- Other tools (e.g., Excel)

Some other tools you might consider:

- Many apps have tasks or are free
- And work because you learn to do
- Find document tools that make things easier

Then
How to get started?

Go to cedate with your Gmail addresses. Each team has an address.

Then download the mindmapping tool XMIND. You can document your OSINT data and analyze relationships between people using a data visualization application.

Let's get this party started....
Creation of a sock puppet account?

- What are you planning to do?
- Who do you want to be online?
- Operational security reasons.

Do you already have a sock puppet account?
Controlling your sock puppets

Most of the time you have more than one sock puppet. That's challenging.

You can also use Excel to administrate your accounts.

Use tools like Framebox or Meetfranz.com and a good password manager to keep your accounts connected.

www.morphing.com and facebookplus.com

Most of the time there is a photo of a face.

Sometimes you need to add a photo to your account.

Select a stock photo. Find or use free images.

Here in Photoshop for example, you can do:

- Morph a couple of photos to one photo. You can do that by using the move tool.

www.morphing.com and facebookplus.com

Photo
Controlling your sock puppets

Interesting add-ons/extensions

A other automation tool you can use is Microsoft Flow. This also works with recipes.

Can you also use Islu.com recipes to automate actions with your accounts?

How can you keep your accounts alive?

Use a calendar to remind you to post something and be active. And do you do that also before and after work hours?

Also, let Twitter posts from Instagram cetera.

What you can also use is Islu.com recipes to automate actions with your accounts.

How can you keep your accounts alive?
Thank you for your attention!

Do not re-use your passwords

Make regular back-ups
Financial investigations
and the internet
OSINT stream today
1. Introduction
2. Crime & Algeria
3. Bitcoin laundering

Money Laundering
Money laundering is the process of taking 'dirty' funds and converting them into 'clean' funds allowing the criminal / fraudster uninhibited and untraceable enjoyment of his funds.
Statistics

- According to the International Monetary Fund, about $1.5 trillion dollars is laundered every year, amounting to about 5% of the world’s entire GDP.
- That’s a lot of dough getting washed. (1,500,000,000,000 USD)
- This is more than the total output of an economy the size of the United Kingdom.
- If you ever plan on breaking bad, one of the key things you’ll have to know is how to take your ill-gotten gain and launder it into “clean,” usable money.
- Worldwide regulation is strengthening especially since 9/11-2001.
- In The Netherlands, 17 million inhabitants, criminals launder up to 16 BILLION Euro’s each year!

Approach trends regarding money laundering investigations

- The moneylanndering approach: Find indicators and trace (proceeds of) (tax) crimes not seen before and confiscate these proceeds.
- Monitoring approach; the confiscation gap: ‘Confiscate future proceeds/assets’
- Joint government/agencies approach; ‘Take what you can trace/confiscate together’
Financial Profile
- Salary
- Income
- Profit
- Pension
- Bank balance
- Real estate
- Mortgage
- Car, boat
- Social media
- Family
- Partner
- Employer
- Company records
- Company website

Personal Profile
- Profession
- Lifestyle
- Criminal record
- Alimony
- Bankruptcies

Risk Profile

Target

Social Profile

Business Profile

The three stages in money laundering...
1: Placement
2: Layering
3: Integration
Placement

Placement is the first stage in money laundering where the cash proceeds of criminal activity enter into the financial system.

This is most critical stage for any money launderer as the criminal can effectively mask his 'dirty' funds by commingling his 'clean' funds and create an aura of legitimacy.

Layering

Layering is the second stage in money laundering where attempts are made to distance the money from its illegal source through layers of financial transactions. Layering often entails the international movement of the funds.
Integration

Integration is the third stage of money laundering. This stage involves the re-introduction of the illegal proceeds into legitimate commerce by providing a legitimate-appearing explanation for the funds to the criminal.

Money Laundering in Algeria

- Extent of money laundering is considered minimal
- Stringent regulations and banking sector dominated by state owned banks
- Close monitoring by government
- Updated criminal law against terrorism financing

Vulnerabilities:
- Large cash-based economy (Hawala banking) is a security problem
- Cash-based is appr. 40% of the GDP
- Real-Estate market is vulnerable in Algeria to money laundering
- Trafficking. Drugs, illicit goods, stolen goods etc
- Terrorism
Algerian in depth fears > money laundering/crimes

- Customs fraud
- Use of offshore havens for tax evasion
- Abuse of real estate transactions
- Commercial invoice fraud
- Informal economy with a lot of cash

Al Qaida in the Islamic Maghreb is also a concern. They raise money through drug smuggling and trafficking.

Source: state.gov
Algerian criminality

- Big criminal in Algeria. Is doing drug trafficking, especially hash.
- He is working in the port of Oran.
- Algeria seized almost 700 kg of cocaine. (real estate mogul) leader.
- Nickname: Coke line from Brazil via Algeria
- Oran is a hub for drug trafficking to Europe. Oran has a major port.
Data breaches which are shared on the internet

- More and more data leaks
- With a lot of sensitive data
- Internal leakages are very dangerous and could expose a lot of secrets

You can use them to do research against criminals

Panama Papers

Algeria launches money laundering probe on back of Panama Papers
How can we leverage internet data (OSINT)?

- Companies data
- Chamber of commerce data
- LinkedIn profiles
- Websites
- Email addresses
- Social media profiles in general
Follow the money
What is a cryptocurrency?
Crypto currencies & Terror/Crime

1. **Bitcoin**: is used to conduct funding campaigns for terrorism. 
   Also agents to hack the Democratic National Committee and the 
   Clinton campaign, and so on.

2. **Legitimate use**: A lot of people do use Bitcoin for legitimate use 
   and don’t use it for illegal purposes.

3. **Blockchain**: And the underlying technology is an very important 
   new innovation in the world of technology.

Terrorist and cryptocurrencies

**Terrorists using cryptocurrencies to evade detection and to 
fundraise**

Like other criminals, terrorists use crypto because it provides the 
same form of anonymity in the financial setting as encryption does 
for communication systems.

In this way they can avoid interference from financial regulators.

*Europol produced a report in 2015. According to this report 40% of high profile 
cases bitcoin was used in the EU.*
Terrorist and cryptocurrencies

Just seen a brother with one arm going to fight the regime in muna. What is your

CEPOL
Hawala banking
An ancient system of money transfer

How hawala works
Hawala is a legal but informal means of transferring money across the globe.

**STEP 1**
In Country A...

**SEND**
HAWALADAR A

Sender gives cash to hawala agent (Hawaladar A). Agent gives sender a code.

**STEP 2**
Hawaladar A to B...

HAWALADAR A
HAWALADAR B

Hawaladar A tells a counterpart in country B how much cash has been received.

**STEP 3**
Sender to Recipient...

**SEND**
HAWALADAR B

Recipient receives the code and the cash from the counterpart in country B.

**STEP 4**
In Country B...

**RECEIPIENT**

Recipient gives code to Hawaladar B who hands over cash, minus fee. Hawala agents settle their account separately.

Sources: Financial Action Task Force (FATF); Interpol

---

Malicious laundering process of virtual currency

![Diagram of malicious laundering process of virtual currency](image)

Figure 1. Malicious laundering process of virtual currency
1. Collect virtual currencies with zero or extremely low cost. 
   eg attacker can hack users' accounts, exploit the system 
   vulnerabilities, or participate in online promotion activities to win 
   virtual currency for free.

2. Attract potential buyers with high discounts, through various ways 
   such as spreading spams and posting advertisements. And then sell 
   the virtual currency in popular e-commerce websites like eBay or 
   Taobao.

3. Once a buyer commits (paid real money to an attacker) the purchase 
   her account will receive virtual currency (eg as gifts) from one or 
   multiple malicious accounts controlled by an attacker. 
   Attackers mostly uses multiple accounts to evade control.
Preparation
What do you need to use in this investigation?

https://www.blockchain.com/explorer
Google dorking

Blocks in the blockchain

Transaction data in the blockchain is continuously recorded and recorded in files that we call blocks. You can see the blocks as the individual pages of a ledger. The blocks within the network are arranged in a specific linear order. New transactions are added continuously at the end of the chain. The blocks can never be changed or deleted once they have been added to the chain in the blockchain network.
Blocks in the blockchain

Every block contains an overview of all recent transactions, but also a reference to the block immediately before it. In addition, a block is equipped with “the answer” to a very complex algorithmic puzzle. The answer to such a puzzle is unique for each individual block. New blocks cannot be added to the blockchain if the puzzle is not solved by the correct answer.

Analyze

Keep in mind that hundreds of millions of transactions have occurred since his conception 2009.

Work with the higher numbers, eg with 100,000th block.

Block Height 100000 Blocks at depth 100000 in the bitcoin blockchain

<table>
<thead>
<tr>
<th>Summary</th>
<th>Height</th>
<th>Hash</th>
<th>Previous Block</th>
<th>Next Blocks</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>100000</td>
<td>Main chain</td>
<td>380000000b3d3203e567e989f860abf74d04a464b1e23c1e8e939a4a3c3</td>
<td>d8c92711c7e3da23b100f2d4136b8f231d2a7f123</td>
<td>2010-12-29 11:37:43</td>
<td></td>
</tr>
</tbody>
</table>
We need to get closer to the right date

Go and find transactions matching with:

0.026043 BTC

To do so we need to click on the hash portion of block 396049

Block #396103

<table>
<thead>
<tr>
<th>Summary</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number Of Transactions</td>
<td>279</td>
<td></td>
</tr>
<tr>
<td>Output Total</td>
<td>116,520,600 BTC</td>
<td></td>
</tr>
<tr>
<td>Estimated Transaction Value</td>
<td>6,000,944,000 BTC</td>
<td></td>
</tr>
<tr>
<td>Transaction Fee</td>
<td>0.08020005 BTC</td>
<td></td>
</tr>
<tr>
<td>Height</td>
<td>1364 (655 Close)</td>
<td></td>
</tr>
</tbody>
</table>

Hashes

Hash

Pre-headers

Next headers

Meta flags
Eventually

Transaction

Looking further into the transaction from block 396123, at 11:13:42, TLQv8aKtQoIY5M5zkaG8RW2
Dorking

Essentially, there was suggested that by utilizing Google indexing, you can simply find a transaction by googling the exact amount of BTC you are looking for, as well as the date in a YYYY-MM-DD format. By using this alternative, you can subvert a lot of the
cur
ted.
What to use in this investigation

- [https://www.blockchain.com/explorer](https://www.blockchain.com/explorer)

- [https://bitcoinwhoswho.com/](https://bitcoinwhoswho.com/) which is a tool that allows you to look up certain BTC addresses and see if there are various scams associated with them. Important to point out that scams or illicit activities on BitcoinWhosWho are user-reported; therefore, just because an address is not flagged on here does not mean it is not connected to illicit activity.

- [https://www.walletexplorer.com/](https://www.walletexplorer.com/) though similar to a block explorer in reporting transaction history, WalletExplorer also goes a step further by showing other addresses that are in the same BTC wallet, occasionally connecting an address to a specific exchange.

And, again, Google searching!
Method

- Insert the address Nj3y into the block explorer and then just methodically through the transactions.
- Enter address of interest into Bitcoinwhoiswho, Walletexplorer and Google — the order doesn’t matter.
- Go through each tab and see if anything is flagged.
- If yes, enter into your spreadsheet. If no, move onto next transaction.

Some interesting things

On February 1, 2019, 0.13747974 BTC was sent from Bu1s and another address ending in 3g.
If we dive deeper into 3sVc on our blockexplorer, we'll see that it has only had two transactions which doesn't immediately signal to us that this address belongs to an exchange. But, if you utilize WalletExplorer to interrogate this other address, you'll find that it belongs to the same wallet as 31bo, and therefore, is also connected to Binance.
An introduction to technologies for online criminal activities

Introduction

Agenda
- OSINT
- Terrorist use of Internet (and Darknet potentialities)
- TOR Marketplaces
- Crawling Tor
- Introduction to crime data mining
- Investigative analysis of Tor Marketplaces data

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 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 Rooms, Web Archive ...
  - Open Data: government reports, financial plans, demographic data, legislative debates, press conferences, speeches, various ethnographics, disease spread.
  - Direct observation: 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

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

- Rumiyah 10
- Worldofcloud.com
OSINT (Rapidminer) [Diagram]

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 [Diagram]

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 stemming from large amounts of data (through automatic or semi-automatic methods and scientific, industrial or operational use of this knowledge).

OSINT in place

- Dedicated servers
- 24/7 monitoring
- Continuous cataloging of targets
- Continuous study of variation of the targets
- Extrapolation and normalization some data
- Organization and analysis of data (automatic and human)
- Timely reaction to events (automatic and human)

OSINT and REPUTATION

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

- The onion routing
  - http://thetorproject.org/
  - http://h5p-o27k2x5agpt2s.onion

Data extraction techniques

- Official Web APIs
  - Ease
  - Rich documentation

Data extraction techniques

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

Data extraction techniques

- Official Web APIs
  - Ease
  - Rich documentation

Captchas

- Twing (e.g. Vicarious pharse)
Global terrorism database

Research findings (2017)

- A small minority of individuals (6%) bought to recruit others online.
- Although a third of the sample prepared for some aspect of their attacks online, 6% specifically chose their target after conducting some online research.
- The analysis undertaken by police at one Jihad-inspired jail showed that the majority 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.


CEPOL

radicalization

1. The Internet offers more prospects for radicalization. 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 radicalization.

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-radicalization, interactions, be they physical or virtual, are still crucial for radicalisation.


CEPOL
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 lone 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

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

• The sources of terrorist funding vary. Firstly, they may originate from illegal activities, ranging from low-scale criminality to organised crime (e.g. trafficking in drugs, weapons or human beings).
• The origin of the funds might, however, also be legitimate, being provided for example by the members of the organisation (usually the newcomers) or obtained through the abuse of non-profit organisations. New funding techniques of terrorist organisations were recently identified by the FATF in respect of Da'esh (also known as the "Islamic State").
• Given the way of its functioning, Da'esh resorted to new methods of funding which could be considered more inherent for a state, such as leveraging taxes or exploiting natural resources (such as in this case natural gas and oil).

Financing

• The funding of terrorist activities often requires funds to be moved within or across countries. This might be done through official channels of the financial market and money remittances, through unregulated channels (e.g. online) or with the use of cash couriers (e.g. through hawala).
• In particular, unregulated channels and hawala can receive strong facilitation benefits by using anonymous networks (e.g. the well-known site Ishtar on Tor sought bitcoin contributions from supporters).

Financing

• A fundamental aspect to take into account is the broadly use made by terrorist groups of apparently legitimate organisations or religious centres to disguise and launder their illegal financial activities: the "Dawa infrastructure".
• In some cases, the Dawa infrastructure is established around charity organizations (including the illicit values of charity donation: zakat and alms) which are publicly represented by non-profit companies, Islamic education centers, and hubs for fundraising events.
• Cryptocurrencies are introducing new forms of crowdfunding, making, in most cases, a clear distinction between crowdfunding online campaigns to finance terrorist behind a talas intent and those made for explicit philanthropic purposes.
• Online charity crowdfunding campaigns, more similar to the Dawa infrastructure politically correct approach.
• Crowdfunding campaigns requiring donations in digital currencies are more explicit about their "Talal" intent (e.g. Jihazia campaign explicitly showing that the donations were intended for buying weapons for terrorist groups).
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.
- 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.

short list of hidden marketplaces (tor&i2p)

- *New markets & under construction:*
  - [budes另行](https://budes另行)
  - [Fedex](https://Fedex)
  - [Trials](https://Trials)

- *Dead/Scam Marketplaces links*:
  - [budes另行](https://budes另行)
  - [Fedex](https://Fedex)
  - [Trials](https://Trials)

Financing

- There is no evidence of transactions of relatively large amounts of money by cryptocurrency to finance Islamic terrorist groups, especially compared to the extensive illegal use of digital currencies perpetrated by small/middle criminality or extremist political movements (as neo-Nazi groups).
- Indeed, the largest amount of money that terrorist groups raise from donations are those coming from false Islamic charity organizations through crowdfunding campaigns or from wealthy donors from Gulf countries by direct money or gold donations.
- These actors may have avoided a massive use of cryptocurrency to take part in the *jihad bi maal* for reasons related to the instability of the digital-currencies market.
Research findings (2017)
- A level of the sample (20%) prepared for the attack by using online resources
  - bomb-making instruction videos;
  - pass-on manuals;
  - downloaded copies of三期 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 training records;
  - terrorist training manuals.


### Table 1

<table>
<thead>
<tr>
<th>Variable</th>
<th>N</th>
<th>%</th>
<th>CR</th>
<th>OR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-belligerent</td>
<td>942</td>
<td>56.1</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>Belligerent</td>
<td>656</td>
<td>78.0</td>
<td>1.50</td>
<td></td>
</tr>
<tr>
<td>Gender Male</td>
<td>990</td>
<td>95.0</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>Gender Female</td>
<td>646</td>
<td>85.0</td>
<td>1.10</td>
<td></td>
</tr>
<tr>
<td>Education Level School</td>
<td>942</td>
<td>85.0</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>Education Level College</td>
<td>656</td>
<td>85.0</td>
<td>1.10</td>
<td></td>
</tr>
<tr>
<td>Employment</td>
<td>942</td>
<td>56.1</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>Employment Full-time</td>
<td>656</td>
<td>85.0</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>Employment Part-time</td>
<td>942</td>
<td>85.0</td>
<td>1.10</td>
<td></td>
</tr>
<tr>
<td>Employment Volunteer</td>
<td>656</td>
<td>85.0</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>Employment Other</td>
<td>942</td>
<td>85.0</td>
<td>1.10</td>
<td></td>
</tr>
</tbody>
</table>

CR = Cohen’s d; OR = odds ratio

Planning

A recent case from France, Public Prosecutor v. Hicheur, 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.
**Operation Bayonet**

- **Law enforcement from Europe, Canada and the United States joined forces early 2019 to target vendors and buyers of illegal goods on dark web marketplaces. During the course of this operation, international law enforcement agencies made 61 arrests and shut down 50 dark web accounts used for illegal activity.**
- **Law enforcement executed 65 search warrants, seizing 299.5 kg of drugs, 51 firearms, and over €6.2 million (almost $6 million in cryptocurrency, €2.2 million in cash, and €935,000 in gold).**
- **They also conducted 122 interviews.**

26 March 2019 EUR-POL


---

**Drug data categories**

<table>
<thead>
<tr>
<th>Drug data category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prescription drugs</td>
<td>Intended use, name, quantity, method of administration, route, batch number, expiry date, dosage, packaging, period of dispensation.</td>
</tr>
<tr>
<td>Non-prescription drugs</td>
<td>Intended use, name, quantity, method of administration, route, expiry date, dosage, packaging, period of dispensation.</td>
</tr>
<tr>
<td>Tobacco products</td>
<td>Intended use, name, composition, quantity, method of administration, route, marketing period.</td>
</tr>
<tr>
<td>Herbal products</td>
<td>Intended use, name, composition, quantity, method of administration, route, marketing period.</td>
</tr>
<tr>
<td>Synthetic cannabinoids</td>
<td>Intended use, name, composition, quantity, method of administration, route, marketing period.</td>
</tr>
<tr>
<td>Inhaled substances</td>
<td>Intended use, name, composition, quantity, method of administration, route, marketing period.</td>
</tr>
</tbody>
</table>

---

**Feedback**

<table>
<thead>
<tr>
<th>Feedback</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law enforcement</td>
<td>Law enforcement agencies from various countries.</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>Cybersecurity measures taken by law enforcement agencies.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Compliance regulations and guidelines followed.</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>Risk assessment and mitigation strategies.</td>
</tr>
<tr>
<td>Evidence collection</td>
<td>Evidence collection methods and procedures.</td>
</tr>
<tr>
<td>Investigation</td>
<td>Investigation techniques used by law enforcement agencies.</td>
</tr>
<tr>
<td>Reporting</td>
<td>Reporting procedures followed by law enforcement agencies.</td>
</tr>
<tr>
<td>Evaluation</td>
<td>Evaluation of the effectiveness of law enforcement actions.</td>
</tr>
<tr>
<td>Coordination</td>
<td>Coordination between law enforcement agencies.</td>
</tr>
<tr>
<td>Planning</td>
<td>Planning and preparation for law enforcement operations.</td>
</tr>
</tbody>
</table>

---

**Drug data categories**

<table>
<thead>
<tr>
<th>Drug data category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prescription drugs</td>
<td>Intended use, name, quantity, method of administration, route, batch number, expiry date, dosage, packaging, period of dispensation.</td>
</tr>
<tr>
<td>Non-prescription drugs</td>
<td>Intended use, name, quantity, method of administration, route, expiry date, dosage, packaging, period of dispensation.</td>
</tr>
<tr>
<td>Tobacco products</td>
<td>Intended use, name, composition, quantity, method of administration, route, marketing period.</td>
</tr>
<tr>
<td>Herbal products</td>
<td>Intended use, name, composition, quantity, method of administration, route, marketing period.</td>
</tr>
<tr>
<td>Synthetic cannabinoids</td>
<td>Intended use, name, composition, quantity, method of administration, route, marketing period.</td>
</tr>
<tr>
<td>Inhaled substances</td>
<td>Intended use, name, composition, quantity, method of administration, route, marketing period.</td>
</tr>
</tbody>
</table>

---

**Feedback**

<table>
<thead>
<tr>
<th>Feedback</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law enforcement</td>
<td>Law enforcement agencies from various countries.</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>Cybersecurity measures taken by law enforcement agencies.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Compliance regulations and guidelines followed.</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>Risk assessment and mitigation strategies.</td>
</tr>
<tr>
<td>Evidence collection</td>
<td>Evidence collection methods and procedures.</td>
</tr>
<tr>
<td>Investigation</td>
<td>Investigation techniques used by law enforcement agencies.</td>
</tr>
<tr>
<td>Reporting</td>
<td>Reporting procedures followed by law enforcement agencies.</td>
</tr>
<tr>
<td>Evaluation</td>
<td>Evaluation of the effectiveness of law enforcement actions.</td>
</tr>
<tr>
<td>Coordination</td>
<td>Coordination between law enforcement agencies.</td>
</tr>
<tr>
<td>Planning</td>
<td>Planning and preparation for law enforcement operations.</td>
</tr>
</tbody>
</table>
Surface Web

USER
Every computer on the internet has a unique address (IP number).

SERVER
When a user connects to the Internet, their identity can be traced back through the server.

MERCHANT
The merchant requires personal information to sell and shipping details from the buyer.

Darknet Market

USER
No unique address. The Internet's anonymity makes it the drug of choice.

SILK ROAD

TOR SERVER

Key findings

- The trade in illicit drugs on darknet markets is a dynamic area subject to rapid change due to marketplace apper and disappear. Overall, the importance of the darknet seems to be expanding and it now affects most EU Member States in some way.

- When compared with current estimates of the annual market value of the overall EU drug market, sales volumes on darknet markets are currently modest, but are increasing and have the potential to grow.

- EU-based suppliers are important players in the darknet ecosystem. In the 2011-2013 period, they accounted for around 45% of all drug sales in terms of revenue on the darknet markets analyzed.

- Between 2015 and 2017 on Adbay, 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 cited origin of NPS sales, which may reflect both patterns of demand and recent changes in legislation.

- The relative unimportance of darknet markets suggests that they will be most commonly used for mid-to-high-volume 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 highest level, and total sales volume was greatest for cannabis and cocaine.

- The picture was different for MDMA and ecstasy, however, where mid-level sales represented a relatively large proportion of all sales (although still was 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, when 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 thatdarknet markets may play a different role in the supply chain for these substances.
- Few 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 organized 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.

Marketplaces impacting events

1. Operation Onymous
2. Evolution exit scam
3. Operation Bayonet

Silk Road closed by FBI

Byngstads B., Spagnoletti P.
The Forces of the Dark Net. A Critical Realist Investigation

Lifetime of marketplaces

CEPOL - Drugs and the darknet: Perspectives for enforcement, research and policy
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 toolkits or fake documents, are enablers for further criminality.

- Sale of illicit goods to dedicated criminal websites and markets hosted on anonymity 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, non-criminal .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.
CDR history and versions

- Do you recognize some problems?
- Changes of data bases in mobilephones service providers (MSP) structure – big or small
- Data sets (CDR) from different MSP’s are slightly different
- Different methods of giving the outcome (hard copy, electronic)
- Different time intervals for cutting material by time periods (usually 3 months) – eg. 1 year means 4 files...
Thank you for your attention!
DATA SETS IN TELECOMMUNICATION – possibilities to LEA

How Mobile Phones Work
Facts and Figures (December 2016)

- Around 41.2 million mobile phone subscribers (SIM cards) in ALGERIA
- 18.6 mln - DJEZZY
- 13.0 mln - MOBILIS
- 11.7 mln - OOREDOO

Cell Types

- Omni Cell
  - Omni-directional cells have one antenna which gives 360 degree coverage
- Macro Cell
  - Are the work horses of a network.
  - Cells have more than one antenna and the coverage area is split up into sectors (normally 3 or 6)
  - Antennas mounted on masts, buildings, normally elevated
  - Provide coverage over varying distances typically 1 KM to 15 KM.
- Micro Cell
  - Provide additional coverage in areas of high number users
  - Mounted at street level and often disguised
  - Provide coverage over distances between 100m and 1 KM
- Pico Cell
  - Provide coverage up 10 to 100m
  - Generally found in buildings with dense population
- Nano Cell
  - Smallest standard cell, found in offices
  - Provide coverage between 1m to 10m
Seizure of Mobile Phones

Legislation covering Telecommunications

Is part of cyber
Issues around Forensic Examinations of SIMs / Handsets & Communications

The Differing items of Communications Data
Attributing Mobile Phones

Evidencing Communications Data
Any Questions?

Thank you for your attention!
How Mobile Phones Work?

/previous lecture/
IP’s history and versions

- The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.
- Its routing function enables internetworking and essentially establishes the Internet.
- Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahn in 1974; the other being the connection-oriented Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.
• The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet.

• Its successor, Internet Protocol Version 6 IPv6, has been growing in adoption for the last years, reaching almost 20% of the Internet traffic as of April, 2018

• Why this evolution from v4 to v6 main reason? 😊

• More possibilities...more addresses

• But

• No geo location...
**IPv4, IPv6**

An IPv4 address (dotted-decimal notation)

172.16.254.1

10101100.00010000.11111110.00000001

One byte = Eight bits

Thirty-two bits (4 x 8), or 4 bytes

---

**WEB 1.0 to 2.0 concept – why?**

- What is the main difference?
- From sharing knowledge to sharing and creating content
- 2.0 is the SOCIAL WEB
Thank you for your attention!
What is OSINT for You???

- ...
- ...
- ...
- ???
- !!!
OSINT - definitions

Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an Intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources). It is not related to open-source software or public intelligence.
Thank you for your attention!

Europol Union Agency for Law Enforcement Training
Axelrod, 1004 Brussels, B-1050 Belgium - info@europol.int
Telephone: +32 2 289 0330 - Fax: +32 2 289 0330 - http://www.europol.int
SPECIAL TECHNICAL SOLUTIONS FROM SCIENTIFIC PROJECTS IN THE AREA OF PREDICTIVE AND DESCRIPTIVE ANALYTICS

Thank you for your attention!
DISCUSSION

- What are your problems with the investigations?
- Probable solutions?
- Some advice to us?
At the very beginning...

- around 5000 b.c. — first abacus
- 250-230 b.c. — Sieve of Eratosthenes - simple, ancient algorithm for finding all prime numbers up to any given limit.
- 876 a.c. - First, registered in India, usage of 0 symbol.
- 1642-1643 - Blaise Pascal — first mechanic calculator to make a sum +.
- 1666 - Samuel Morland — plus and minus + -.
- 1679 - Wilhelm Leibniz - binary arithmetics (0 and 1) and in 1694 first, mechanic binary calculator.
- 1810 - Abraham Stern first, mechanic calculator for five calculations (+, -, *, /, \text{Roots}).
- 1820 - Joseph-Marie Jacquard - loom computed the punched cards as a source of commands.
- 1888 — Graham Bell — phone.
Phones – why???

- Telephone: Bell 1888 - first telephone. Then analogue, digital...
- 1992 - creation of CENTERTEL.
- The first phones were very expensive.
- Telephones used analog radio signals, which made it very easy for them to be tapped.
- Forecasts for the Polish market were predicted by a total of 6 million subscribers of mobile phones... and these forecasts were considered extravagant!
- In 1991, the introduction of GSM (meaning Global System for Mobile communications), the standard of a digital network enabling telephone connections with the whole world.
- 1994 - text messages enter the market, changing the way of writing (eg forever - for ever: 4eva)
- September 1996 - establishment of the ERA network.
- October 1996 - establishment of the PLUS network.
- 2002 - the number of phones in the world exceeds 1 billion.
- 2004 - new technologies abolish the limitations of previous mobile phones, introducing PDA (ie Personal Digital Assistant - Individual Digitizer) and Blackberries (allowing access from the phone to the Internet and e-mails).
- 2005 - IDEA mobile operator changes its brand to ORANGE.
- 2005 - entry to the 3G standard market; third generation mobile phones. 3G phones combine high speed internet access and video phones.
- October 2007 - PLAY creation.
- December 2007 - the Polish market has reached 42 million subscribers.

Computers used to be lonely....
ARPANET 1969

• ARMY HAS MADE THE DEMAND FROM INDUSTRY/UNIVERSITIES
• CREATED AS SCIENTIFIC PROJECT
• HOW IT CHANGED THE LIFE? (most EU countries has switched on 80s, 90s, our salaries)
• HOW LEA SHOULD CHANGE? Is there another way?

International Network

Internet
Google has indexed just 0.004% of the internet!
So what’s here?

What is the “Deep Web”?

- Websites search engines have yet to index, or have opted out of being indexed
- Pages not linked by any other pages
- Websites that sit behind a pay wall
- Some news and magazine sites
- Government owned databases
- Online storage
- Emails
- Online Chat
- Private content on social media
- Forums
What is the “Dark Net”? LEA challenges...

- Big amount of data to process
- How extract the important things (crimes and information related to)
- How not to duplicate
- How to be within the legal frameworks
- How to be technically and technologically ready
- How to change the way of thinking (politicians, society, bosses)
- How to change the law
- How prepare the evidences
- ...(catalogue is still open)
There are some successes 😊 even global

- Have you heard?

- Why are these successes possible? How do you think? Read carefully and tell me how it was possible 😊

- Some work to do??? We will see 😊

Internet in Poland

- officially from December 20, 1991
- On April 30, 1991, the national domain of the highest level "pl" was registered at the Computer Center of the University of Copenhagen.
- On August 17, 1991 from the Faculty of Physics of the University of Warsaw, the first, lasting one minute Internet connection using the TCP / IP protocol was compiled.
- In June 1991, the POLPAK Telekomunikacja Polska backbone network was launched.
- In 1992, the first Polish internet.pl website was created, followed in 1995 by the Polish internet portal Wirtualna Polska. In April 1996, TP SA launched access to the Internet using modems.
- In August 1993, the first Polish web server was created under the name "Polish Home Party"
- BUT – 1996 polish national operator has start selling modems and from this time INTERNET starts...
• HOW IT IS IN ALGERIA?

• WHEN THE INTERNET HAS BEEN SWITCHED ON?

• MAIN PROBLEMS FOR LEA? CAN YOU DEFINE THEM PLEASE...

Cybercrimes - definitions

• Cybercrimes (computer crimes):
  o sensu largo,
  o sensu stricte.

• Polish statistics
• **Sensu largo** – all crimes in which some part has connection to computer, network. Computer is a thing to commit some crime but it does not have to be digital crime ex. cheating, piracy.

• **Sensu stricte** – digital crimes in which data processing is attacked. Np. hacking, computer sabotage...
Polish Cybercrimes – most popular

The basic legal act on which the fight against cybercrime in Poland is based is the Act of June 6, 1997 Penal Code (Journal of Laws No. 88, item 553, as amended), and in particular:

Art. 190a § 2 - impersonation of other false profiles,
Art. 200a of the Penal Code - contact with a minor below 15 years,
Art. 202 of the Penal Code - pedophile content,
Art. 256 of the Penal Code - political extremism - fascist content, hate speech
Art. 267 § 1 of the Penal Code - unauthorized retrieval of information (hacking),
Art. 268 § 2 of the Penal Code - blocking the information being obtained (ransomware),
Art. 268a of the Penal Code - unauthorised access to IT data,
Art. 269 A § 1 and 2 of the Penal Code - computer sabotage,
Art. 269a of the Penal Code - dissemination of malicious programs and cracking,
Art. 269b of the kk, the so-called - hacker tools,
Art. 271 of the Penal Code - trade in fictitious costs,
Art. 286 of the Penal Code - fraud committed via the Internet,
Art. 287 of the Penal Code - computer fraud,
Art. 293 of the Penal Code - handling of a stolen computer program

EU REGULATIONS ON CYBER

- 1995 - DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (data retention periods, telecommunication traffic regulation)
- 2001 – Budapest Convention on Cybercrimes,
- 2018 - The Commission will present concrete proposals in early 2018 to facilitate swift cross-border access to electronic evidence
Budapest, 23 November 2001

- Convention on Cybercrime
- Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States
- Entry into force - 01/07/2004 - 5 Ratifications including at least 3 member States of the Council of Europe
- 56 States are now Parties and another 14 States have either signed it or been invited to accede

Budapest Convention on Cybercrime

- The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.
- It also contains a series of powers and procedures such as the search of computer networks and interception.
- Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.
NIS Directive

- Member States preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority,
- cooperation among all the Member States, by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among Member States – CSIRT Network.
- After GENVAL cyber evaluation CSIRT Network is cooperating really well

GDPR

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
- Thanks to this regulation a lot of companies, institutions and organisations has changed the awareness and technical solutions
NATIONAL REGULATIONS ON CYBER

- Are different in every country.
- First steps are always adjustments of the old law to the new situation and later new paragraphs to the old codes (acts)
- Then we create some legislations to manage the telecommunication movement
- Then we create specialised acts which consider some cyber aspects
- Then there are Cyberlaws which grows whole the time
- Then there are cyber strategies for some technological changes
- And Cyber Policies as Cyberdefence or Cybersecurity for the country
- And... what would be in the future?????

National Cybersecurity Policies/Strategies

1. Principles for cybersecurity
2. Strategic priorities and actions
3. Roles and responsibilities of different actors at national and international level
NATIONAL REGULATIONS ON CYBER

• BUT...

• Not all countries are going in the same directions...
• Not all countries are going within the same time...
• Should it be one EUROPEAN CYBER LAW? OR GLOBAL LAW?
• There would be EU Cyber Law but would it solve the problem? (eg. SPAM – e-privacy directive)
Vision

• In 2022, Poland will be a more resistant country to attacks and threats coming from cybersecurity. Thanks to the synergy of internal and international cyberspace activities, the Republic of Poland will constitute a safe environment enabling the implementation of all state functions.

Main goal

• Ensuring a high level of security for the public sector, private sector and citizens in the provision and use of key services and digital services.
Specific objectives

Specific objective 1

- Achieving the ability to coordinate actions at the national level aimed at preventing, detecting, combating and minimizing the effects of incidents violating the security of ICT systems relevant to the functioning of the state
- Adaptation of the legal environment to the needs and challenges in the area of cyber security
- Improving the structure of the national cyber security system
- Increased effectiveness of cooperation of entities ensuring the security of the cyberspace of the Republic of Poland

Specific objectives

Specific objective 1

- Increased ICT security of key and digital services as well as critical infrastructure
- Development and implementation of standards and good practices for the security of network and information systems
- Development and implementation of a risk management system at the national level
- Ensuring a secure supply chain
- Building a cyberspace users warning system in terms of risk resulting from cyber threats
Specific objectives

Specific objective 2

- Strengthening the ability to counter cyber threats
- Enhancing the ability to fight cybercrime, including cyber-espionage and terrorist events occurring in cyberspace
- Obtaining the ability to conduct a full spectrum of military activities in cyberspace
- Building capacity to analyze threats at the national level
- Building a secure communication system for national security purposes
- Audits and security tests

Specific objective 3

- Increasing national potential and competence in the field of security in cyberspace
- Expansion of industrial and technological resources for cyber security
- Building cooperation mechanisms between the public and private sectors
- Stimulating research and development in the area of IT systems security
Specific objectives
Specific objective 3

- Increasing the competence of the staff of entities important for the functioning of cyberspace security
- Creating conditions for the safe use of cyberspace by citizens

Specific objectives
Specific objective 4

- Building a strong international position of Poland in the field of cyber security
- Active international cooperation at the strategic and political level
- Active international cooperation at the operational and technical level
Management of the National Security Policy Framework

- The National Policy Framework for Cybersecurity is adopted for a period of 5 years.
- The minister responsible for computerization is the coordinator of the implementation of the National Framework of Cybersecurity Policy.
- Two years after the adoption and in the fourth year of validity, the document is subject to review and assessment of the effects of its impact.

Management of the National Security Policy Framework

- The results of the review are presented to the Council of Ministers.
- As a result of the review, the minister responsible for computerization prepares a proposal for corrective actions or a draft document for the next five-year period.
- In case of justified circumstances, the National Cybersecurity Policy Framework may be updated at other dates than those referred to above.
Financing

Within the state budget, a Multiannual Program dedicated to the construction and development of projects in the area of cyber security will be created

• DO YOU HAVE CYBERSECURITY STRATEGY OF ALGERIA? (when established)

• DO YOU HAVE CYBERDEFENCE STRATEGY OF ALGERIA? (when established?)
Types of threats in cyberspace.

Cyberattacks:
- malware (malware);
- phishing;
- spam;
- DDoS attacks;
- botnets;

Cyberattack - a type of virtual space activities aimed at blocking or taking over websites, mailboxes or databases.

Malware - The malware world is still growing rapidly and dynamically. The power of threats is perfectly demonstrated by statistics - in the world every 4 seconds there is a download of unknown, infected files, while every 5 seconds, users enter infected websites.
Phishing

- It involves obtaining confidential information about a specific person by use of dishonest methods.
- Most often fraudsters claim to be a trustworthy company, or a person who needs certain personal data at a given moment.
- Very often cybercriminals send spam to a large number of people, providing a fake site and claiming to be a specific bank or online store. After the victim enters the fake site, the information entered by the victim is captured (this situation may include false information about deactivation of the account and the request to re-enter all personal data).

In a nutshell, malicious software, also known as malware, is a computer program written specifically to perform malicious activities. The term malware comes from English with the complexity of two words: malicious (malicious) and software (software).
Phishing – large view

In a broader sense, phishing consists in using ignorance or introducing a mistake in the user who uses the Internet through crafted, electronically reliable information designed to achieve the expected behavior by the perpetrators, e.g.:
- providing sensitive data for the user, such as personal or financial data (bank account numbers, logins and passwords, etc.) - classical phishing;
- introduction and installation of malicious software by the user on the computer, which performs functions defined by the perpetrators.

Phishing

Malicious software can:
- follow the history of pages viewed and send information to the perpetrators;
- act as a keylogger on the computer and send information to the perpetrators (access password, credit card number);
- send spam;
- enable DoS attack, DDoS;
- connect the user's computer to the botnet network;
- act as spyware or adware (for displaying advertisements), etc.;
Phishing

Mechanism

**Phishing PHASES**

**Attack preparation:**
- registering the domain;
- preparation of malicious software and websites and placing them on a compromised server;

**Attacking:**
- sending out crafted information to users on the Internet via email;
- gathering information;

**End of attack:**
- use of collected information for criminal purposes;
- delete the evidences of your criminal activity.
SPAM

Spam — unwilling or not ordered electronic messages. The most popular is spam with the usage of e-mails but others are communicators (np. ICQ, Gadu-Gadu, Facebook Messenger, Whatsapp...), and in SMS messages.

SPAM History

On May 1, 1978, he sends approximately 1000 invitations to his birthday through the Arpanet network, receiving many funny as well as malicious messages, the number of which blocks hard drives on the first spammer's server.

May 1, 1978, he writes, and on May 3, he sends mini-computer advertisements from Digital Equipment Corporation, inviting all users of Arpanet from the West Coast of the United States to "open day" in order to present the company's latest products. The program he used to edit and send messages first required that each recipient's address was entered "manually" - hence the long message editing time, and secondly allowed only 320 entries in the "recipient" field. Gary, a representative of a company operating on the East Coast, decided to help Arpanet to propagate its products also on the West Coast. To this end, he obtained the addresses of Arpanet users from the West Coast, but there were more than 320 of them and some of them went into the message, so a large number of people who should have received the message did not receive it. Gary re-sent the message, which caused some users to receive it several times, which, for example, at a certain user from the University of Utah caused the operating system to be disabled on the computer.
Common legends in SPAM are:

1. **spam for winner** – simple method, very effective. You win sth but enter the link then trojan soft is installed – changing bank accounts numbers (ZEUS and it’s combinations)
2. **banking spam** – fake bank offers with a great %%% then trojan soft is installed – changing bank accounts numbers (ZEUS and it’s combinations) or fake web page to steal login and password for bank account.
3. **heritage spam** – info that you have inheritted sth and you have to pay tax, administrative fee or sth else.
4. **african spam** – some offer to help someone insted of some money – help me to take over my heritage without paying taxes.
5. **Love spam** – help me to run away from family or I want to transform to some country

**DDos**

- **DDoS - Distributed Denial of Service**

Serwer - computer, on which there is WWW – is having so much “questions” that is override. The connection is blocked.

Sometimes only high, lawfull connection rate to bed prepared WWW can cause the same effect like DDOS attack 😊.
Botnet

**Bot** – abbreviation from robot. Malware sent by criminals to change our device into bot (zombie). Then our device is managed by criminals – and is doing the orders of the criminals.

Usually bots are creating bigger networks which are called **Botnets**.

**DEFINITION**

**Botnet** – net of devices type zombie with the malicious software working whole the time beneath.

Nowadays Botnets are one of the biggest threat in the Internet.
DEFINITION

**Zombie (zombie device):**
Device connected to the Internet in which (without the knowledge of the owner) malicious software has been installed and this device is managed by someone from outside.

---

**Dangers connected to botnet**

Can block the Internet access from a large number of devices.

Can block the state services – e.g. banking system accessibility or critical infrastructure management.
PREVENTIVE APPROACH

- use only the legal software,
- use antivirus software which always is updated,
- use always updated version of OS and browser,
- DO NOT INSTALL THE SOFTWARE FROM UNKNOWN SOURCES!!!

Examples of BOTNET

Storm – is considered to be the biggest all over the world. Main task is to send spam. More then 20% of word spam is being sent by Storm. First noticed in January 2007. Storm consists from around 1,9 milion zombie devices. Only Windows devices are in danger.
Examples of BOTNET

**ZEUS** – has been created to steal from computers in USA and UK private information - mainly different types of logging passwords.
Then next versions has been modified to exchange the bank account number during online transactions.
Whole the time we can see that it is developed software.

Basic version you can buy from 3.000 USD.

---

**LEA problems with hate speech**

- On Facebook, a huge number of profiles, entries, events that may exhaust the statutory hallmarks of "hate speech" classified in Polish criminal law arises.
- Facebook servers and headquarters are located in the USA:

  1601 Willow Road,
  Menlo Park CA 94025
How Internet PEDOFILES work?

- Internet pedophiles offer their attention, feeling and kindness, gradually seduce their victims, often with a considerable amount of time, money and effort.

- They are up to date with music and hobbies with which children can be interested. They listen to children and they sympathize with their problems.

- Trying to make young people eager sex, they gradually introduce erotic content to conversations ....

Crimes against property

- Can we list them now...?
How to recover money from a dishonest seller

Using the Chargeback service. Chargeback is a refund of the service provider’s account to the account of the cardholder after the complaint process, which begins at the request of the cardholder, when he lodges a relevant complaint with the bank. This is a free service.

Chargeback does not work automatically and its scheme of operation is simplified below:

• You buy an item or service by paying by card.
• If you want to use the Chargeback procedure, you submit such a request to your bank (at the bank of the card issuer).
• Your bank asks you to accurately describe the situation, specify the non-compliance and justify the request for a refund.
• Your bank transfers the matter to the issuer of your card (VISA, MasterCard), which is an arbiter in the case.
• The arbitrator asks for clarification from the seller’s bank, and the latter contacts the seller himself.
• After receiving explanations from both parties, the Arbitrator assesses their validity and issues a relevant decision, informs banks of both parties, and by them also the parties.
• The decision may be appealed against, in which case the procedure described in the items above is repeated.

Money laundering

all activities aimed at hiding the true source of illegal money from criminal activities and giving them marks of legal origin
Money laundering

Money laundering is always a secondary offense in relation to some other major crime, for example the production and sale of drugs, the illegal trade in arms, THB, kidnappings to extort ransom. Serious damage is caused by criminals at the level of the main crime, because their committing causes the spread of drug addiction, pimping, terrorism, corruption and many other negative social phenomena. Part of the laundered funds obtained as a result of the commission of the main crime serves to cover the costs of the criminal organization. The rest is reinvested in legal practices. Money laundering therefore stimulates the development of crime in its most dangerous, organized form.

**Nigerian fraud**

- This fraud first appeared on the Internet in the late 1980s. It is known by several names, including:
- "419" - paragraph number of the Nigerian Criminal Code regarding this type of extortion;
- Nigeria Scam, or Nigerian fake,
- Advanced Fee Fraud - cheating with initial costs,
- The Nigeria Connection - a Nigerian link.

**ALWAYS WE USE MONEY TO SENTENCE CYBERCRIMES – TRUE?**
SMS Premium Fraud

fraud involving the extortion of money from people who pay for using the services available on various websites by sending an SMS text message.

Legal obligations of mobile phone providers:
- free blocking of outgoing calls to premium rate service numbers and incoming calls from such numbers;
- free blocking of outgoing calls to the numbers of individual types of premium rate services and free blocking of incoming calls from such numbers.
IDENTITY THEFT

• Most common danger...

Data of interest:

- first name and last name,
- address,
- Pesel – personal number,
- date of birth,
- credit card number,
- mobile phone number,
...
Economic / Industrial Spying

- In addition to political and military espionage, **economic espionage** is often conducted to gain the secrets of production technology and technical solutions.

... but also login and password to:

e-mail account,
accounts on the auction site,
accounts on the social network,
bank account,
...
**Economic / Industrial Spying**

- In recent years, the **definition** of industrial **espionage has significantly expanded**. This includes, for example, sabotage actions inside the corporation, which was not previously done. In many cases, **embezzlement and installation of spyware software in computers are also included**. Often this catalog is extended by other deeds, such as staff corruption, extorting knowledge about the company, hijacking of managerial staff or members of its families.
SOCIAL ENGINEERING

• Social engineering in political science, sociology and marketing is a set of techniques to achieve specific goals through the manipulation of society.

• A person using social engineering thinks that the goal he goes is more important than the independence of thinking of other people who are subject to manipulation.

• Social engineering refers to human emotions and tries to lull human reason. Often the manipulator tries to convince the recipient of his message to his ideas even at the expense of unethical detachment from reality, because he believes that the purpose of his activity justifies such measures.

The use of social engineering

Social engineering cycle:

Recognition - general analysis of publicly available information about organization - financial results, catalogs, applications to the patent office, press mentions, articles in the professional press, the content of the website, as well as the contents of garbage cans;

Building relationships and trust - using internal information, giving in to someone else, remembering the names of people known to the victim, reporting the need for help or suggesting power;

Using trust - a request for information or action addressed to the victim. To manipulate the victim so that she herself can ask for help. (as IT personel)

Use of information - if the information obtained is enough - the next step that brings the attacker closer to the target, if not he returns to the previous steps of the cycle, until success.
QUESTIONS??