

EU/Algérie - Partenariat Contre-Terrorisme

Activité résidentielle

«OSINT, Darknet et techniques d'investigation »

Ecole supérieure de la Gendarmerie Nationale

Zeralda/Alger, Algérie

Dimanche 21 Avril – Jeudi 25 Avril 2019

Le contenu de ces sessions a été développé dans le respect de la loi et des droits

fondamentaux

CEPOL: [REDACTED]

Experts: [REDACTED]

Samedi 20 Avril

Arrivée de la délégation des experts CEPOL, suivant différents itinéraires et horaires.

Dimanche 21 Avril

- 08:00 Prise en charge de la délégation CEPOL et des experts à leur hôtel.
- 09:00 Ouverture de la session [REDACTED]
- 09:30 Internet utilisé pour commettre un crime du point de vue algérien
- 10:45 Break thé ou café
- 11:00 Internet utilisé pour commettre un crime du point de vue de l'UE I
- 12:00 Repas de midi.
- 13:00 Internet utilisé pour commettre un crime du point de vue de l'UE II
- 14:00 Break thé ou café
- 14:15 Internet utilisé pour commettre un crime du point de vue de l'UE III
- 16:00 Questions - réponses et fin de session.

Lundi 22 Avril

- 08:00 Prise en charge de la délégation CEPOL et des experts à leur hôtel.
- 09:00 OSINT I
- 10:45 Break thé ou café
- 11:00 OSINT II
- 12:00 Repas de midi.
- 13:00 OSINT III
- 14:00 Break thé ou café.
- 14:15 OSINT IV
- 16:00 Questions - réponses et fin de session.

Mardi 23 Avril

- 08:00 Prise en charge de la délégation CEPOL et des experts à leur hôtel
- 09:00 Analyse CDR et IPDR et attaques éventuelles contre l'utilisateur mobile I
- 10:45 Break thé ou café
- 11:00 Analyse CDR et IPDR et attaques éventuelles contre l'utilisateur mobile II
- 12:00 Repas de midi.
- 13:00 Analyse CDR et IPDR et attaques éventuelles contre l'utilisateur mobile III
- 14 :00 Break thé ou café.
- 14 :15 Analyse CDR et IPDR et attaques éventuelles contre l'utilisateur mobile IV
- 16:00 Questions - réponses et fin de session.

Mercredi 24 Avril

- 08:00 Prise en charge de la délégation CEPOL et des experts à leur hôtel
- 09:00 Darknet I
- 10:45 Break thé ou café
- 11:00 Darknet II
- 12:00 Repas de midi.
- 13:00 Darknet III
- 14 :00 Break thé ou café.
- 14 :15 Darknet IV
- 16:00 Questions - réponses et fin de session.

Jeudi 25 Avril

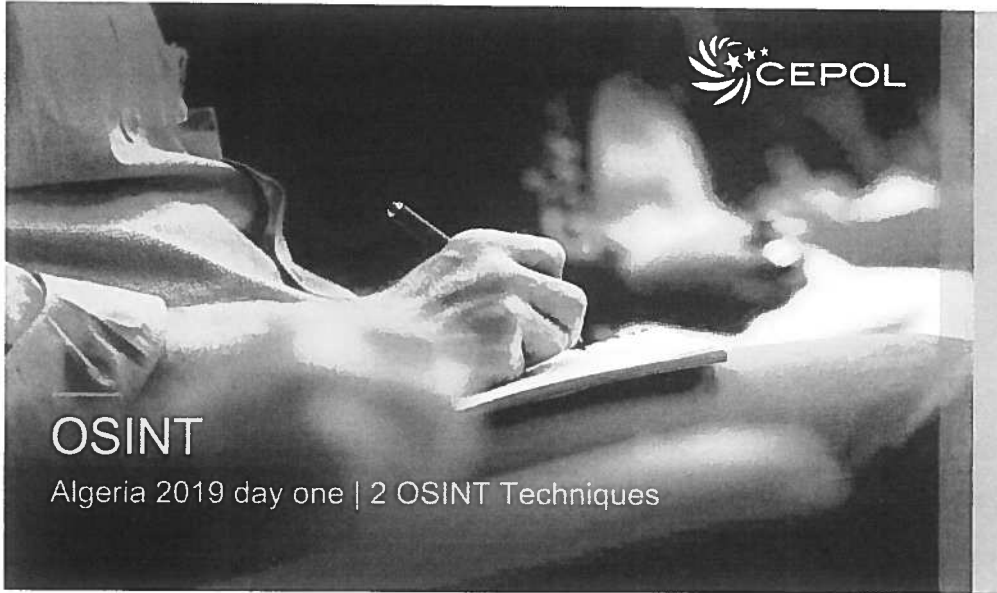
- 08:00 Prise en charge de la délégation CEPOL et des experts à leur hôtel
- 09:00 Enquêtes financières sur Internet I
- 10:45 Break thé ou café.
- 11:00 Enquêtes financières sur Internet II
- 12:00 Repas de midi.
- 13:00 Enquêtes financières sur Internet III
- 14 :00 Evaluation de l'activité résidentielle.
- 15:00 Cérémonie de fin de session – remise des certificats.
- 16:00 Fin de l'activité résidentielle.

Vendredi 26 Avril

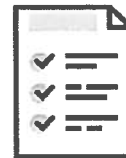
Départ de la délégation des experts vers l'aéroport. (à organiser au cas par cas avec nos hôtes algériens.

Cadres du Commandement de la Gendarmerie Nationale, devant prendre part au séminaire résidentiel sur le Darkweb, la recherche du renseignement sur les sources ouvertes (OSINT), social média, malware et les investigations numériques, prévu à l'ESGN/Zéralda, du 21 au 25 avril 2019.

N°	Nom & Prénom	Grade
01	[REDACTED]	Lt/Colonel
02	[REDACTED]	Lt/Colonel
03	[REDACTED]	Lt/Colonel
04	[REDACTED]	Lt/Colonel
05	[REDACTED]	Lt/Colonel
06	[REDACTED]	Lt/Colonel
07	[REDACTED]	Commandant
08	[REDACTED]	Commandant
09	[REDACTED]	Commandant
10	[REDACTED]	Commandant
11	[REDACTED]	Commandant
12	[REDACTED]	Commandant
13	[REDACTED]	Commandant
14	[REDACTED]	Commandant
15	[REDACTED]	Commandant
16	[REDACTED]	Commandant
17	[REDACTED]	Commandant
18	[REDACTED]	Commandant
19	[REDACTED]	Commandant
20	[REDACTED]	Lieutenant



OSINT (Open Source Intelligence)



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

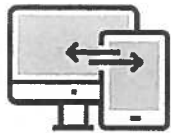


Photo validation

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

InVID Fake video news debunker by InVID

Proposé par : invid.project.eu

★★★★★ 13 | Actualités et météo | 12 461 utilisateurs

Ajouter à Chrome

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.

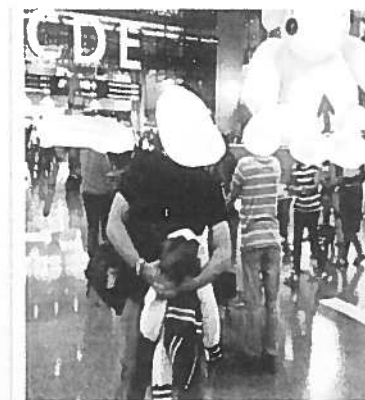
INTERNET ARCHIVE
WayBackMachine

Where is this?

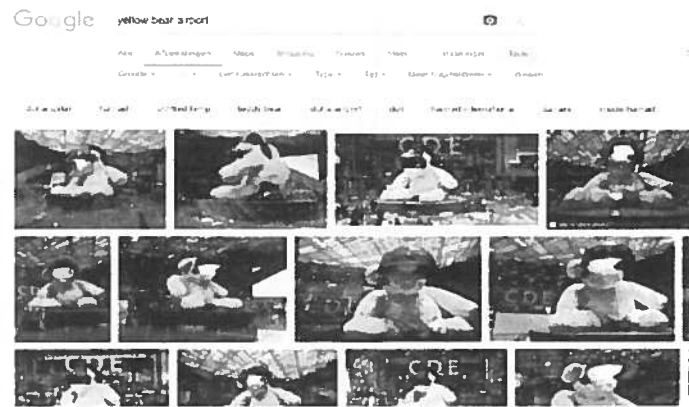
- This is one of the terrorists who drove into the crowd with a van in Sweden.
- A friend of him made this picture and posted it via social media online
- When looking with reverse image search it came back at a Facebook profile
- He didn't tagged it and also didn't gave it geo information



- 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.



Het vliegveld is in Doha, Qatar.

Shodan tutorial



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 (ISPs)
- 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



194.69.36.22 maildommail.ludth.de

Ports

Country	Europe
Organization	Ludthke Ludthke GmbH
ISP	AT&T Global Network Services Nederland B.V.
Last Update	2015-05-13T12:00:12.775249
Hostnames	maildommail.ludth.de
ASN	AS64183

Services

LIST

```

228 mail.in.immigration.net SMTP ready
250 mail.in.immigration.net POP3 AAA AAA AAA AAA AAA AAA AAA AAA
250 SIZE 37671800
250 8BITMIME
250 PIPELINED
250 AUTH PLAIN LOGIN
250 STARTTLS
250 VCLP
  
```

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



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 /x 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 Apache servers in San Francisco:

apache city:"San Francisco"

Find Cisco devices on a particular subnet:

cisco net:"216.219.143.0/24"

*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

6. Etc.

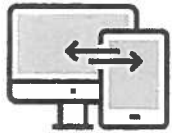
Combining filters

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**, you could use the following search query:

```
ip:"San Francisco" port:"8080" product:"Apache Tomcat/Coyote JSP engine"
```

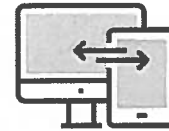
Check this out and play for yourself





OSINT techniques

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

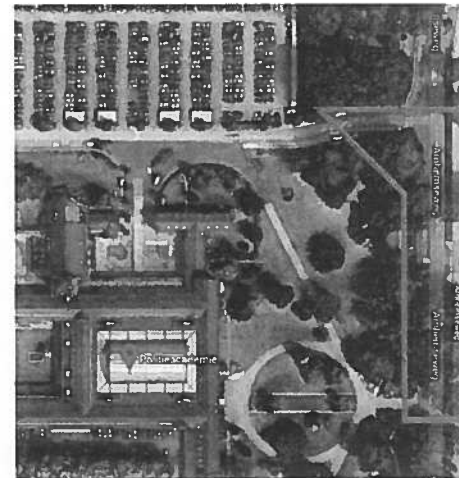


Wigle

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.

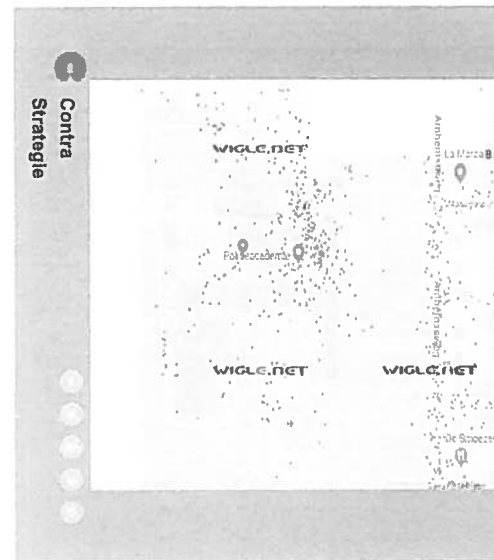
Tracking via WIFI

Some explanations:

MAC = unique adres from a device which identifies itself in this way

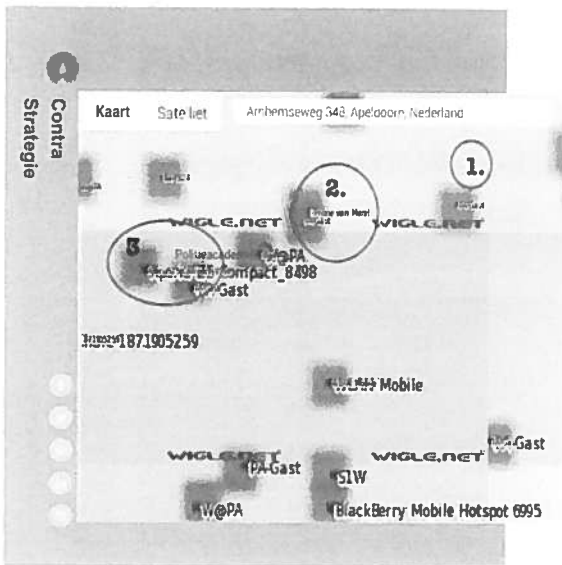
SSID = the network name (Service Set identifier)

BSSID = the MAC address from the access point (Basic Service Set Identifier)



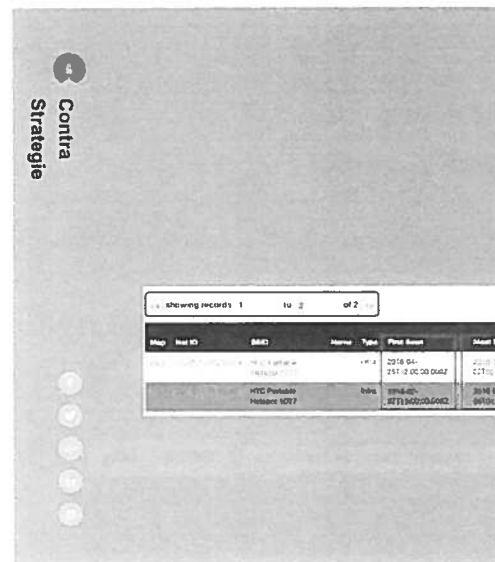
WiGLE WiFi test

Learn more [to wigle.net](http://wigle.net)



WiGLE zoomed in

Dutch Police backbone



WiGLE WiFi test

HTC Portable Hotspot 1577

WiGLE test

time: estimo

Map	Net ID	SSID	Name	Type	First Seen	Seen Recently	Country	Lat. Lon.	Est. Long.	Channel	Beacon	OSK
				wifi	2014-09-18T12:00:00.000Z	2015-01-21T08:00:00.000Z	nl	52.06314263 4.48097729		11	0	0
				wifi	2012-09-18T20:00:00.000Z	2014-09-18T13:00:00.000Z	nl	52.06368807 4.48870003		11	0	4
				wifi	2013-05-15T00:00:00.000Z	2014-09-18T14:00:00.000Z	nl	52.06310044 4.48265044		1	0	0
				wifi	2013-05-14T18:00:00.000Z	2013-05-14T18:00:00.000Z	nl	52.06368810 4.48960300		1	0	0
				wifi	2013-05-14T18:00:00.000Z	2013-05-14T18:00:00.000Z	nl	52.06368810 4.48960300		1	0	0
				wifi	2013-05-14T18:00:00.000Z	2013-05-14T18:00:00.000Z	nl	52.06368810 4.48960300		1	0	0
				wifi	2014-09-01T01:00:00.000Z	2014-09-01T01:00:00.000Z	nl	52.06368810 4.48960300		1	0	0
				wifi	2014-09-01T01:00:00.000Z	2014-09-01T01:00:00.000Z	nl	52.06368810 4.48960300		1	0	0
				wifi	2014-09-01T01:00:00.000Z	2014-09-01T01:00:00.000Z	nl	52.06368810 4.48960300		1	0	0
				wifi	2014-09-01T01:00:00.000Z	2014-09-01T01:00:00.000Z	nl	52.06368810 4.48960300		1	0	0
				wifi	2014-09-01T01:00:00.000Z	2014-09-01T01:00:00.000Z	nl	52.06368810 4.48960300		1	0	0
				wifi	2014-09-01T01:00:00.000Z	2014-09-01T01:00:00.000Z	nl	52.06368810 4.48960300		1	0	0

WiGLE test

The screenshot shows a web-based map application. At the top, there's a navigation bar with 'Home Map', 'My Maps', and 'About'. Below that, a search bar contains 'Den-Haag locatie'. The main area is a map with several red location pins. A callout bubble is positioned over one of the pins. On the right side, there's a sidebar with a 'Save' button and a 'Run Query' button. Below these, there's a 'Description' section and a list of 'Add markers for this' with various coordinates and a '0' next to each.

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 lot of criminal activities. They are showing their message

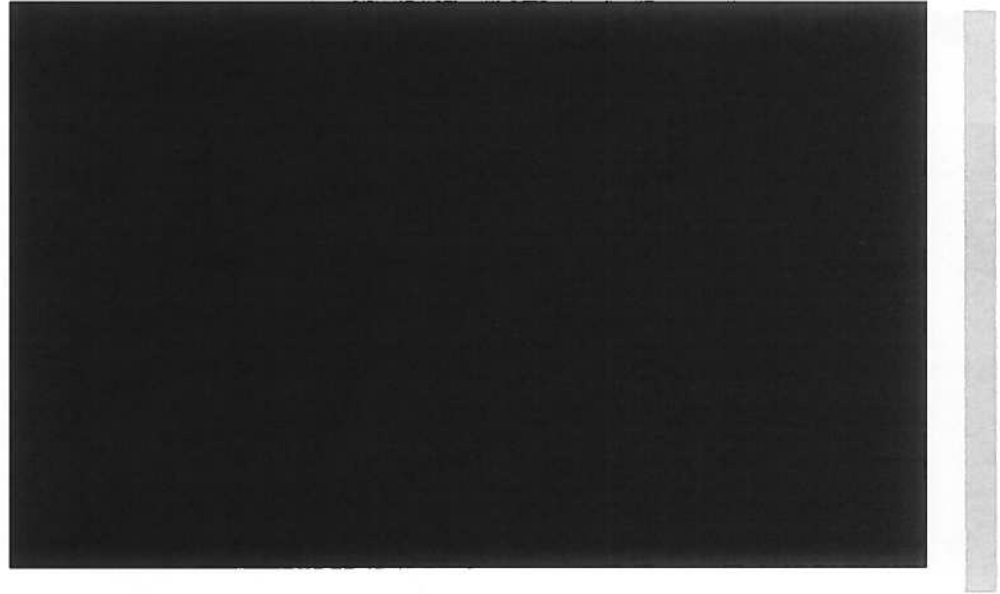
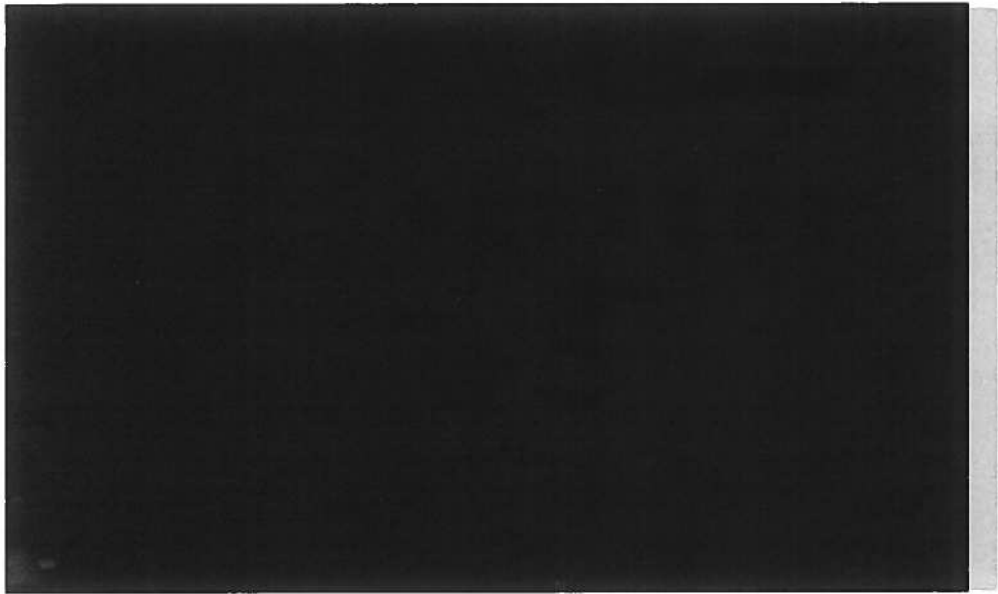


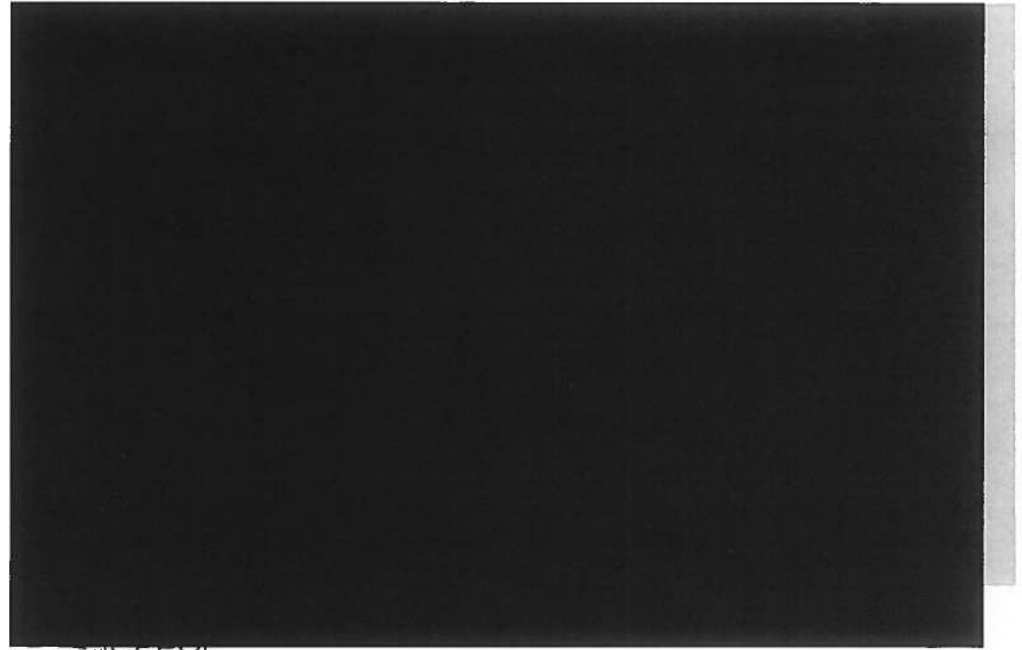
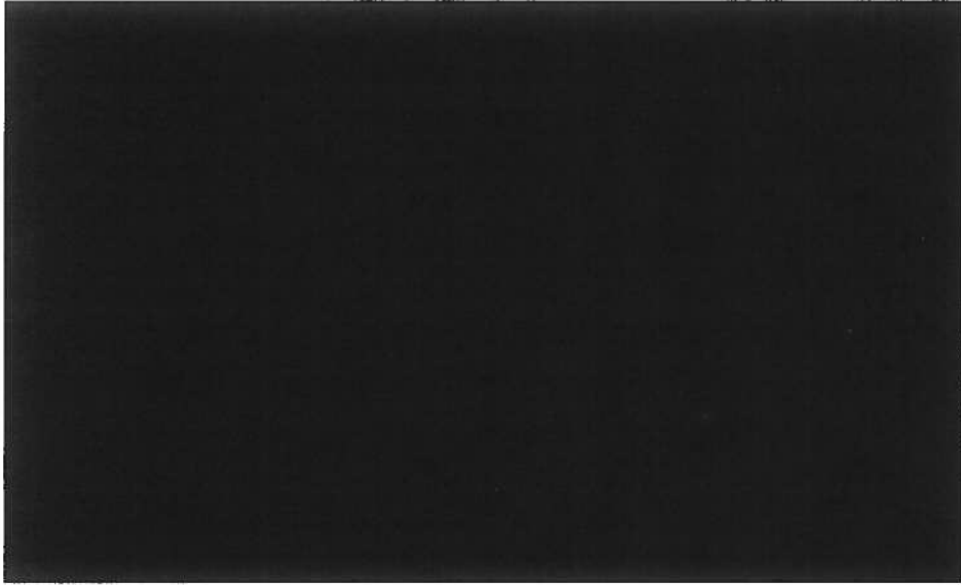
Instagram

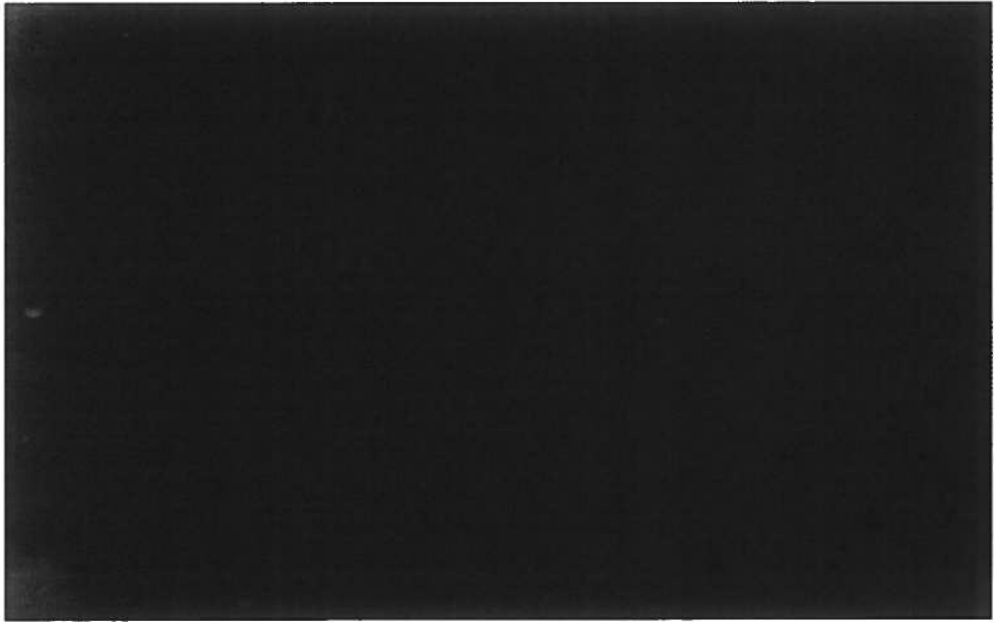
Instagram is used by a lot of people. And also criminals.

In Europe we see a vast amount of criminal activities

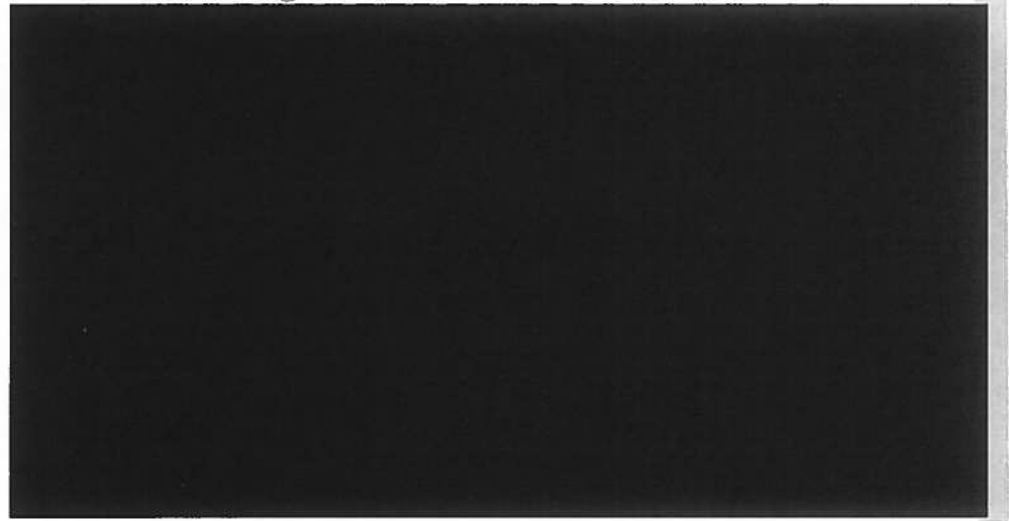








Crowdsourcing



Let's get over to my PDF from the case..

Airport OSINT

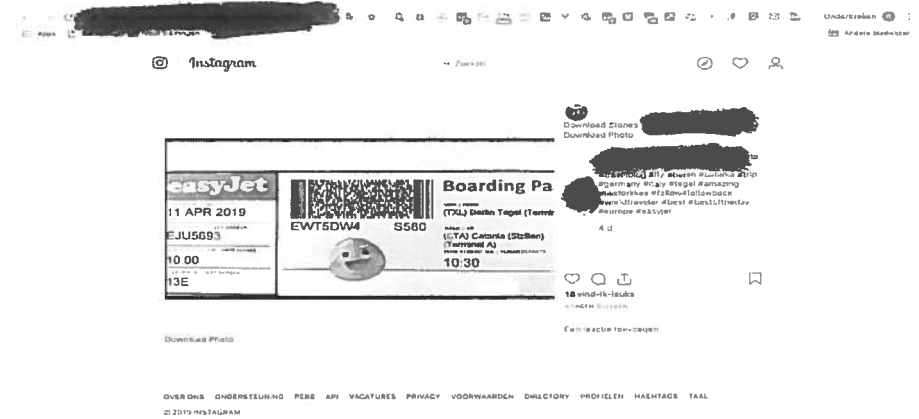


Airport OSI



Download Photo

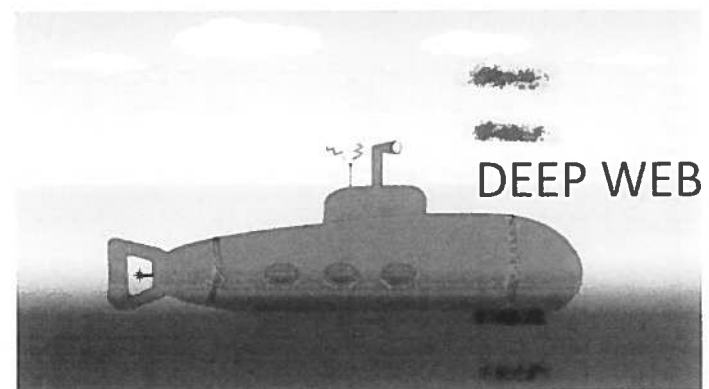
Using "goldmine" Instagram...



CEPOL

Social media gathering

GOOGLE DORK



1

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-ept 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 allows 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...

2

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

intitle
Find that word or sentences in the title of a website
intitle:search

inurl
Find that word or sentences in the URL
inurl:php?id=

related
Find that related websites
related:www.google.com

site
Restrict to a specific site
site:takesite.com

filetype
research by file type
filetype:pdf:shakespeare

OTHER OPERATORS FROM WIKIPEDIA

Operator	Purpose	Mixes with Other Operators?	Can be used Alone?	Web	Images	Groups	News
intitle	Search page Title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	specific files	yes	no	yes	yes	no	not really
intext	Search text of page only	yes	yes	yes	yes	yes	yes
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

3

Queries examples

This presentation is meant for educational purposes only

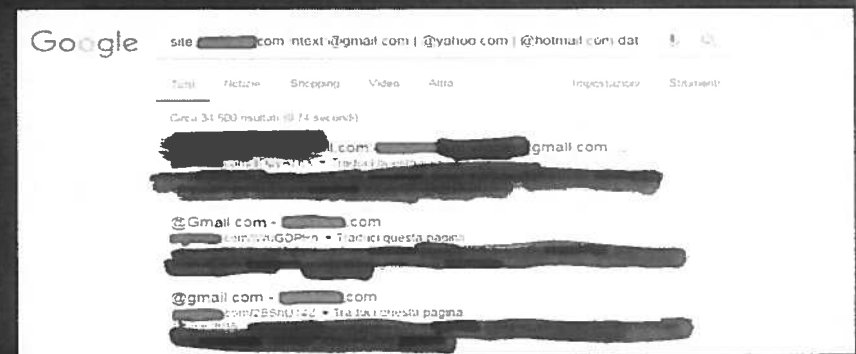
- Google Hacking Database - Exploit Database

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
- 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

Let's see those underlined...

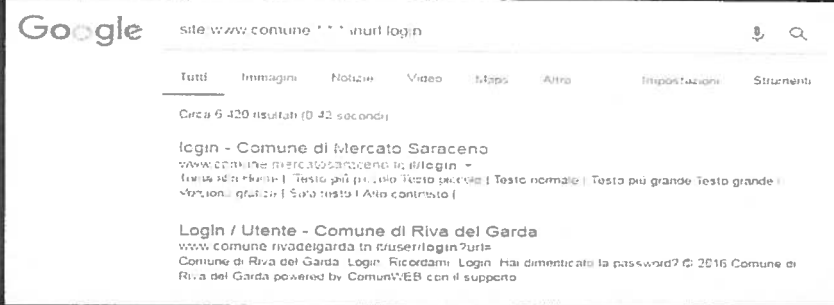
- File containing passwords example



site: [redacted].com intext: @gmail.com | @yahoo.com | @hotmail.com daterange:20170301-20170401

List of pastes (username and password) . Check your email status on haveibeenpwned.com by Troy Hunt.

Pages containing login portal example

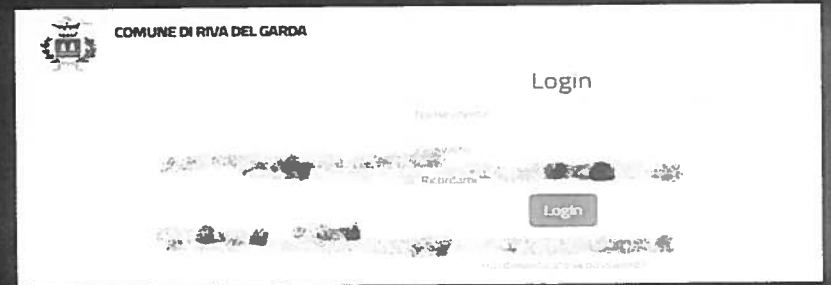


[site:www.comune.*.*.it/login](https://www.comune.*.*.it/login)

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.

Pages containing login portal example

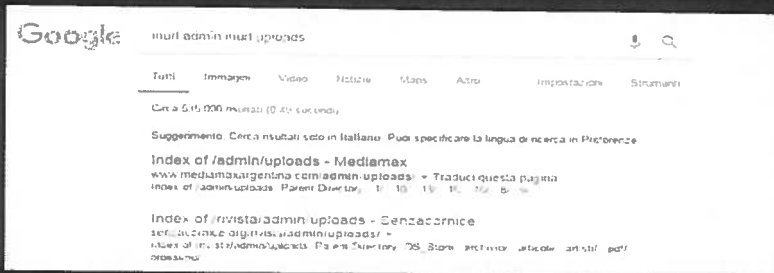


[site:www.comune.*.*.it/login](https://www.comune.*.*.it/login)

With a simple query, we could find "any" website's login page!

comune means municipality, district.

Sensitive directory example



[inurl:admin inurl:uploads](#)

The following folders probably contains sensitive data !

4

Conclusion

• 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?



```
[-] Checking username webbreacher on:
[-] 500px: Not Found!
[-] 9GAG: Not Found!
[-] About.me: Not Found!
```

<https://github.com/sherlock-project/sherlock>

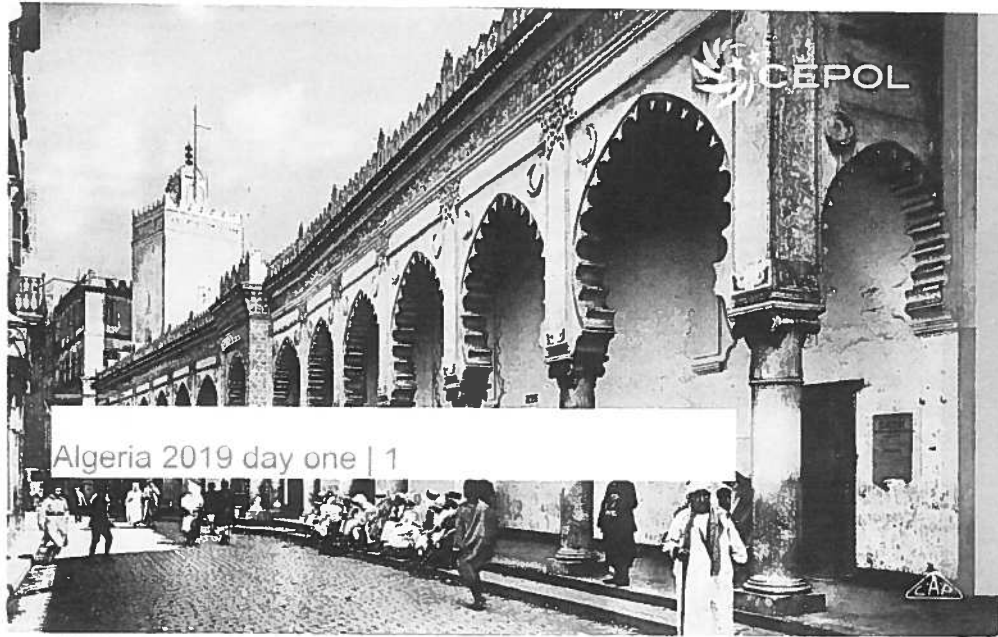
Thank you for your attention!

European Union Agency for Law Enforcement Training

Offices: H-1066 Budapest, Ózka 27., Hungary • Correspondence: H-1903 Budapest, Pf. 314, Hungary

Telephone: +36 1 803 8030 • Fax: +36 1 803 8032 • E-mail: info@cepol.europa.eu • www.cepol.europa.eu





Algeria 2019 day one | 1

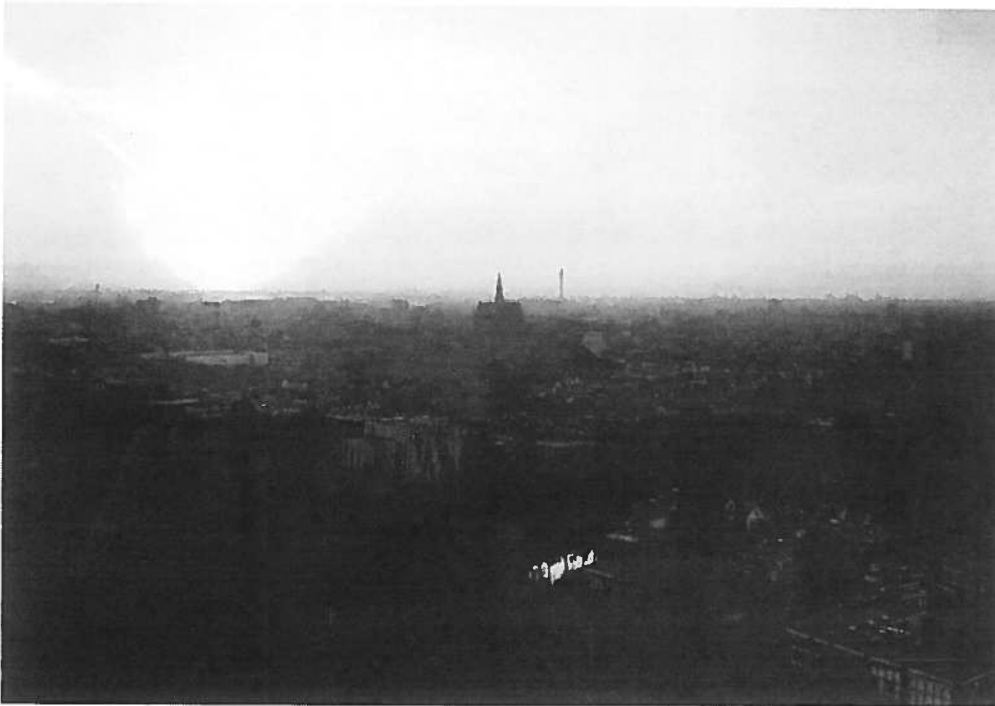
EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING



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

Did you know?

As of October 2018, There are more than 1.9 billion websites on the Internet



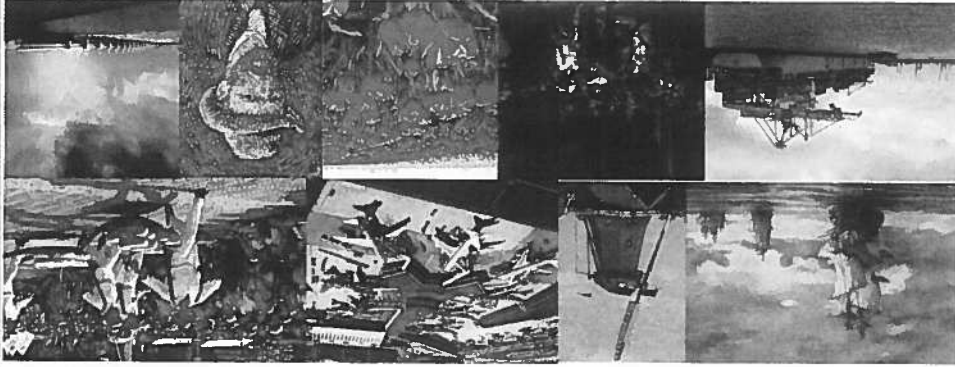
Algerian statistics



Algerian statistics



Introduction



Welcome to the Netherlands

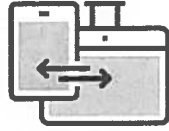


Ranking	Short name	Name	City	Established	Members	Throughput (Gbit/s) max	Throughput (Gbit/s) aver
1	DC-IX	Deutscher Commercial Internet Exchange	Frankfurt, Hamburg, Munich, New York	1995	610	4005	2523
2	AMS-IX	Amsterdam Internet Exchange	Amsterdam, Haarlem, Schiphol-Rijk	1997	710	3701	2293
3	LINK	London Internet Exchange	London, Manchester, Edinburgh, North	1994	624	2537	1813
4	NSK-IX	MASK-IX	Moscow, Saint Petersburg, Novosibirsk	1995	375	1557	746
5	Equinix	Equinix Exchange	Paris, Zurich, New York, Ashburn, Virg	1998	768	1409	990
6	Datalix	Data IX	Moscow, Saint-Petersburg, Novosibirsk, Various cities	2002	130	1240	756
7	NL-IX	Netherlands Internet Exchange	Various cities	2002	513	1021	619
8	Brazil Internet Ex	Belo Horizonte, Brasilia, Campinas, Gr. Brazil	Stockholm, Malmö, Sundsvall, Gothenb	2004	861	862	586
9	Nemod	Nemod Internet Exchange in Sweden	Stockholm, Malmö, Sundsvall, Gothenb	1997	64	947	510
10	W-IX	W-IX LTD	Moscow, Saint-Petersburg, Frankfurt, L	2008	143	695	469

Size, or what you want to do with it

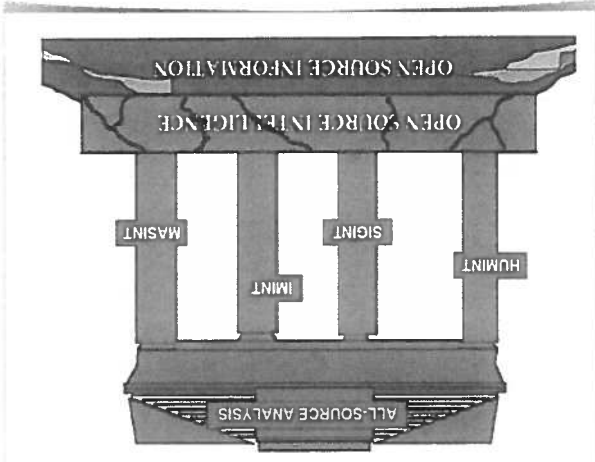
- Intelligence from publicly available information that is collected, exploited, and reported to address a specific intelligence requirement.
- One of many forms of "INT" (SIGINT, HUMINT etc)
 - "Open" refers to overt, publicly available sources (as opposed to covert or clandestine sources).
 - CIA: "Information does not have to be secret to be valuable"
- Social Media
- Sometimes called SOCMINT for SOCIAL Media INTelligence

What is OSINT?

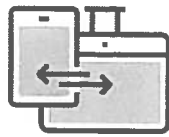


Cyber landscape



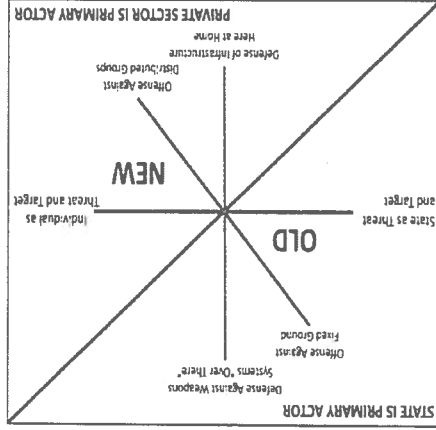


OSINT is a process and a red line in the process of intelligence gathering



What is OSINT?

- What professions can leverage OSINT data?
- Information Security
 - Private Investigators
 - Law Enforcement
 - Businesses
 - Attorneys
 - But basically, EVERYONE



Another area where OSINT is fundamental, is in relation to the new reality that war is less about state on state military power and more and more about distributed individuals each capable of shutting down entire power and communications and water networks.

Ultimately OSINT is about turning every citizen into an intelligence minuteman, and being on guard, openly, all the time.

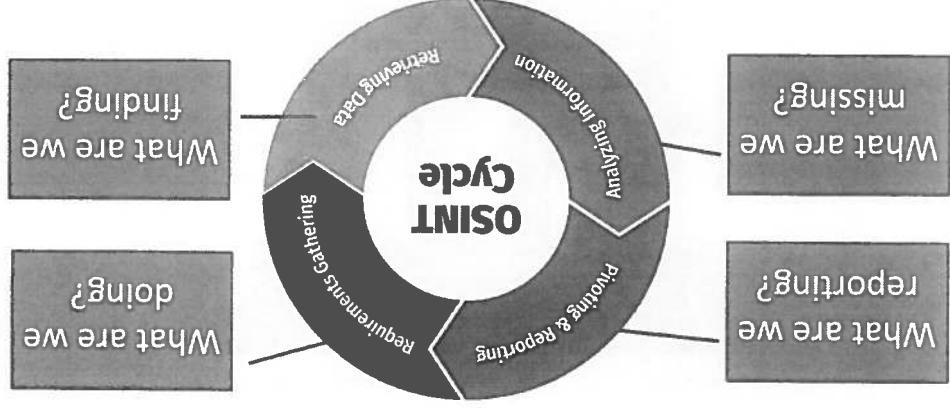
-Robert David Steele



- Overt information and accessible for everyone
- Spies only tell secrets, you do not (most of the time) need secrets
- Verification of information you've collected

Why does LE uses OSINT?

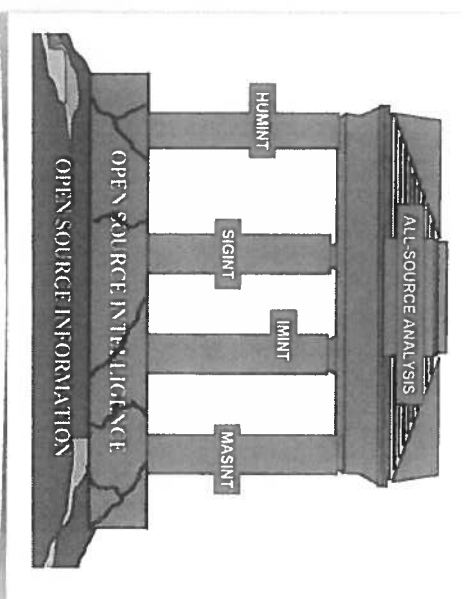
The OSINT proces



The OSINT proces | 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, symposia
5. **Commercial data**: commercial imagery, databases, financial assessments
6. **Grey literature**: technical reports, patents, working papers, newsletters

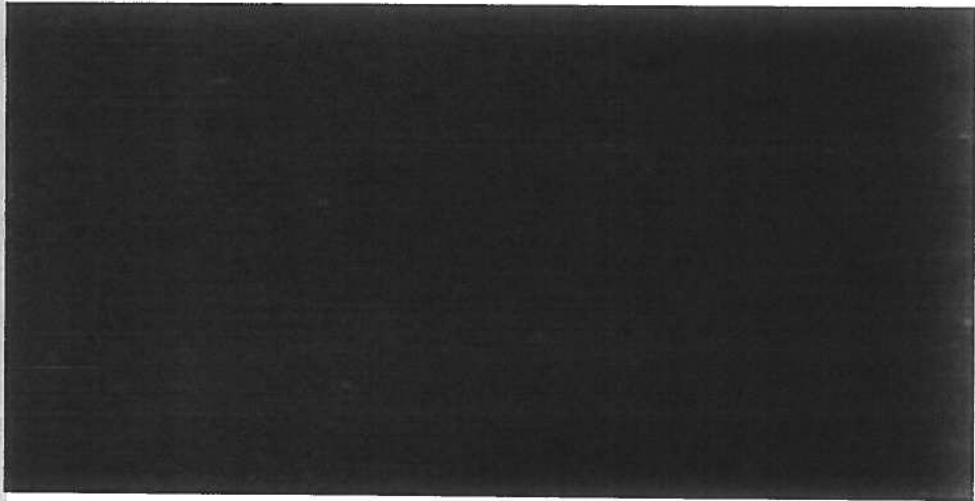
The relation of OSINT with other INT's



Types of OSINT

1. **Non-technical**: basically making use of the internet and other open sources without difficult technical knowledge
2. **SOCMINT**: social media OSINT
3. **Technical OSINT**: doing reconnaissance and search for IP addresses, dns information, port scanning etc.

Operational Security (opsec)



OSINT is HOT

Fingerprinting

You are leaving traces behind.

- Location 
- Software 
- Hardware 
- Connection 
- Social Media 



Operational Security (Opsec)

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?

- ## Fingerprint by correlation
1. Browser fingerprinting
 2. IP fingerprinting
 3. Time online or time zone settings
 4. Choice of words
 5. Behavior (browser habits/patterns)



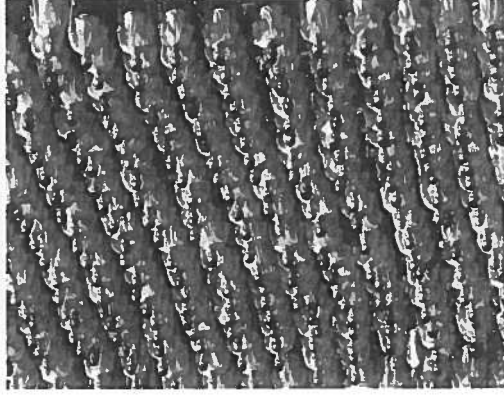
- ## Be mindful at all times
1. Adjust activities to threat level
 2. Residential internet or 4/5G?
 3. Proxy/VPN or TOR?
 4. Referrer on/off?
 5. User agents
 6. Tracking blockers?
 7. Do not login with a (fake) account in Google, Yahoo ets..
 8. What is the risk if an account gets compromised (connection with other accounts?)

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)



WIFI safe >>> ?

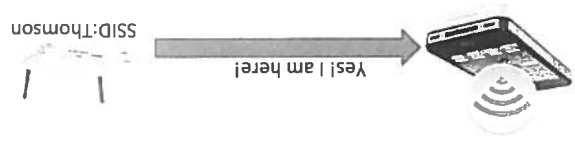


38

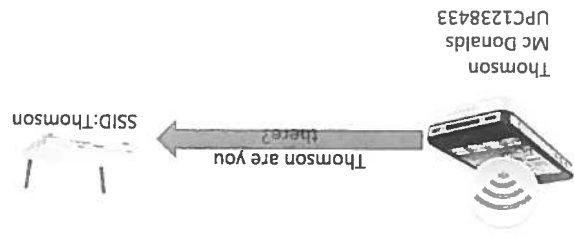


MAC-adres
60:D9:C7:2C:6A:D0

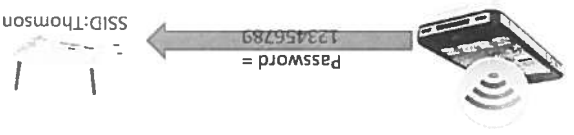
a MAC-adres (Media Access Control) is a unique identification number that is been assigned to any wireless device.



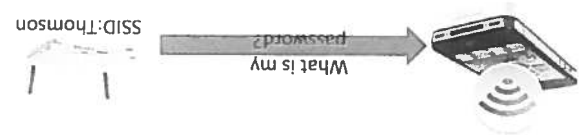
Probe request
Wifi handshake



Probe request
Building the network connection



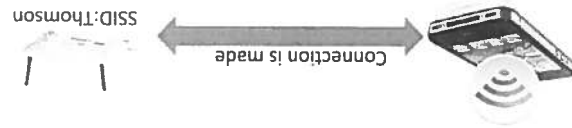
Probe request



Probe request



But what if someone is listening...

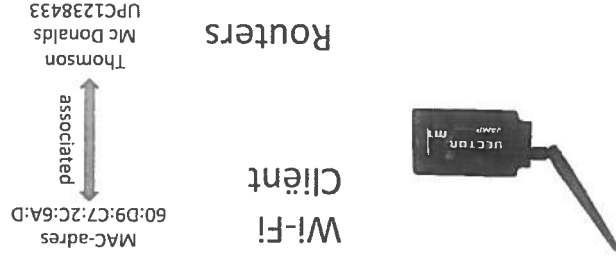


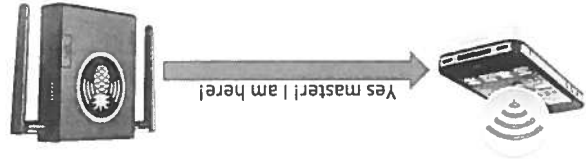
Probe request

Man in the middle - the theory

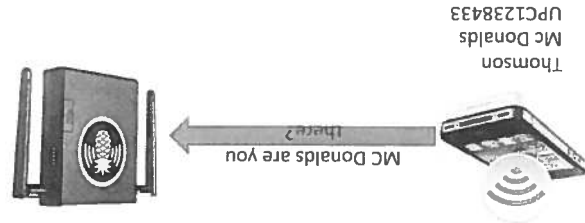


What can we detect?





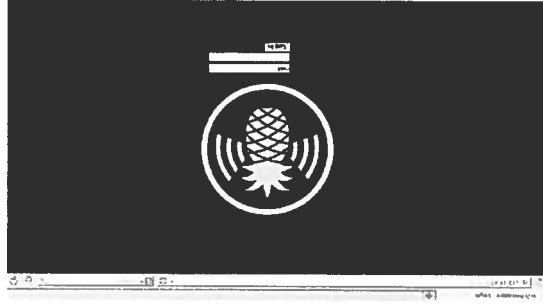
Probe request



Probe request

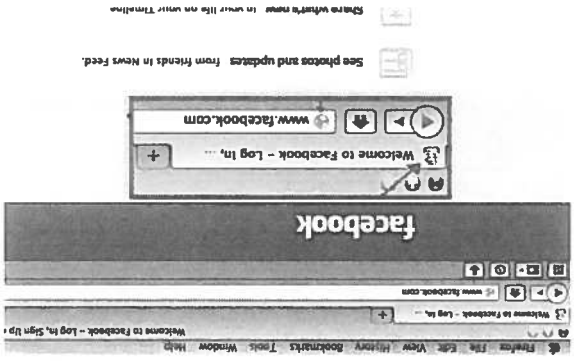


./pineapple - OpenWRT Linux



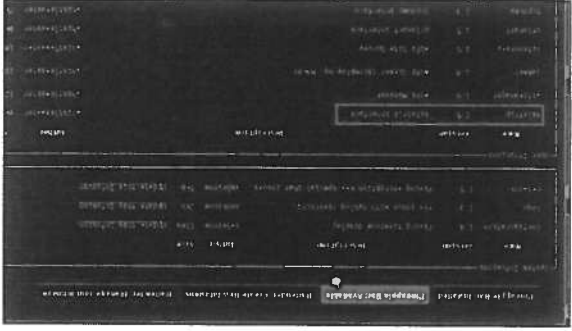
./pineapple - webinterface

Man in the Middle with SSL

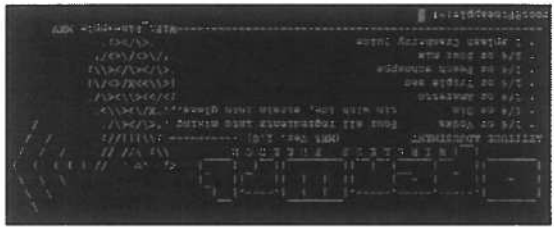


46

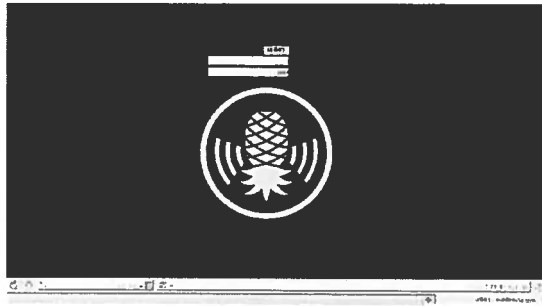
./dashboard (for skiddies)



45

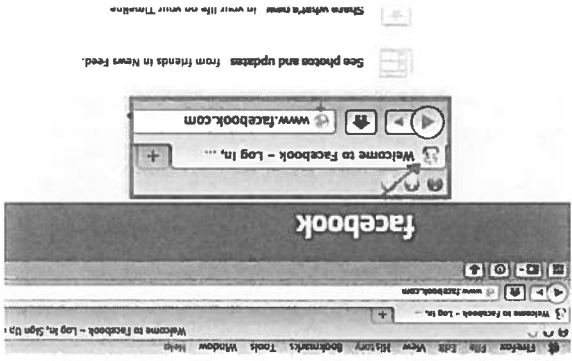


./pineapple - OpenWRT Linux



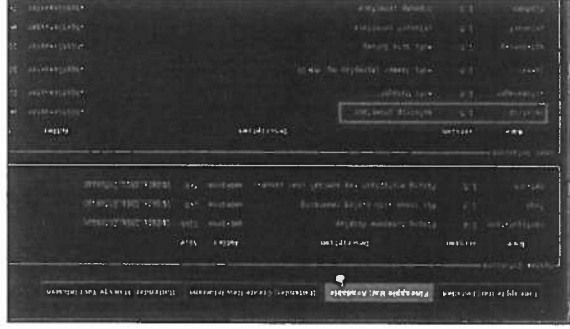
./pineapple - webinterface

Man in the Middle with SSL



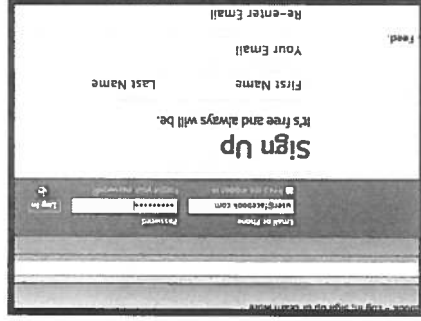
52

./dashboard (for skiddies)



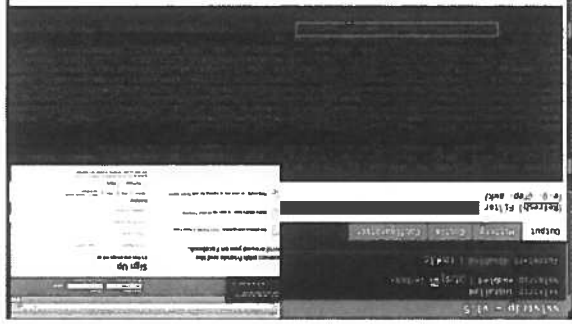
53

Man in the middle - Login



53

./Pineapple - credentials found!



54

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

Password manager



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

Fingerprinting



Great documentation Great reporting



Documenting



Types of OSINT Data

- Images
- Videos
- Downloads
- Web pages
- Text

- Analysis
- URLs
- Dates/times
- Command line
- tool output

Considerations

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

Number of teammembers

- How many people will contribute?
- Just you?
- Team, geographical spread
- Enterprise?

Considerations

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

Why are you documenting?

- Only for yourself?
- To use it in a product?
- We collect data and provide our analysis and recommendations



13

Documenting tools

Word Processors/Text Editors <ul style="list-style-type: none">• Report-writing• General documentation	Documenting Apps <ul style="list-style-type: none">• Meant for recording your work for you• Trail of your work
--	--



14

Visualizers <ul style="list-style-type: none">• Good for analyzing relationships between objects• Analyzing large data sets	Note-taking Apps <ul style="list-style-type: none">• Dedicated to recording (manually) notes on your work
---	--



Preparation of the workplace

49

- ### Prepping your workplace
- What kind of machine do you use, Windows, Linux, MacOS?
 - Do you want to work with a virtual machine?
 - What kind of distribution do you want to use?
 - Are you making use of smartphones to do research?
 - Who do you want to be? >> VPN/Proxy etc.

50



- Most flexible
- Most complete features
- Easiest to use
- Decrease our work

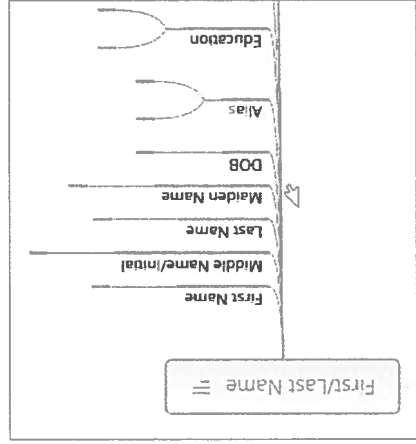
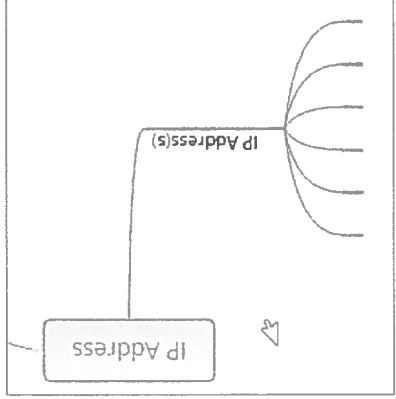
Let's focus!



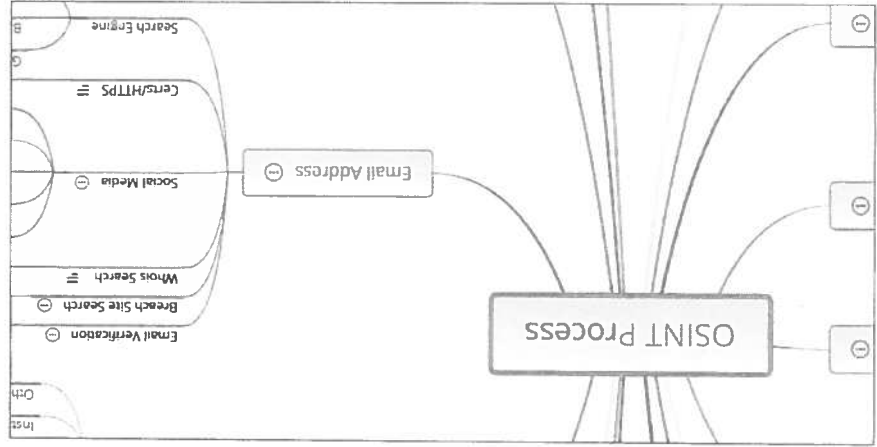
- Visual note taking
- Embed images and documents
- Some are multi-user

Mindmaps





Data collection tab



OSINT process tab



Hunchly

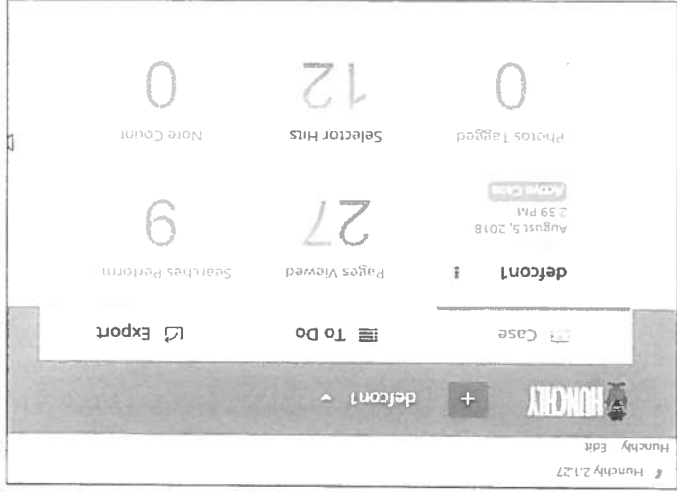
- Passively extracts data
- Automated recording of browsing
- Time-lining
- Hashing of images
- Downloaded files included
- Google Chrome extension
- Not expensive \$130 year



Mindmap con's

- Not always easy to look back in time
- Exporting the data isn't easy, especially with free mode
- Manual data entry proces





So, if you know

- Why you are documenting
- Where you are documenting
- Who you are documenting with
- Who you are documenting for

Then

- Find documenting tools that make things easier
- And work how you/your team do
- Many apps have trials or are free



What kind of software do you use?

- iBase (IBM)
- Analyst Notebook (IBM)
- XMind (opensource analytics application)
- Excel
- Something else



Let's get this party started....



77

How to get started?

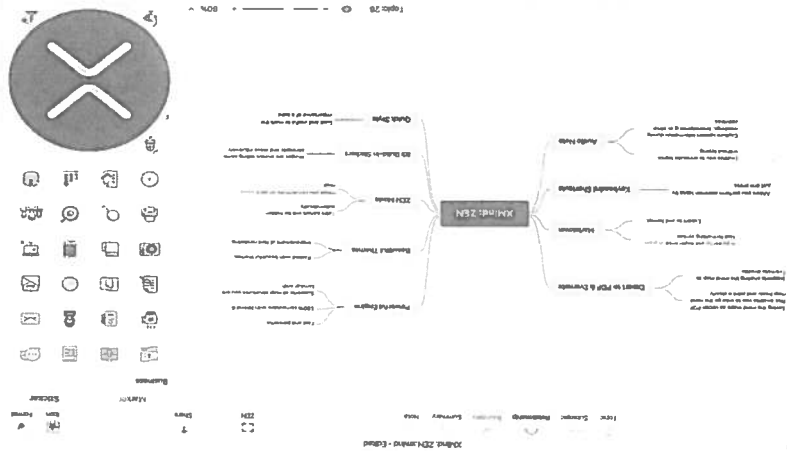
Go to coda.io with your gmail addresses. Each team has an address.

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

Just go on and play with it!



78



Creation of a sock puppet

- Do you already have a sock puppet account?
- When doing OSINT research, it's important to use a fake networking platform, especially on social profile, or what we like to call a *sock puppet* for operational security reasons.
- Who do you want to be online?
 - What/who are you researching?
 - How can you blend in, what about behaviour, ip address?



Name?

Look at your CODA doc. Over there you can find a link to FAKENAMEGENERATOR.

Take a look there and look how it works.

Got a cool name? Always do a quick search on the name. Just to make sure that your chosen name isn't the biggest criminal in history. Do the same if you've also selected a username. You can check a username just by using any search engine, or try namechk.com to see if your username hasn't already been taken.



Phone number

At a lot of platforms you need to verify yourself with a phone number. So it is very important to have one for your sock account.

Go to your local drugstore and buy a sim card. You don't need any extra's with it. So do not sign up or whatever.

Use different numbers for different accounts, otherwise the platform can get alarmed.



Photo

Sometimes you need to add a photo to your account. Most of the time a photo of a face.

- Select a stock photo. Paid or for free.
- Morph a couple of photo's to one photo. You can do that in Photoshop for example. But there are also websites like:

www.morphing.com and faceplusplus.com



Controlling you sock puppets


Most of the time you have more than one sock puppet, that's a challenge!

Use tools like [Rambox](http://Rambox.com) or meetfranz.com and a good password manager to keep your accounts connected.

Ofcourse you can also use Excel to administrate your accounts.

Interesting addons/extensions

 **HTTPS Everywhere 5.2.6**
Door CTF Technology Ltd

 **S3.Google Translator 5.26**
Door Oleksandr

 **Hoxx VPN Proxy 1.8.9**
Door Hoxx VPN

 **Change Referrer Button 0.44.1-signed.1-signed**
Door del.LPC

 **Resurrect Pages 3**
Door Anthony Lewellen

 **Random Agent Spooler 0.9.5.6**
Door gpm

 **Nimbus Screen Capture - editable screenshots. 9.1.1**
Door Nimbus Web

 **Reverse Image Search**
Door

Canvas Defender
Avatar: door @ www.rndbg.com

Instead of blocking jsAPI Canvas Defender creates a unique and perster

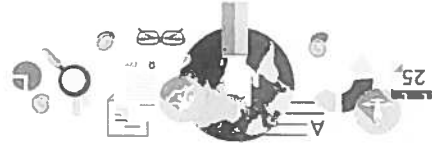
***** 88 *****

BeckyVid

Perform a search by type. Choose between the major search engines: Google, Bing, Yahoo!, Firefox and Duck



85



25

Controlling you sock puppets

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?

What you can also use is ifttt.com recipes to automate activation with your accounts. eg. let ifttt twitter posts from instagram etcetera.

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



86

**Make regular back-ups
Do not re-use your passwords**

Thank you for your attention!

European Union Agency for Law Enforcement Training
Offices: H-1066 Budapest, C/ura 27, Hungary • Correspondence: H-1903 Budapest, Pf. 314, Hungary
Telephone: +36 1 803 8030 • Fax: +36 1 803 8032 • E-mail: info@cepol.europa.eu • www.cepol.europa.eu



Financial investigations

and the internet





OSINT stream today

1. Introduction
2. Crime & Algeria
3. Bitcoin laundering

Money Laundering

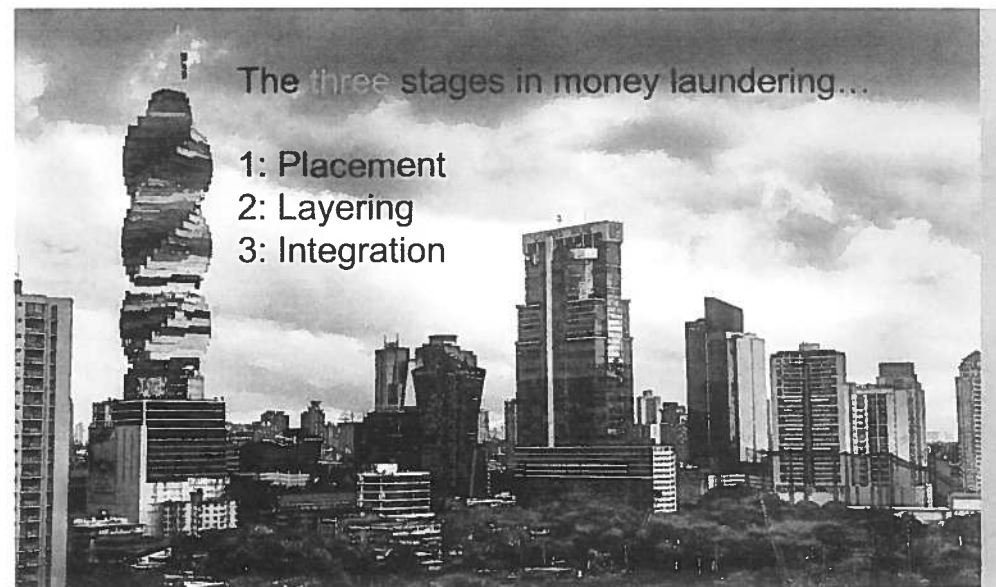
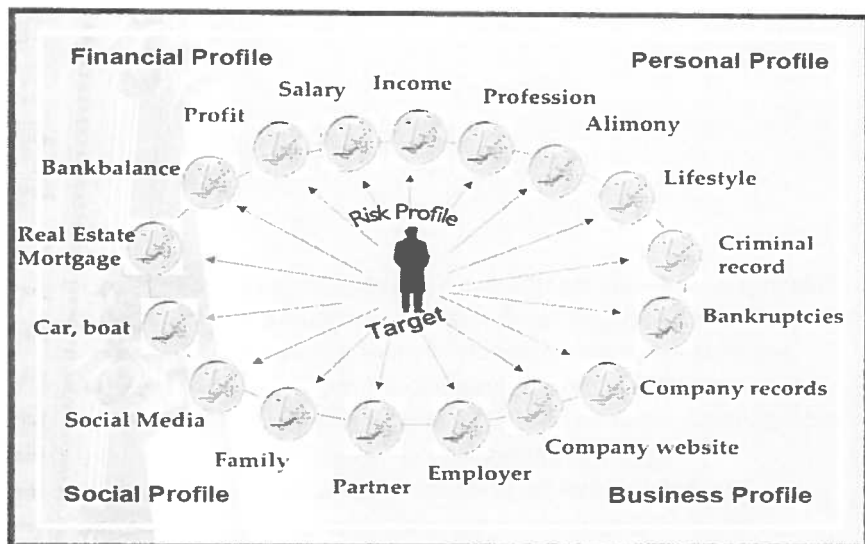
Money laundering is the **process** of taking 'dirty' funds and converting them into 'clean' funds allowing the criminal / fraudster uninhibited and untraceable enjoyment of his funds.

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 moneylaundering 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'



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



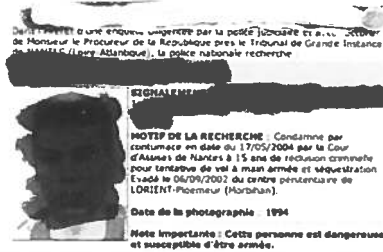
13



14

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.



LA VACHE À LAIT VERSION ALGÉRIENNE

[Panama papers]



Data breaches which are shared on the internet

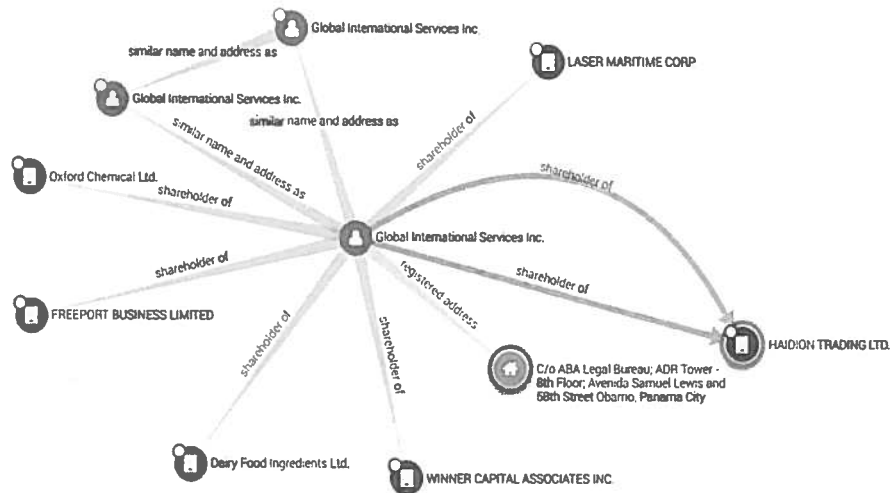
- More and more data leaks
- With a lot of sensitive data
- Internal leakages are very dangerous and could expose a lot of secrets

You can use them to do research against criminals

Panama Papers

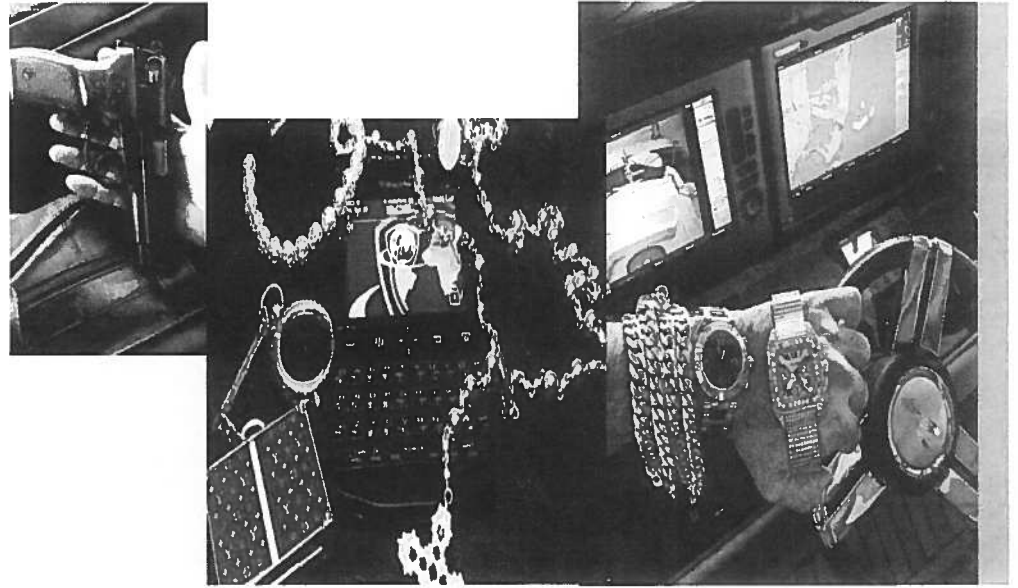


Algeria launches money laundering probe on back of Panama Papers



How can we leverage internet data (OSINT)?

- Companies data
- Chamber of commerce data
- LinkedIN profiles
- Websites
- Email addresses
- Social media profiles in general



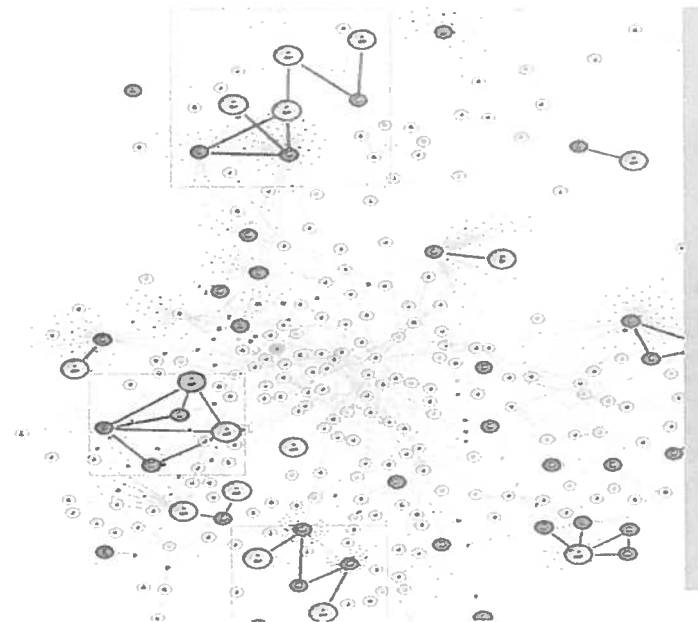
Upperworld
Bovenwereld



Middle world
Tussenwereld



Underworld
Onderwereld



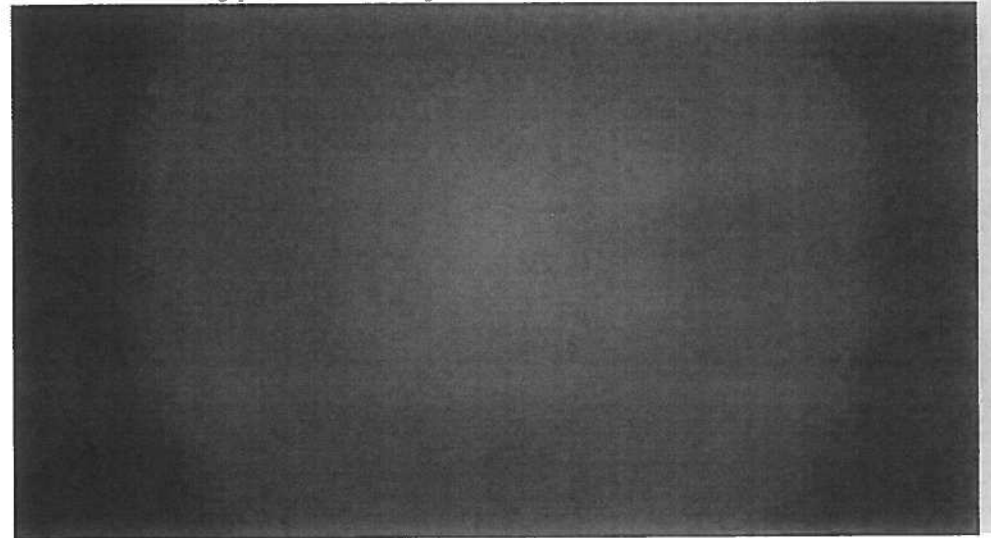


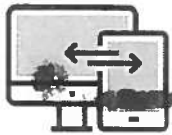
Follow the money

“Bitcoin” laundering



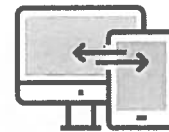
What is a cryptocurrency?





Crypto currencies & Terror/Crime

1. **Bitcoin**; is used to conduct funding campaigns for terrorism. GRU 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

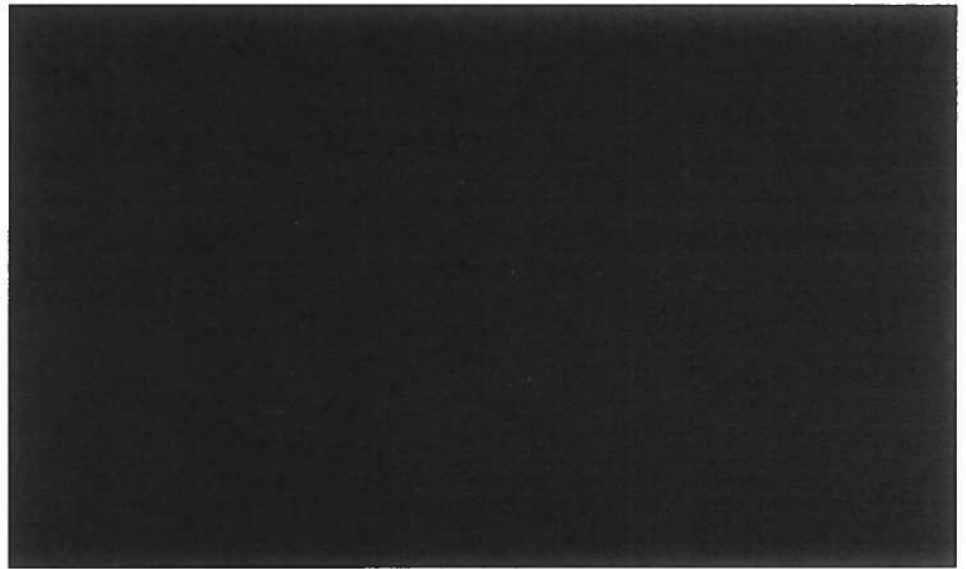
[REDACTED] Jan 19
if anyone has a Bitcoin ATM in your area or country, then you can send money to the mujhdeen 100% anonymously with cash. It is really that simple. Look at coinatmradar.com for your nearest Bitcoin ATM, Inbox [REDACTED] for more help.



Bitcoin ATM Map – Find Bitcoin ATM, Online Rates
Find Bitcoin ATM locations easily with our Bitcoin ATM Map. For many Bitcoin machines online rates are available.
coinatmradar.com



[REDACTED] Jan 11
Just seen a brother with one arm going to fight the regime in Hama, what is your



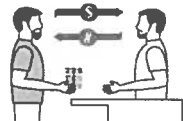
Hawala banking

An ancient system of money transfer

How hawala works

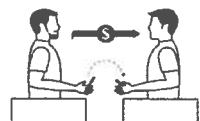
Hawala is a legal but informal means of transferring money across the globe.

STEP 1
In Country A...



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

STEP 2
Hawaladar A to B...



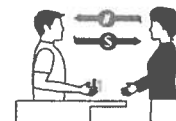
HAWALADAR A HAWALADAR B
Hawaladar A tells a counterpart in country B how much cash has been received.

STEP 3
Sender to Recipient...



SENDER RECIPIENT
Sender passes the code to the recipient, saying how much cash was handed in.

STEP 4
In Country B...



HAWALADAR B RECIPIENT
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

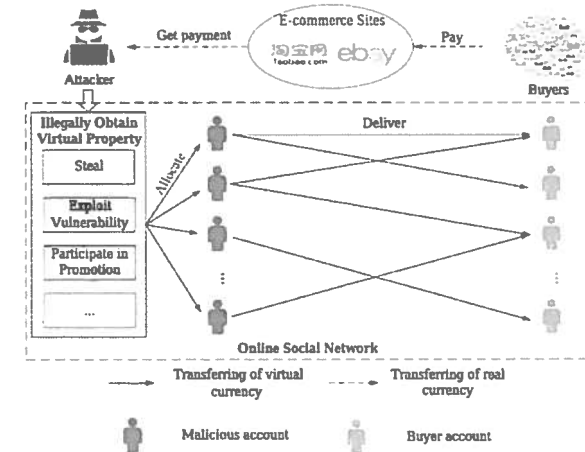
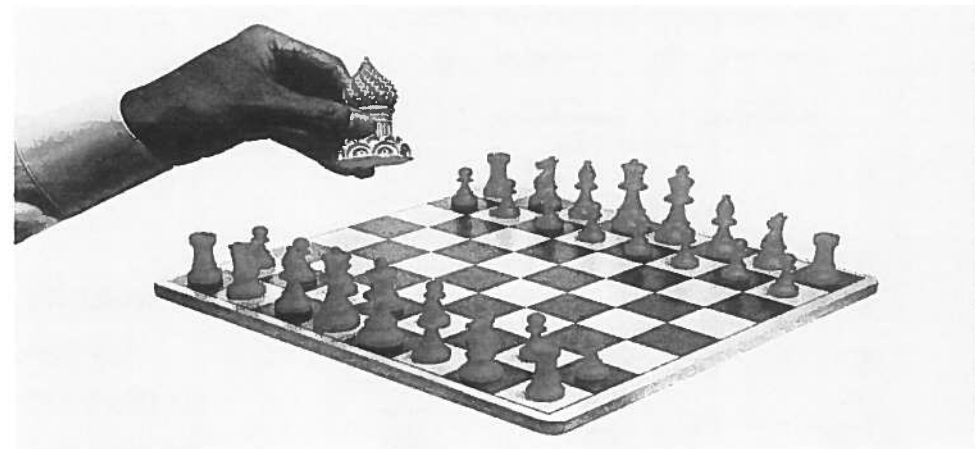


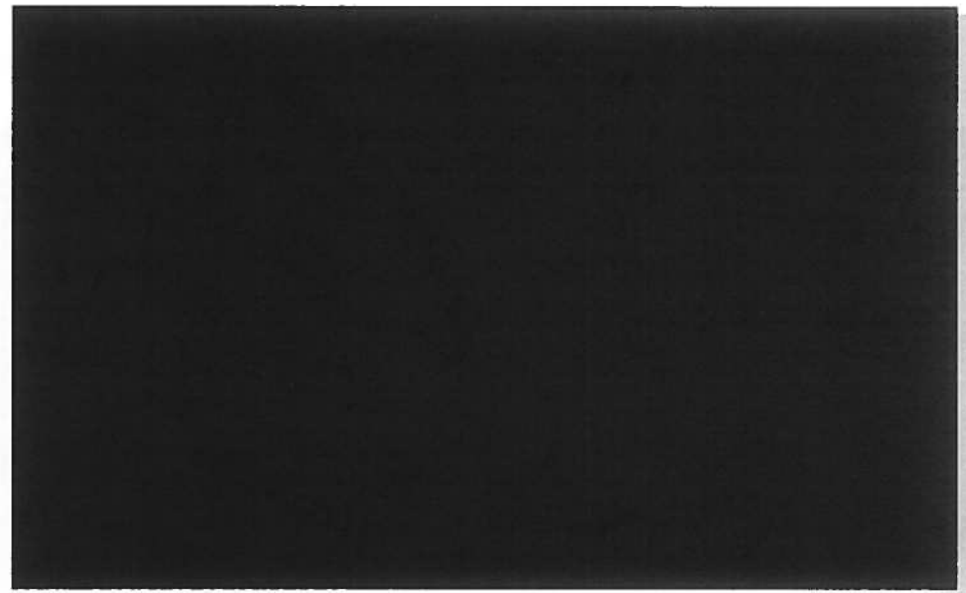
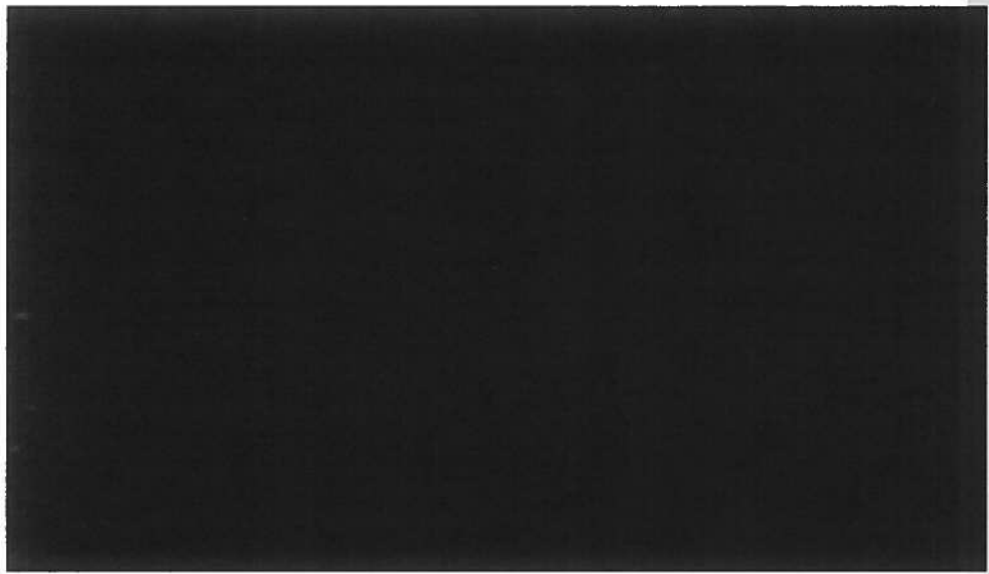
Figure 1. Malicious laundering process of virtual currency

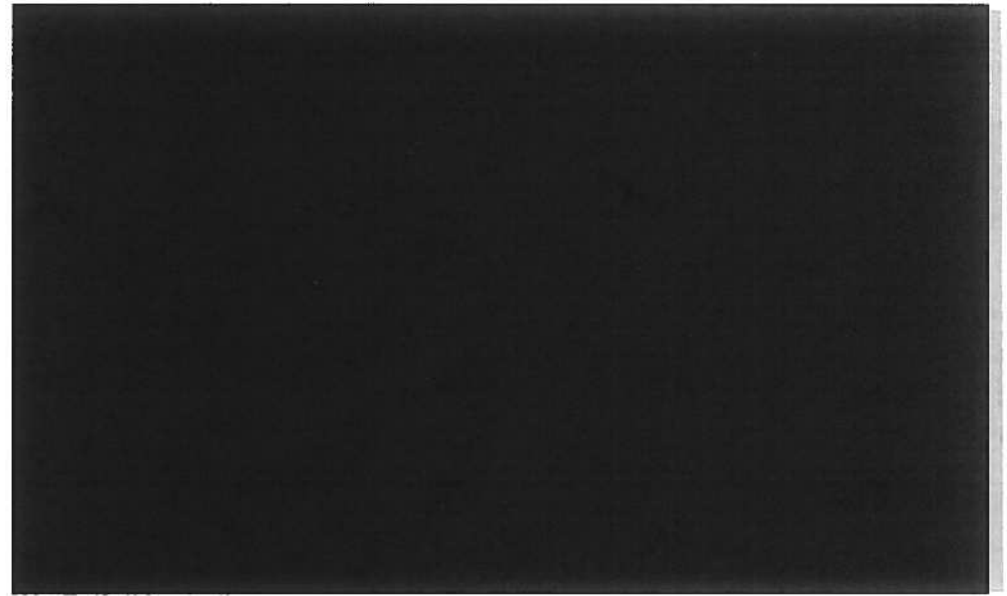
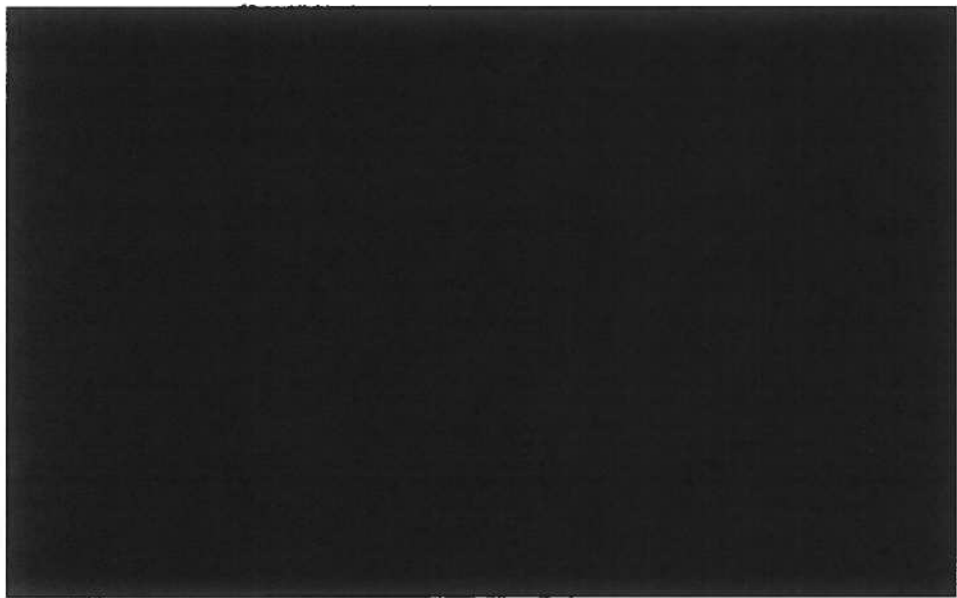
1. Collect virtual currencies with zero or extremely low cost. eg attacker can hack users' accounts, exploit the system vulnerabilities, or participate in online promotion activities to win virtual currency for free.
2. Attract potential buyers with high discounts, through various ways such as spreading spams and posting advertisements. And then sell the virtual currency in popular e commerce websites lik 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.

Case study Mueller indictment









Preparation

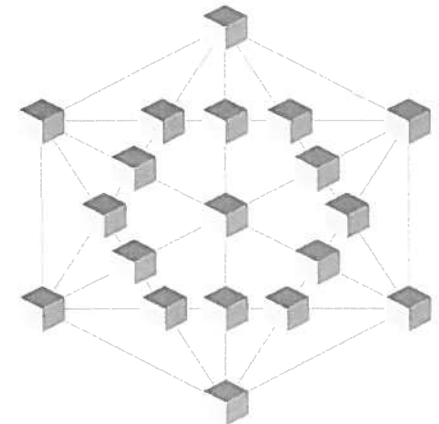
What do you need to use in this investigation?

<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.



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

Summary	
Number Of Transactions	2175
Output Total	116,528.86063148 BTC
Estimated Transaction Volume	6,089,948,40061 BTC
Transaction Fees	0.45890815 BTC
Height	396103 (Main Chain)

Hashes	
Hash	00
Previous Block	00
Next Block(s)	00
Merkle Root	34d2e77c23d0c55900ae92512be133356b6020071a693a16b0ec3c56b

Eventually

Transaction View information about a bitcoin transaction



Looking further into the transaction from block 396123, at 11:13:42, 1Qv8aKtQoiY5M5zkaG8RWL

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

tec)



Let's do it yourself!

- Check out the website blockchain.com
- And have a look at the possibilities



What to use in this investigation

- <https://www.blockchain.com/explorer>

- <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/> 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 as well as 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 Bitcoinwhoswho, 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



1b21218a2d4c10135666d570e07967b45f314eaf5d278a2c947d170e41ac44

1Nj3y... → 3PaPWymUexhewHPczmLQ8CMYatKAGNj3y

2019-02-01 15:49:06

0.13747974 BTC

0.13747974 BTC

On February 1, 2019, 0.13747974 BTC was sent from bu1s and another address ending in 3e

Bitcoin Address

Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	3AscCY9Uc8nc5rMkq95TLnJjZs5PDX3eVc	No. Transactions	2
Hash	64bb92ba08d8fa07639570fd7569c5a36100be4d	Total Received	4.6516693 BTC
160		Final Balance	0 BTC



Request Payment Donation Button

If we dive deeper into 3eVc 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 bu1s, and therefore, is also connected to Binance.

WalletExplorer.com: smart Bitcoin block explorer

Search address/wallet id/firstbits

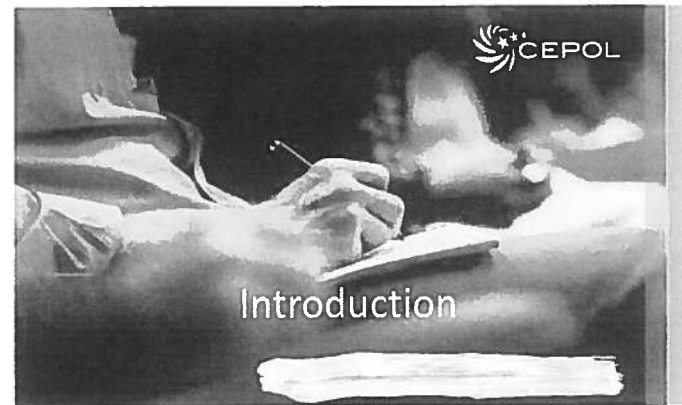
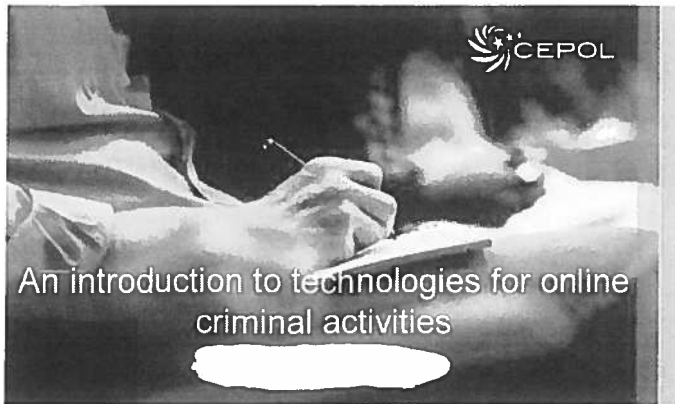
Wallet **[0000b55c1]** (show transactions)

Page 1 / 649 Next... Last (total addresses: 64 869)

address	balance	incoming txs	last used in block
3AscCY9Uc8nc5rMkq95TLnJjZs5PDX3eVc	9247.72370245	326786	567246
1711zow3JEra1Bka3y1b25Lfo3E18A9b14	0.	2	567123
bc1q075uwp0z0k3j2w92A09Y9zr1d5w0z7x0Zzch	0.	2	566891
1K6Bt19a30j8a6c92uoc0CwZm0a30f1f105	0.	2	566299
1D5tC91NWh0jP27W6C0mD2u1P6b0z1Y2	0.	2	565322
1Q11029ny1L8m020c1J8Z8W0b0ny1Z	0.	2	565317
3NtW01ef9vz130w0P9m13c4b0fny	0.	2	565240
1B4j6Aw1L5y9aZ55E2cG9a0u10k0Zm021	0.	2	565177
bc1q3t0r437cA0s027w9R90v0z1z0b0k7k00R11n	0.	2	565169

Thank you for your attention!

European Union Agency for Law Enforcement Training
 Offices: H-1066 Budapest, Örtica 27., Hungary • Correspondence: H-1903 Budapest, Pf. 314, Hungary
 Telephone: +36 1 803 8030 • Fax: +36 1 803 8032 • E-mail: info@cepol.europa.eu • www.cepol.europa.eu



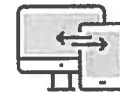
EUROPEAN UNION + G20 + G77 + AFRICA + ASIA + OCEANIA + TRADING

EUROPEAN UNION + G20 + G77 + AFRICA + ASIA + OCEANIA + TRADING



Agenda

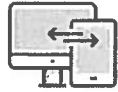
- OSInt
- *Terrorist use of internet (and Darknet potentialities)*
- *TOR Marketplaces*
- *Crawling Tor*
- *Introduction to crime data mining*
- *Investigative analysis of Tor Marketplaces data*



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

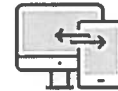


Intelligence

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

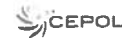


1

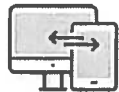


OSINT

- 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



2



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



3

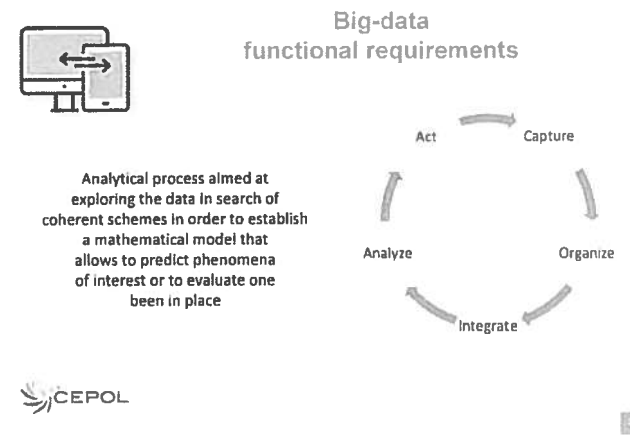
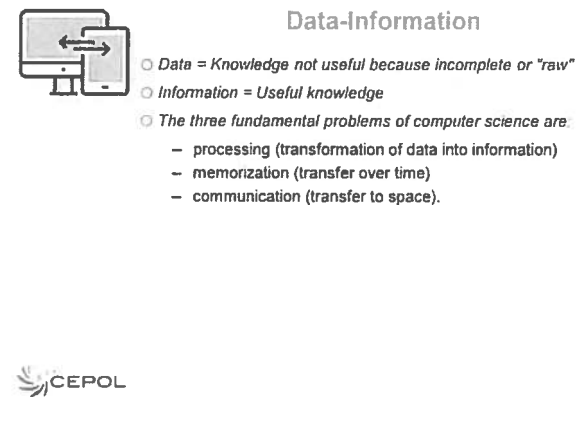
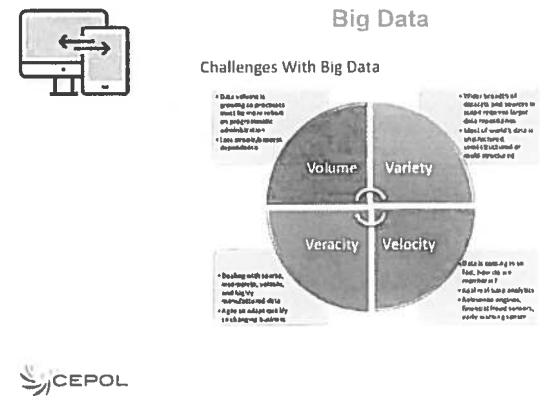
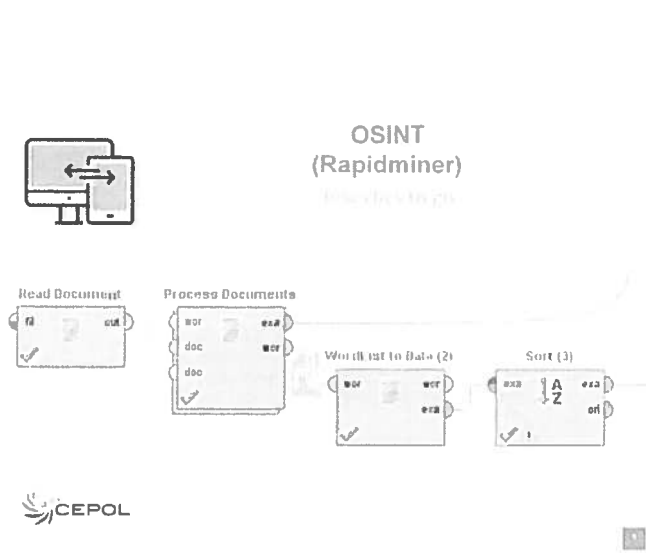


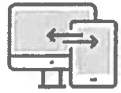
OSINT

- RumiyaH 10
- Worldsclooud.com



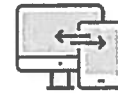
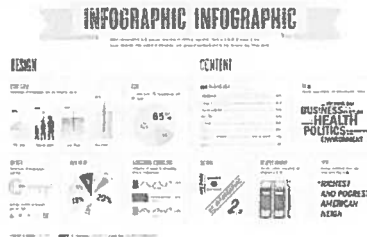
4





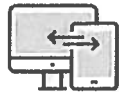
Big data mining

- 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 knowledge.



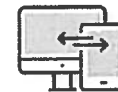
OSINT in place

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



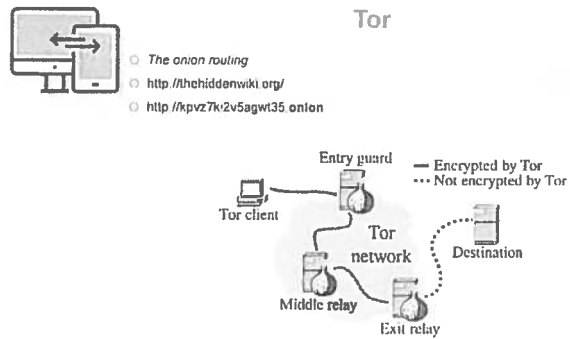
OSINT and REPUTATION

- 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





Data extraction techniques

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

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



Data extraction techniques

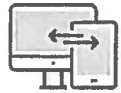
- Official Web APIs
- advantages
 - Ease
 - Rich documentation
- disadvantages
 - Structural limits



Captchas

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





Tools

- OPEN SOURCE INTELLIGENCE TOOLS AND RESOURCES HANDBOOK



https://www.i-intelligence.eu/wp-content/uploads/2018/06/OSINT_Handbook_June-2018_Final.pdf



<https://www.osinttechniques.com/osint-tools.html>

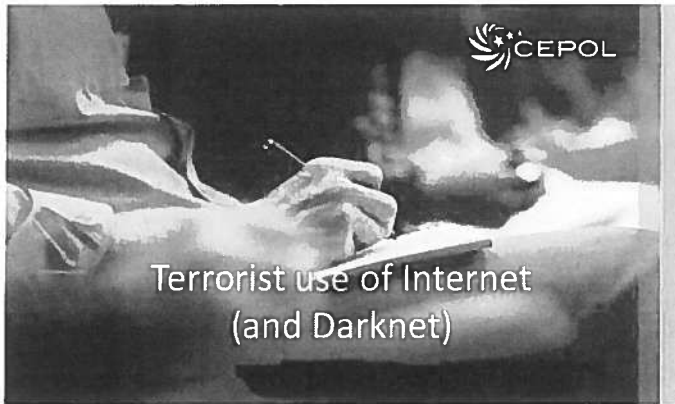


Means by which the Internet is utilized for terrorist purposes



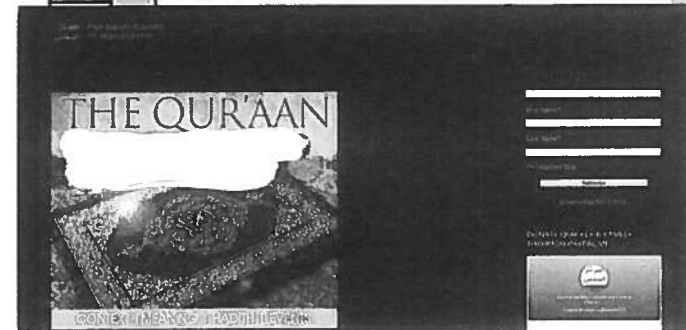
- Propaganda
 - Recruitment
 - Incitement
 - Radicalization
- Financing
- Training
- Planning

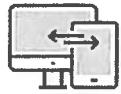
https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf



EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

Means by which the Internet is utilized for terrorist purposes



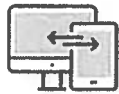


radicalization

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



radicalization



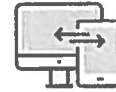
1. The growth of the Internet did not correlate with a rise in lone-actor terrorist activity year-on-year from 1990 to 2011.
2. There is a growing trend amongst lone-actors to make use of the Internet. In other words, whilst the Internet has not caused a growth in numbers of lone actor terrorists, it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



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



radicalization



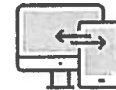
4. The non-US based offenders were significantly more likely to learn through virtual sources.
5. Offenders who interacted virtually with co-ideologues were significantly less likely to successfully carry out a violent attack.
6. Offenders who made use of online tools to prepare for an attack were significantly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

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



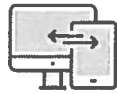
radicalization

facebook.



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





Financing

- 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).

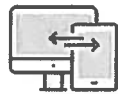


Financing

- growing link between cryptocurrency and terrorism, due to the evolution of either criminal or terrorist groups' financing means and capabilities. The 2018 FATF report, referring to the Joint FATF/Egmont Group analysis on 106 case studies', demonstrates that third parties financial entities (especially Shell Companies) are a key feature in the schemes designed to disguise ML or TF, dividing them into three groups:
 - Shell company: incorporated company with no independent operations, significant assets, ongoing business activities, or employees.
 - Front company: fully functioning company with the characteristics of a legitimate business, serving to disguise and obscure illicit financial activity.
 - Shelf company: incorporated company with inactive shareholders, directors, and secretary, left dormant for a longer period even if a customer relationship has already been established.

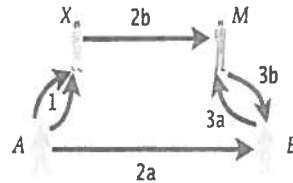


*S. Shay (2002) Somalia Between Jihad and Restoration. Taylor & Francis Group, New York



Financing

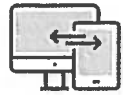
- The funding of terrorist activities often requires funds to be moved within or across countries. This might be done through official channels of the financial market and money remittances, through unregulated channels (e.g. online) or with the use of cash couriers (e.g. through hawala).
- In particular, unregulated channels and hawaladar can receive strong facilitation benefits by using anonymous networks (e.g. the well-known site Isdarat 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 legit front organizations or religious centers to disguise and launder their illegal financial activities: the **Dawa infrastructure**
- In some cases, the Dawa infrastructure is established around charity organizations (exploiting the Islamic values of charity donation: zakat and sadaqah) which are publicly represented by non-profit companies, Islamic education centers, and hubs for fundraising event
- cryptocurrencies are introducing new forms of crowdfunding, making, in most cases, a clear distinction between crowdfunding online campaigns to finance terrorism behind a false intent and those made for explicit militaristic 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 TF purposes (e.g. Jahezona campaign explicitly showing that the donations were intended for buying weapons for terrorist groups).





Exchanges

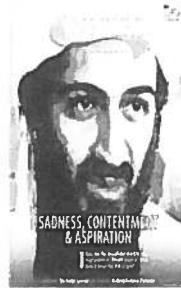


41

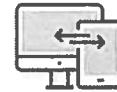


Training

- Instructional material available online includes tools to facilitate counter-intelligence and hacking activities and to improve the security of illicit communications and online activity through the use of available encryption tools and anonymizing techniques.
- The interactive nature of Internet platforms helps build a sense of community among individuals from different geographical locations and backgrounds, encouraging the creation of networks for the exchange of instructional and tactical material.



42



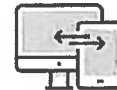
Research findings (2017)

- A third of the sample (32%) prepared for their attacks by using online resources.
- These included
 - bomb-making instruction videos;
 - poison manuals;
 - downloaded copies of *Inspire* magazine;
 - surveillance advice;
 - an assassination guidebook;
 - torture techniques;
 - suicide vest production;
 - body disposal;
 - plans for the London Underground, Buckingham Palace, and other symbolic landmarks;
 - military police voting records;
 - terrorist training manuals.



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

43



Research findings (2017)

TABLE 1

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

Variable	F Value	Sig.	%	Cases
Online Learning (Extreme Right Wing)	5.967	0.015	28.3	1330
Planned Attack	4.120	0.041	60.9	1739
Government Target	4.317	0.038	83.3	4505
LEAD Officers in Syria	7.925	0.005	100.0	—
IED Attack	15.724	0.000	77.5	3154
Armed Assault	5.975	0.015	85.7	5325
Unarmed Assault	4.852	0.029	0.0	—
Acted With a Cell	6.253	0.012	50.5	0.378
Attacked by Police/ Others	7.557	0.006	84.7	3069
International Network Activity	17.487	0.000	79.2	4358
Residential Place Identification	13.747	0.000	73.1	3106

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

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

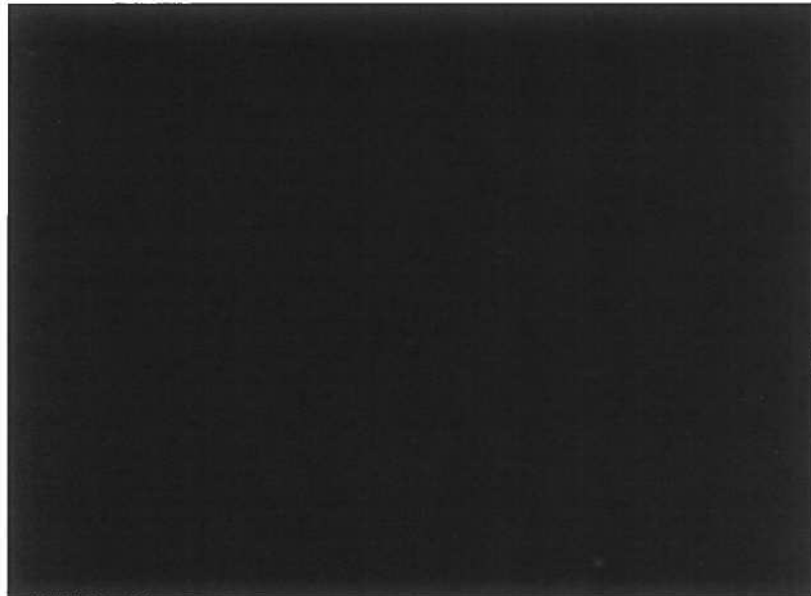
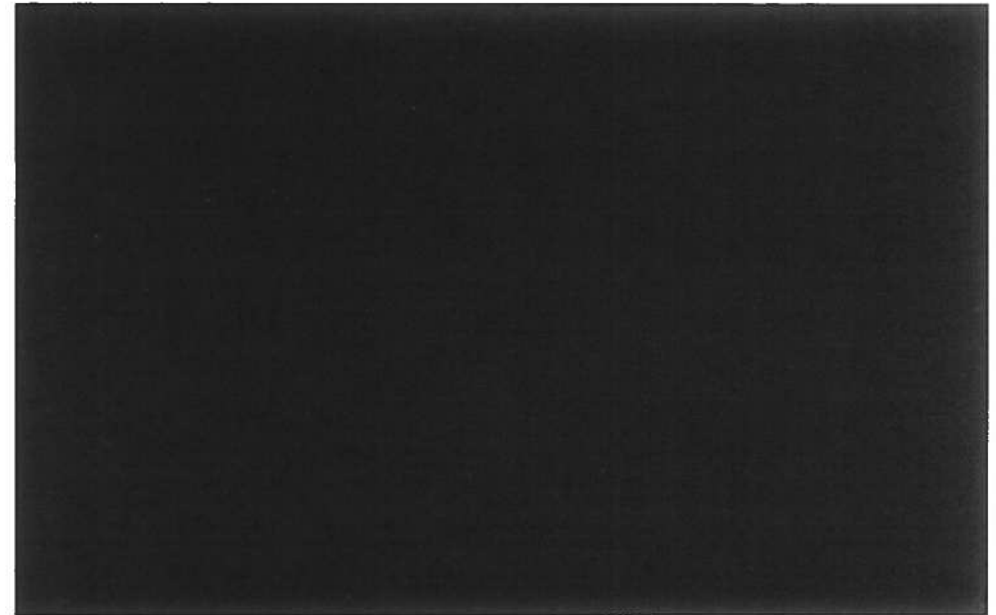


44



Planning

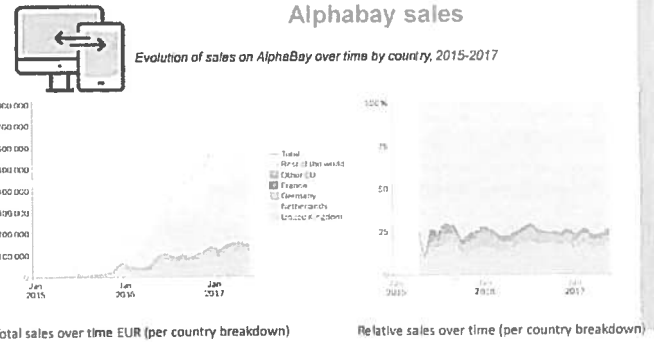
○ A recent case from France, *Public Prosecutor v. Hicheur*, 15 illustrates how different forms of Internet technology may be used to facilitate the preparation of acts of terrorism, including via thorough communications within and between organizations promoting violent extremism, as well as across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



Tor & Marketplaces statistics

Market List With Up & Down

Market	Total listings	Up & Down listings	Market ID	Drug Class	Pharmacop.	Connection	Vendor	Ref. Vendor	Ph. Vendor	Country	Product
1. All Spain Market (EU)	10,124	10,124	101	OTC	OTC	OTC	OTC	OTC	OTC	Spain	OTC
2. All Spain Market (OTC)	10,124	10,124	101	OTC	OTC	OTC	OTC	OTC	OTC	Spain	OTC
3. All Spain Market (Pharm)	10,124	10,124	101	Pharm	Pharm	Pharm	Pharm	Pharm	Pharm	Spain	Pharm
4. All Spain Market (Pharm)	10,124	10,124	101	Pharm	Pharm	Pharm	Pharm	Pharm	Pharm	Spain	Pharm
5. All Spain Market (Pharm)	10,124	10,124	101	Pharm	Pharm	Pharm	Pharm	Pharm	Pharm	Spain	Pharm
6. All Spain Market (Pharm)	10,124	10,124	101	Pharm	Pharm	Pharm	Pharm	Pharm	Pharm	Spain	Pharm
7. All Spain Market (Pharm)	10,124	10,124	101	Pharm	Pharm	Pharm	Pharm	Pharm	Pharm	Spain	Pharm
8. All Spain Market (Pharm)	10,124	10,124	101	Pharm	Pharm	Pharm	Pharm	Pharm	Pharm	Spain	Pharm
9. All Spain Market (Pharm)	10,124	10,124	101	Pharm	Pharm	Pharm	Pharm	Pharm	Pharm	Spain	Pharm
10. All Spain Market (Pharm)	10,124	10,124	101	Pharm	Pharm	Pharm	Pharm	Pharm	Pharm	Spain	Pharm

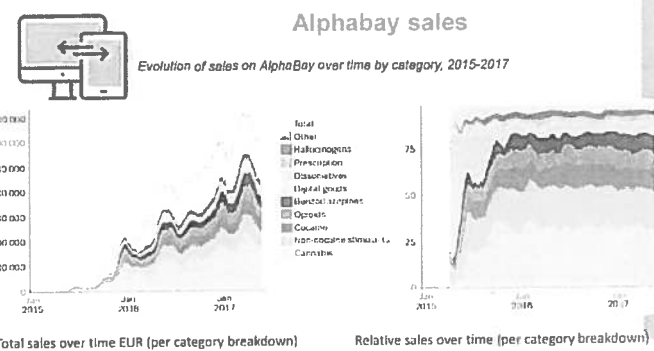


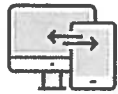
Average prices

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

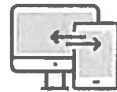
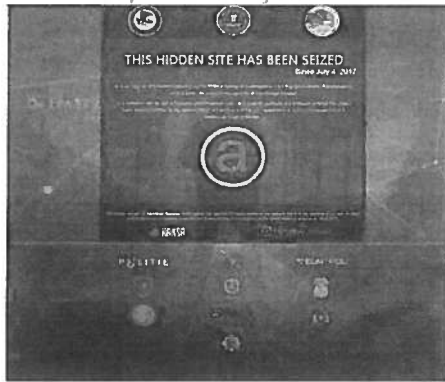
Drug type/ market (country)	YBC-2.0 (Italy)	Flugwamp 2.0 (Sweden)	Depokabanya (10 mg) (Poland)	Salbutamol (Poland)	Other (Poland)
Heroin cannabis	11.7 (+ 2.2)	10.1	20.0	20.0	14.2 (+ 4.7)
Cannabis resin	7.7 (+ 3.3)	8.0	16.0	16.0	11.0 (+ 3.4)
Heroin	NA	10.2	9.5	16.0	16.5 (+ 18.0)
Cocaine	85.8 (+ 9.7)	72.0	140.0	150.0	102.0 (+ 28.0)
Amphetamine	9.3 (+ 5.5)	10.2	40.0	30.0	11.8 (+ 3.0)
MDA	5.2 (+ 0.2)	6.7	16.0	12.0	13.2 (+ 4.0)
LSA	11.0 (+ 4.7)	17.1	NA	16.0	22.4 (+ 4.0)

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





Operation Bayonet

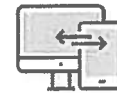


Operation Bayonet

- 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 €4 million in cryptocurrency, €2,2 million in cash, and €35 000 in gold).
- They also conducted 122 interviews.
- By coordinating efforts and acting simultaneously, a strong signal has been sent to those active in selling and buying drugs, counterfeit goods, firearms, etc. on the dark web. This coordinated hit shows that if you are conducting illegal activities on the dark web, you can and will be tracked down by law enforcement.

26 March 2019 **EUROPOL**

<https://www.europol.europa.eu/newsroom/news/global-law-enforcement-action-against-vendors-and-buyers-dark-web>



Feedback

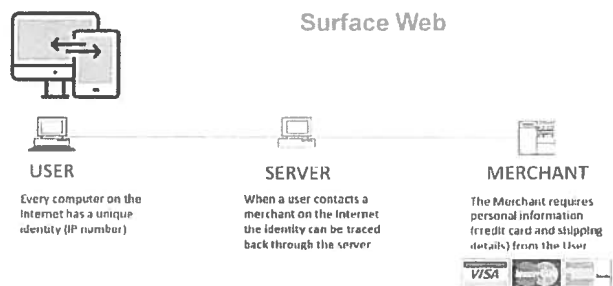
Listing Feedback	Issue	Date	Comments
Q 1	2019-06-20	11:14	Product not search. Last search returned no results. Please help?
Q 2	2019-06-20	11:14	same comment. Product not early enough
Q 3	2019-06-20	11:15	Listing not in list even though I bought it but got stuck in the end
Q 4	2019-06-20	11:17	all my products are with a little party, and some can be from them. Some are in a couple of days
Q 5	2019-06-20	11:17	Q1000
Q 6	2019-06-20	11:18	Product not in list. Please help?
Q 7	2019-06-20	11:18	Product not in list. Please help?
Q 8	2019-06-20	11:18	Product not in list. Please help?
Q 9	2019-06-20	11:18	Product not in list. Please help?
Q 10	2019-06-20	11:18	Product not in list. Please help?
Q 11	2019-06-20	11:18	Product not in list. Please help?
Q 12	2019-06-20	11:18	Product not in list. Please help?
Q 13	2019-06-20	11:18	Product not in list. Please help?
Q 14	2019-06-20	11:18	Product not in list. Please help?
Q 15	2019-06-20	11:18	Product not in list. Please help?
Q 16	2019-06-20	11:18	Product not in list. Please help?
Q 17	2019-06-20	11:18	Product not in list. Please help?
Q 18	2019-06-20	11:18	Product not in list. Please help?
Q 19	2019-06-20	11:18	Product not in list. Please help?
Q 20	2019-06-20	11:18	Product not in list. Please help?
Q 21	2019-06-20	11:18	Product not in list. Please help?
Q 22	2019-06-20	11:18	Product not in list. Please help?
Q 23	2019-06-20	11:18	Product not in list. Please help?
Q 24	2019-06-20	11:18	Product not in list. Please help?
Q 25	2019-06-20	11:18	Product not in list. Please help?
Q 26	2019-06-20	11:18	Product not in list. Please help?
Q 27	2019-06-20	11:18	Product not in list. Please help?
Q 28	2019-06-20	11:18	Product not in list. Please help?
Q 29	2019-06-20	11:18	Product not in list. Please help?
Q 30	2019-06-20	11:18	Product not in list. Please help?



Drug data categories

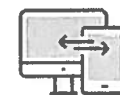
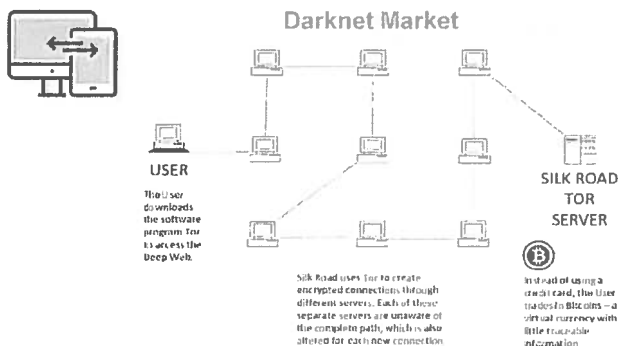
Drug categories of primary interest	Other drugs	Other drugs
<ul style="list-style-type: none"> Heroin, heroin salts Opoids: heroin, opium, analgesics (in g equivalents) Cocaine: all forms of cocaine products Synthetic cannabinoids (with/without phenethylamine) MDMA, MDA Drugs of abuse: ketamine, GHB, GDL Hydrocodone, LSD, PCP (excluding psychotropics) NPS <ul style="list-style-type: none"> Cannabis-based synthetic cannabinoids including skatol 1,2 Opoids: synthetic opioids including fentanyl, M1, 45 Stimulants: amphetamine, 4-fluorophenacetone Dissociatives: MKK, GSKM Hydrocodone 25, NBDOM 4, 4x3, DMF, AC 11 	<ul style="list-style-type: none"> Prescription drugs: benzodiazepines, barbiturates, sedatives and related products Psychotropics: mushrooms and other Serotonergic products 	<ul style="list-style-type: none"> Drug paraphernalia: pipes, pipes, hooks Drug paraphernalia: pipes, pipes, hooks, including forgers, credit cards, numbers, ID cards Electronics: mobile phones and computers Various: various products, including magazines Weapons: all sorts of legal firearms Miscellaneous: miscellaneous items not categorized in any other category





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 46 % 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

- Few 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.



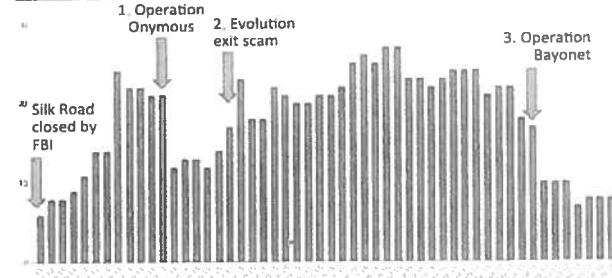


Key findings

- 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.

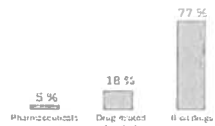


Marketplaces impacting events

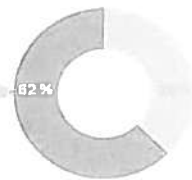


Key findings

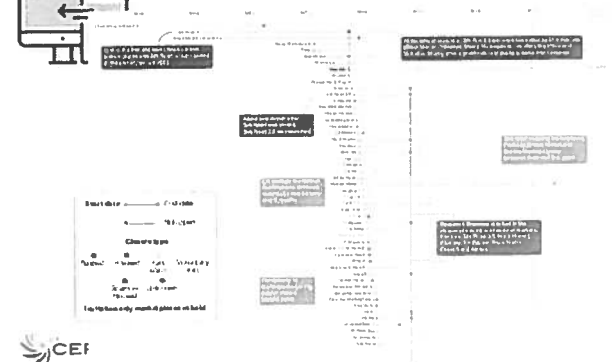
Drugs and drug related chemicals



Source: WebIQ (2017)



Lifetime of marketplaces



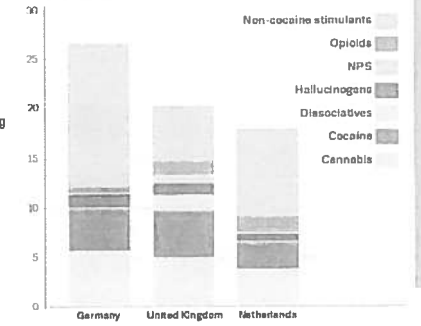


Lifetime of marketplaces



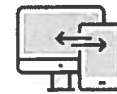
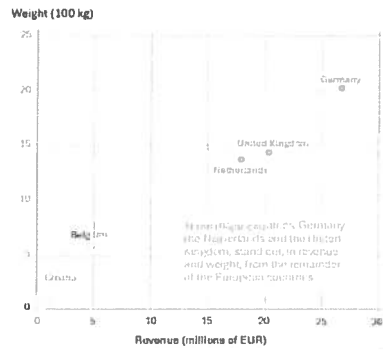
Sales 2011-2015

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



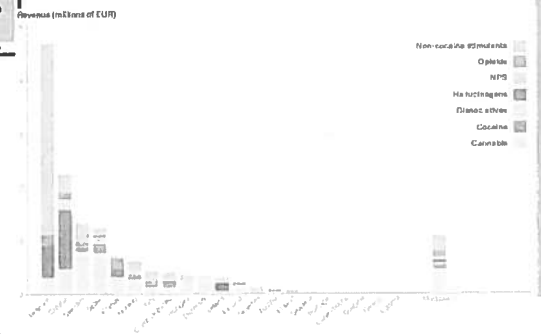
Revenue 2011-2015

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



Revenue 2011-2015

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





Drug sales

EU countries represent roughly 46% of global drug revenue



but only 34% of drug weight



Comparison of drug sales in the EU and the rest of the world, 2011-2015



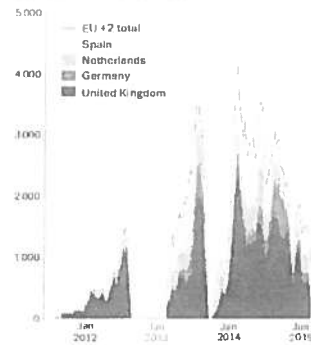
Online and Black Markets

ENL/2015/1280/ACT/ENL/14/04/2015/ENL/14/04/2015/ENL/14/04/2015



Daily NPS sales

Daily volume (EUR, 30 day average)



Breakdown of daily NPS sales originating from the EU, Norway and Turkey



Tor Marketplaces

BLACK MARKETS ONLINE MARKETPLACES

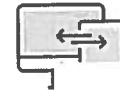


Anonymous networking infrastructure



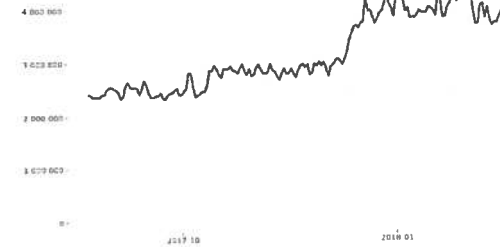
IOCTA 2017

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 toolkits or fake documents, are enablers for further criminality.



Tor USERS

Directly connecting users



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



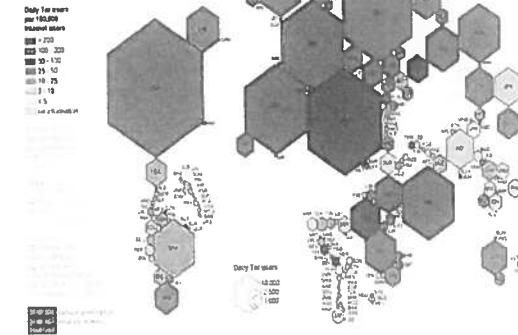
IOCTA 2017

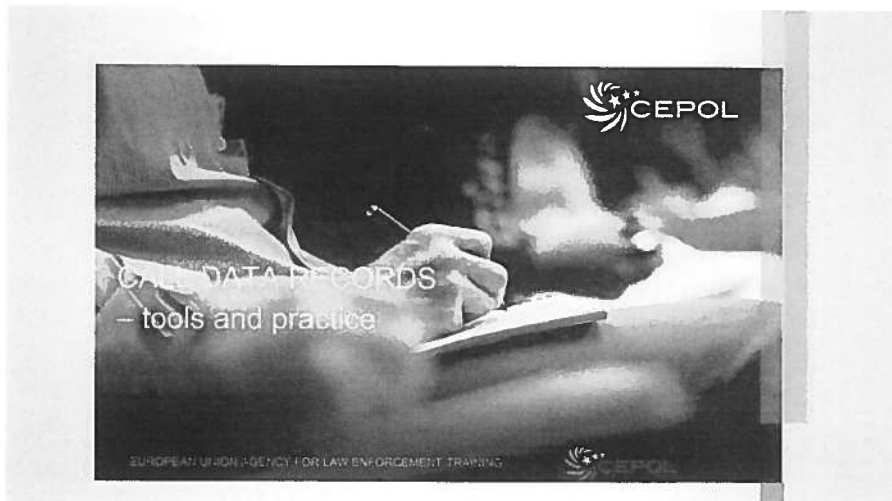
- ❑ Sale of illicit goods to dedicated criminal websites and markets hosted on anonymizing networks such as Tor, I2P and Freenet, although such activity appears to be mainly concentrated on the Tor network
- ❑ As of June 2017, the Tor network had over 2.2 million directly connecting users, and hosted 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

The anonymous Internet





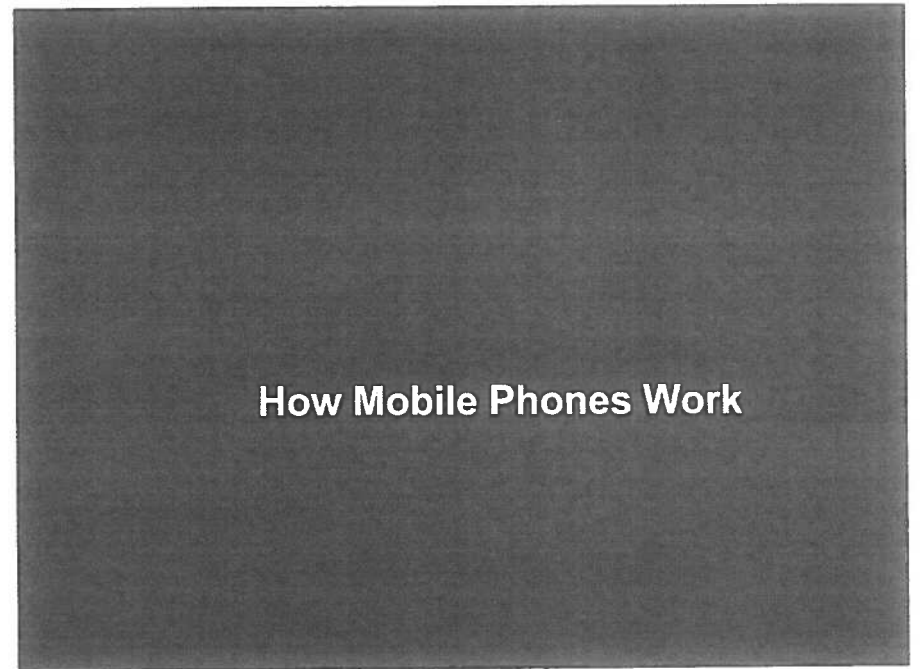
CDR history and versions

- 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!

European Union Agency for Law Enforcement Training
Office: 11100 Budapest, Orlai út 7. Hungary • Correspondence: H-1105 Budapest, Pf. 312 Hungary
Telephone: +36 1 589 9936 • Fax: +36 1 202 4932 • E-mail: info@cepol.europa.eu • www.cepol.europa.eu





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 35 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 1KM
- Pico Cell
 - Provide coverage up 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**

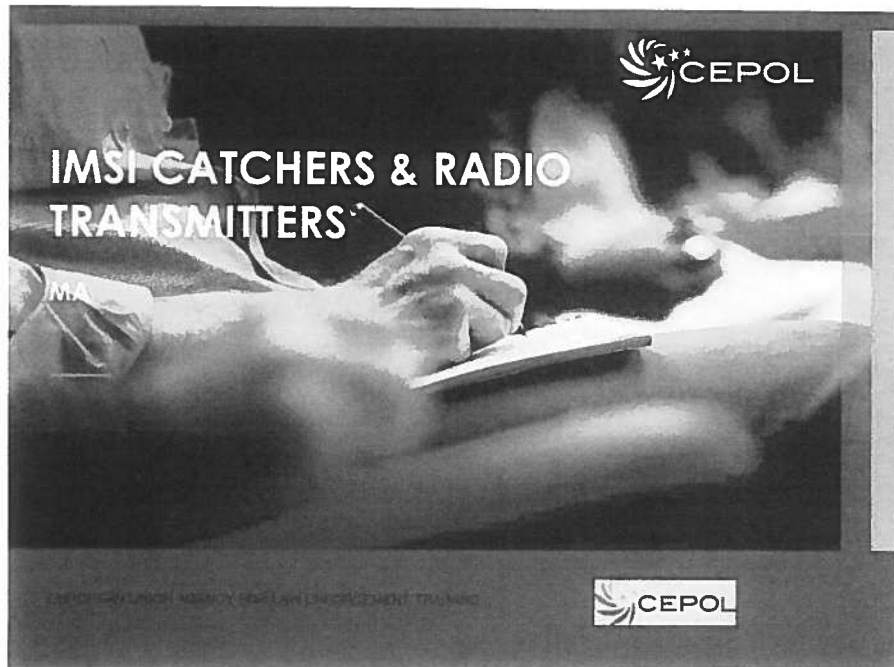
**Evidencing
Communications
Data**

Any Questions?

Thank you for your attention!

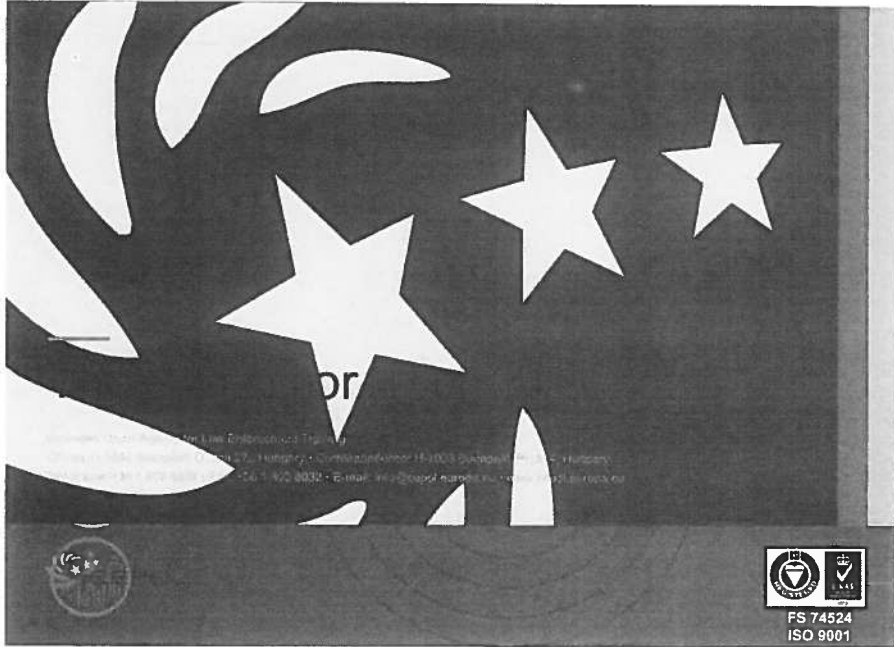
European Commission - The Law Enforcement Training
Department of Justice and Consumer Protection, H-1003 Budapest, 1033/14, Hungary
Tel: +36 1 501 8002 - Email: info@copol.europa.eu | copol@copol.eu





How Mobile Phones Work?

/previous lecture/

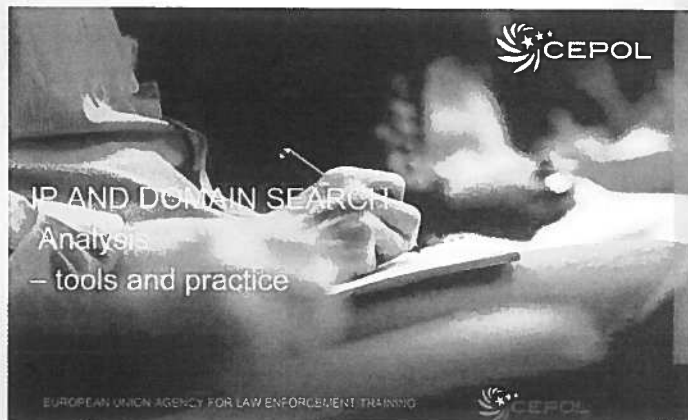


pr

Malaysia's leading provider of the most comprehensive Training
and Development solutions for the public and private sectors.
Tel: +603 8832 8832 • Email: info@topsa.com.my • www.topsa.com.my



FS 74524
ISO 9001



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

An IPv6 address (in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

↓ ↓ ↓ ↓ Zeroes can be omitted
2001:0DB8:AC10:FE01::

0010000000000001 0020110110111000 1010110000010000 11111100000001
0000000000000000 0000000000000000 0000000000000000 0000000000000000

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!

European Union Agency for Law Enforcement Training

Office: H-1094 Budapest, Csilla St., Hungary • Contact: +36 1 801 6000, P.O. Box 314, Hungary

Telephone: +36 1 801 6000 • Fax: +36 1 801 6001 • E-mail: info@cep.eu • www.cep.eu





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!

European Agency for Law Enforcement Training
Ullmasi, H-1135 Budapest, Dóczy 27. Hungary • Csomorhegyi út, H-1023 Eszékút, Pf. 314, Hungary
Telephone: +36 1 952 9030 • Fax: +36 1 952 9322 • E-mail: info@cepil.eu • www.cepil.eu





EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING





SPECIAL TECHNICAL SOLUTIONS FROM
SCIENTIFIC PROJECTS IN THE AREA OF
PREDICTIVE AND DESCRIPTIVE
ANALYTICS

1 800 803 8030 - 1 800 803 8030 - 1 800 803 8030



Thank you for your attention!

European Union Agency for Law Enforcement Training
Orlando, FL 32816, United States of America - Casparystraße 11, 19375 Rostock, DE - 712, Hungary
Telephone: +36 1 803 8030 - Fax: +36 1 803 8030 - E-mail: info@cepol.europa.eu - www.cepol.europa.eu



TEST CDR / IPDR

ALGER, 2019

DISCUSSION

- What are your problems with the investigations?
- Probable solutions?
- Some advice to us?

CYBERCRIMES – LEA PERSPECTIVE



ALGER, 2019

At the very begining...

- 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 (+, -, *, /, $\sqrt{\text{roots}}$).
- 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 Assistance - 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....



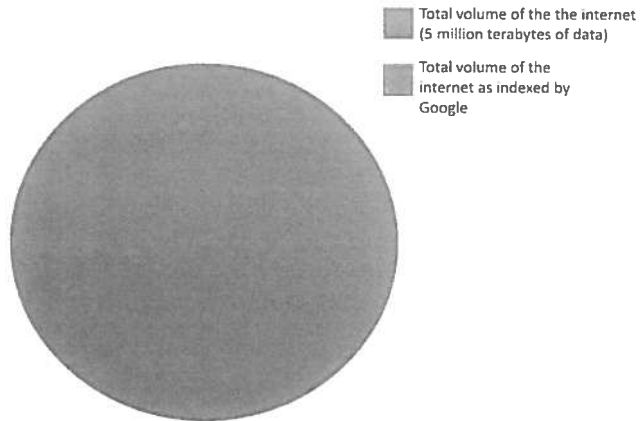
ARPANET 1969

- 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?

■ Total volume of the the internet
(5 million terabytes of data)

■ Total volume as indexed
by Google

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 chalanges...

- BIG amount of data to proces
- 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
- ...(catologue 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...

15

Cybercrimes - definitions

- Cybercrimes (computer crimes):
 - sensu largo,
 - sensu stricte.
- Polish statistics

16

- 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 procesing 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 - on 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 Å§ 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 Penal Code, 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.
- 2002 – Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications – E-PRIVACY) - (SPAM, Cookies).
- 2011 – Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography.
- 2013 / 2016 – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
- 2016 – 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, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
- 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)

National Policy Framework for Cybersecurity of the Republic of Poland for 2017- 2022

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 objectives

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, eg.:

- 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, [redacted] 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 [redacted] 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 troian soft is installed – changing bank accounts numbers (ZEUS and it's combinations)
2. **banking spam** – fake bank offers with a great %%% then troian 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. **haritage spam** – info that you have inharited 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 haritage 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

Server - 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 large number of devices.

Can block the state services – eg. 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 than 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 on line 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

61

Crimes against property

- Can we list them now...?

62

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.

ALWAYS WE USE MONEY TO SENTENCE CYBERCRIMES – TRUE?

65

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.

66

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,
...**

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

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

- **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??

Decipher these location sms-es

- +48602123456 2018-09-20 12:35:35
CS8312 X32231303 Y21004870 @120
R0150 X35231764 Y321005799 R500705
00-000 CITY, Street 1

OUTCOME: ?

- +48602123456 2018-09-20 12:35:35
CS8312 X39381026 Y9185297 @220
R01484 X39377633 Y9180329 R500705
00-000 CITY, Street 2

OUTCOME: ?

- +48602123456 2018-09-20 12:35:35
CS8312 X33897236 Y35496426 @20
R01484 X336695483 Y52819835 R500705
00-000 CITY, Street 3

OUTCOME: ?

Decypher these location from sms-es:

- +48602123456 2018-09-20 12:35:35
C58312 X552231303 Y2109A870 @J20
R01484 X552231764 Y521005799 R500705
00-000 CITY: Street 1

OUTICOMIE: Poland, Warsaw, Culture and Science Palace (Plac
Defilad)

- -48602123456 2018-09-20 12:35:35
C58312 X39381026 Y9185297 @220
R01484 X539377633 Y59180339 R500705
00-000 CITY: Street 2

OUTICOMIE: Dolianowa, Plza del Lan orient, Santegna

- +48602123456 2018-09-20 12:35:35
C58312 X33897236 Y35496426 @220
R01484 X536605483 Y52819835 R500705
00-000 CITY: Street 3

OUTICOMIE: 18063 Zorlida, Algieria, Genlamerie School