Information Gathering via Open Source Intelligence

2023-04-25 00:00 - 2023-04-25 23:59, Sentinel-2 L2A, True color
3 km
Credit: European Union, contains modified Copernicus Sentinel data 2023, processed with EO Browser

Piraeus, Kallithea, Alimos | Sentinel 2 L2A 25/04/2023

Lazarakis Dimitrios, A.M: E18089

Contents

01
Military Intelligence

Definition, Types
The Intelligence Cycle

02
Open Source Intelligence

Data Sources
Standard Operating Procedure
Historic Reference

03
Open Source Investigations

Cyber Security Operations
Monitoring World Events

04
Gathering Intelligence

Red Team Toolset
Social Media

05
Ethics

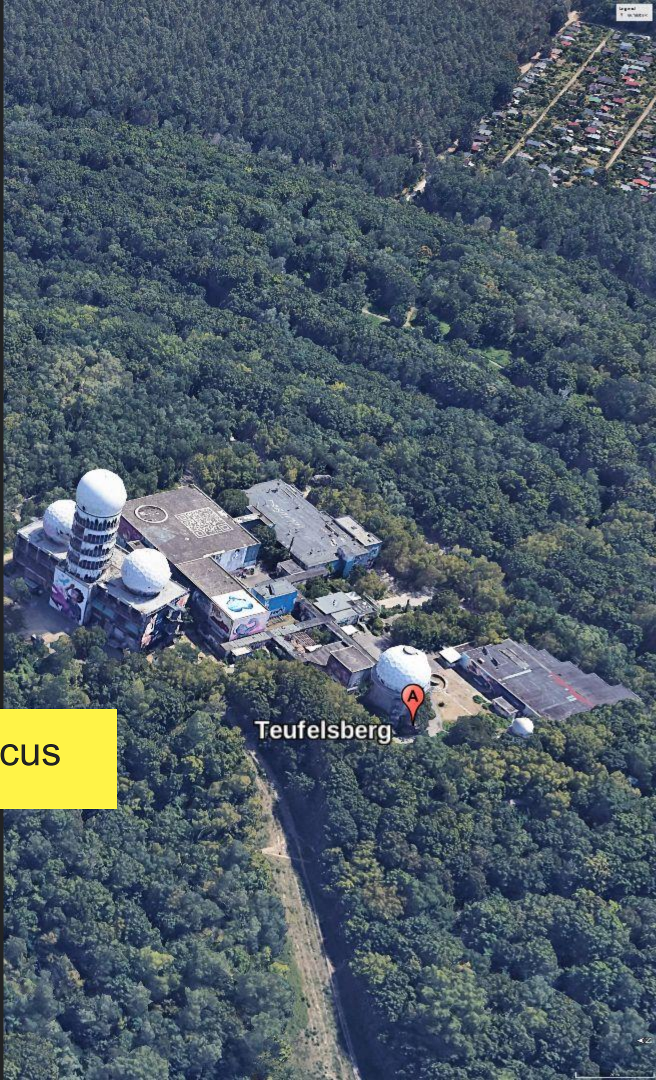
Doxing
Biases
Judgement Criteria

06
Conclusions

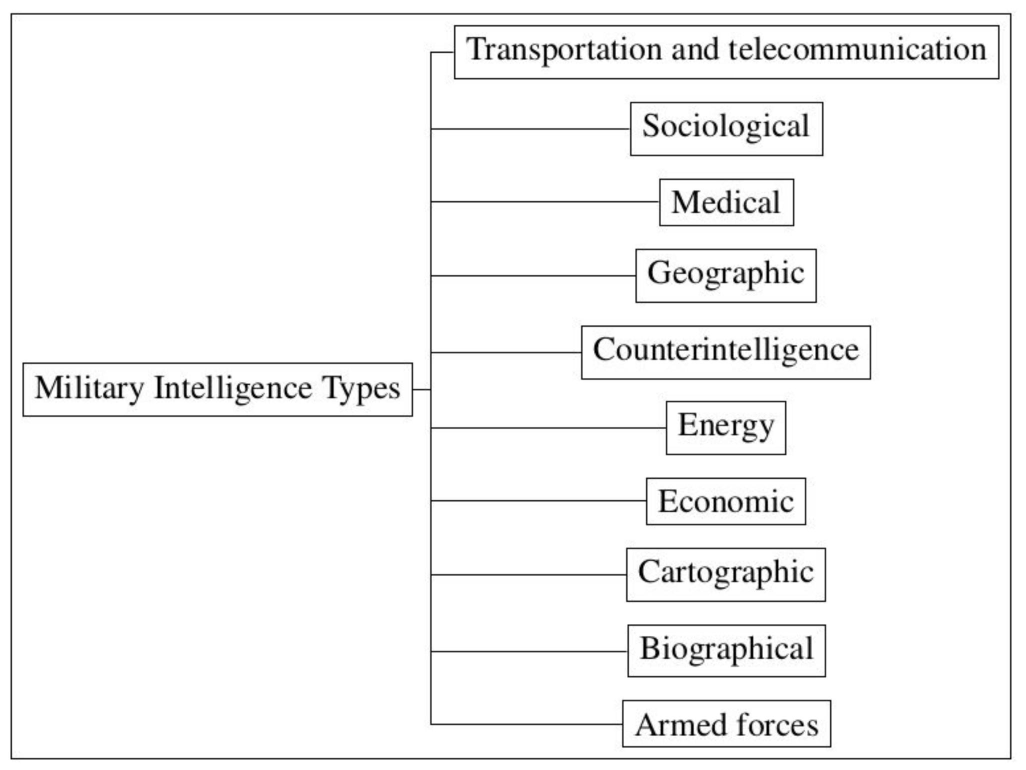
What can be done?

Military Intelligence

Teufelsberg “Spy Tower”, Berlin, Germany | Landsat / Copernicus

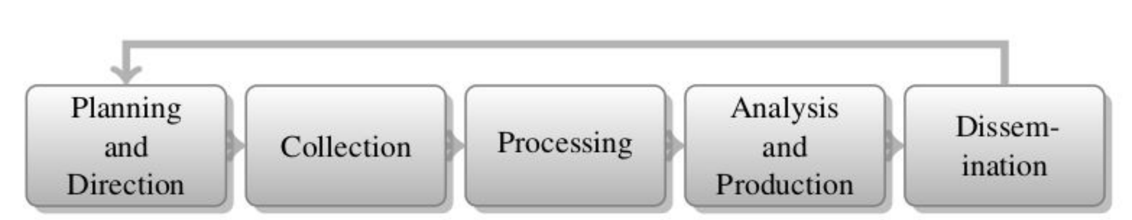


Military Intelligence (by Britannica)



"Intelligence, in military science, information concerning an enemy or an area. The term is also used for an agency that
gathers such information."

The Intelligence Cycle (According to the CIA)



- Planning and Direction
  - Discussion
  - Question Setting
- Collection
  - Gathering Information Overtly
  - Gathering Information Covertly

- Analysis and Production:
  - Evaluation
  - Are the Questions answered?
- Dissemination
  - Presentation to legislators
  - Process restarts if needed

Historic Reference

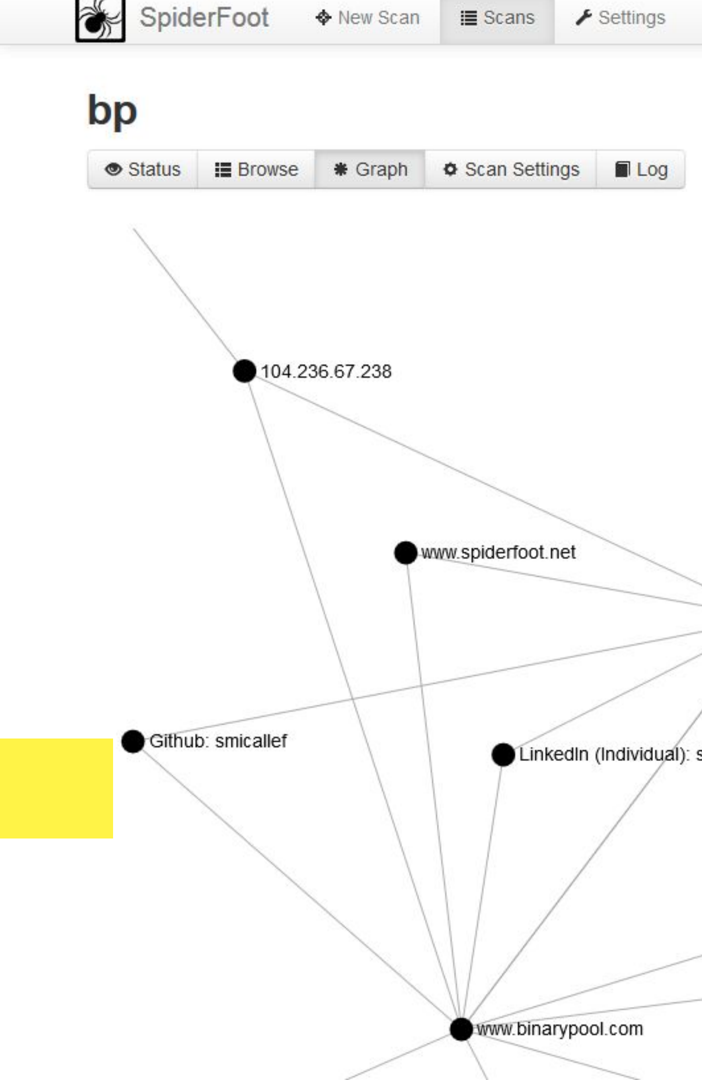
Journal of US. Intelligence Studies, Bellingcat

- Foreign Broadcast Monitoring Service (FBMS) was the result of research of the Princeton University (Established in 1941)
- Pearl Harbor had a profound effect on FBMS, due to the need for military intelligence
- William Donovan, a World War One veteran and International Lawyer laid the founding grounds for the role ‘Coordinator of Information’
    - The Department where Donovan worked in was renamed to Office of Strategic Services
    - Included branch about Open Source Intelligence
    - The branch was positioned in the newly established Central Intelligence Agency (CIA) in 1947
- During WW2, Britain launched BBC Monitoring, later partnering with US intelligence services.
- After World War Two the department saw a decline in agents and went into a deep sleep
- Post 9/11 was renamed to National Intelligence Open Source Center (OSC).
- The Iranian presidential election protests of 2009 highlighted the need for OSINT and the department was put back in operation

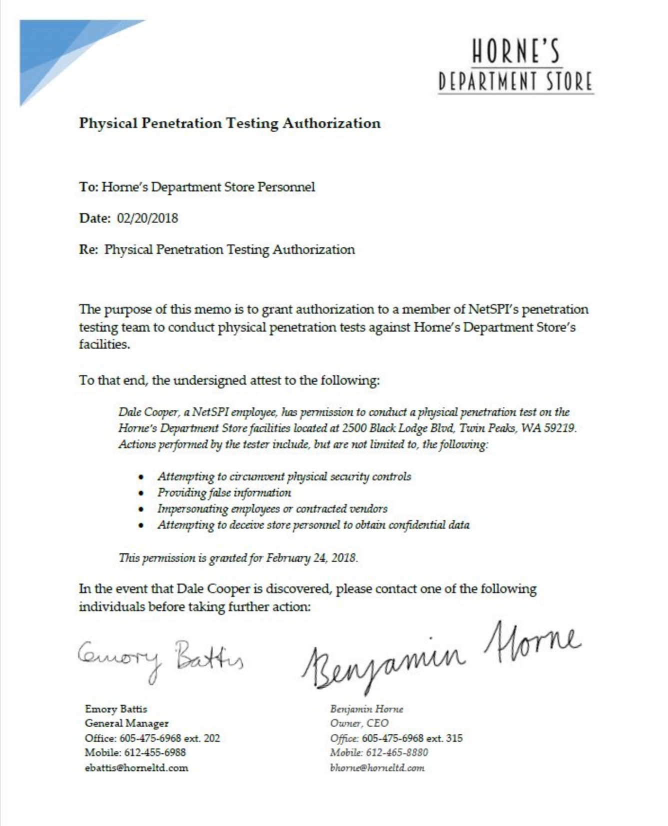
Foreign Broadcast Monitoring Service (FBMS) under FCC | CIA Twitter

Open Source Investigations

Spiderfoot Graph | steemit.com



What is a Red Team?



HORNE'S
DEPARTMENT STORE

Physical Penetration Testing Authorization

To: Horne's Department Store Personnel

Date: 02/20/2018

Re: Physical Penetration Testing Authorization

The purpose of this memo is to grant authorization to a member of NetSPI's penetration testing team to conduct physical penetration tests against Horne's Department Store's facilities.

To that end, the undersigned attest to the following:

> *Dale Cooper, a NetSPI employee, has permission to conduct a physical penetration test on the Horne's Department Store facilities located at 2500 Black Lodge Blvd, Twin Peaks, WA 59219. Actions performed by the tester include, but are not limited to, the following:*
>
> - *Attempting to circumvent physical security controls*
> - *Providing false information*
> - *Impersonating employees or contracted vendors*
> - *Attempting to deceive store personnel to obtain confidential data*
>
> *This permission is granted for February 24, 2018.*

In the event that Dale Cooper is discovered, please contact one of the following individuals before taking further action:

Emory Battis

Emory Battis
General Manager
Office: 605-475-6968 ext. 202
Mobile: 612-455-6988
ebattis@horneltd.com

Benjamin Horne

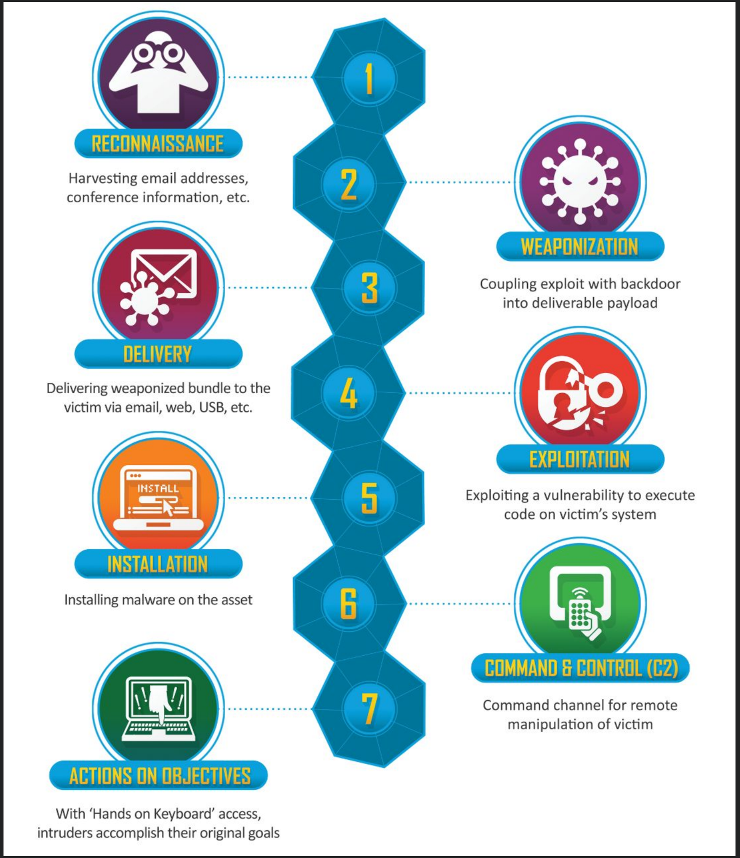
Benjamin Horne
Owner, CEO
Office: 605-475-6968 ext. 315
Mobile: 612-465-8880
bhorne@horneltd.com

Physical Penetration Testing Authorization Sample | NETSPI

The definition of a Red Team according to NIST is:

"*A group of people authorized and organized to <u>emulate a potential adversary's attack or exploitation capabilities</u> against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by <u>demonstrating the impacts</u> of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team.*"

Information Collection in Cyber Security Operations - Red Teams


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
INSTALL
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Cyber Kill Chain® | Lockheed Martin

Reconnaissance techniques according to the MITRE ATT&CK® framework:

- Active Scanning
- Gathering Victim Host Information
- Gathering Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Searching Open Websites/Domains
- Search Victim-Owned Websites

Information Collection in Cyber Security Operations - Blue Teams

- According to Crowdstrike Threat Intelligence is the process of gathering, processing, and analyzing data to comprehend the objectives, targets, and methods of a threat actor
  - Enables proactive protection
  - The techniques of ransomware groups can be predictable
  - Ransomware groups utilize a limited number of TTPs, that may be slightly altered over time
  - Therefore, noticing the attack patterns is vital

- Gathering data about potentials threat from Threat Intelligence platforms. Examples of free and open sources:
  - OTX
  - TALOS
  - VirusTotal
  - Abuse.ch

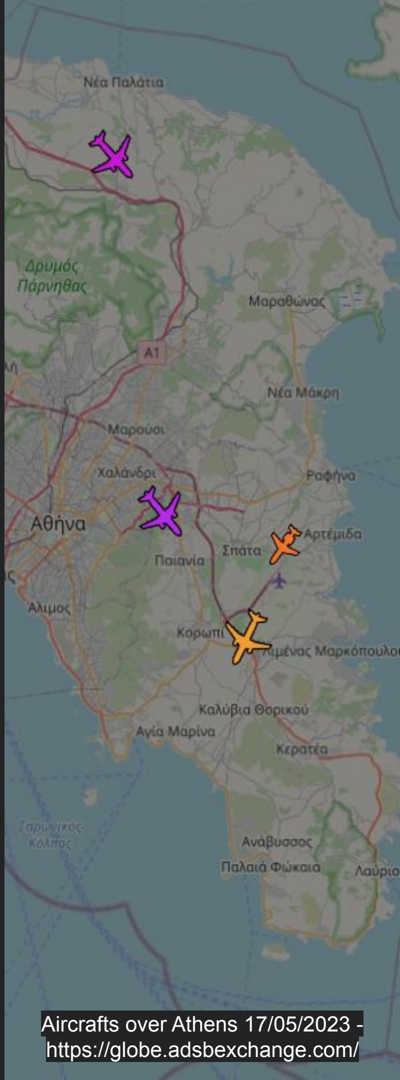
Ivankiv, Ukraine
27/02/2022 - MAXAR
Satellite image

OSINT for Monitoring World Events - Invasion of Ukraine

- Social Media such as Twitter, Instagram, Snapchat and Facebook are used by millions of people every day due to:
  - Improvements of camera technology
  - Improvements of internet connectivity
- During the invasion of Ukraine Twitter and messaging platforms such as Telegram were flooded with photos and videos
- Intelligence services closely monitored known channels
- Open Source Intelligence investigations were brought into mainstream discussion

OSINT for Monitoring World Events - Invasion of Ukraine

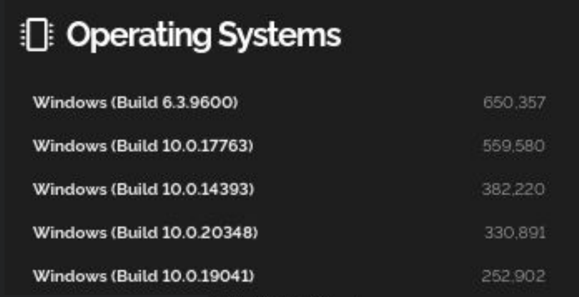
- Journalists use Twitter to effortlessly and quickly post updates and news. The tools they mostly use are:
  - ADS-B
  - Satellite imagery
  - Publicly shared information
  - Private messaging groups
- Cases
  - Document Leak
    - Altered maps publish online
    - Disinformation campaigns
  - Eyes On Russia - Map
    - Document human rights violations, battle misinformation, and prevent abusive behavior



Aircrafts over Athens 17/05/2023 - https://globe.adsbexchange.com/

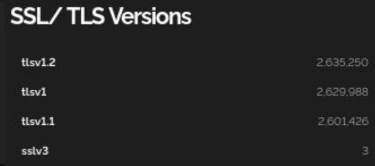
Gathering Intelligence

Port 3389 - Shodan Map | shodan.io



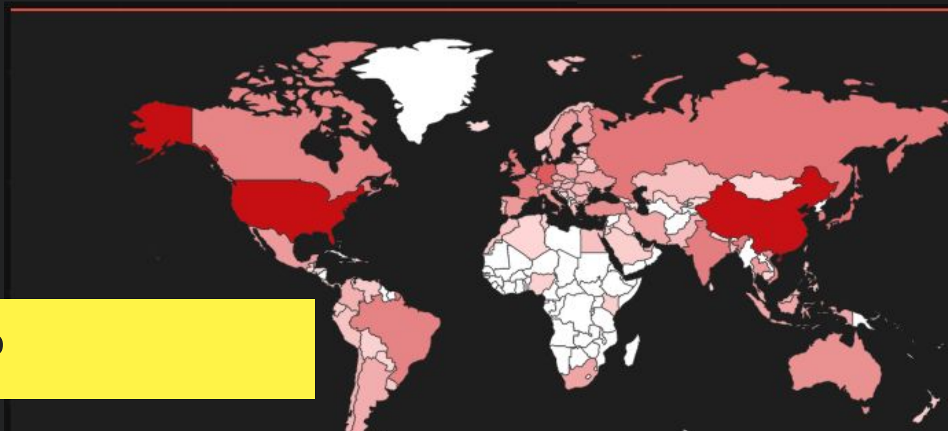
Operating Systems

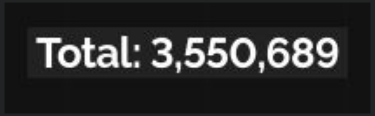
Windows (Build 6.3.9600)	650,357
Windows (Build 10.0.17763)	559,580
Windows (Build 10.0.14393)	382,220
Windows (Build 10.0.20348)	330,891
Windows (Build 10.0.19041)	252,902



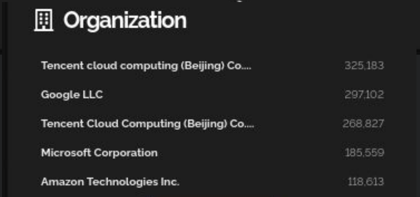
SSL/ TLS Versions

tlsv1.2	2,635,250
tlsv1	2,629,988
tlsv1.1	2,601,426
sslv3	3





Total: 3,550,689



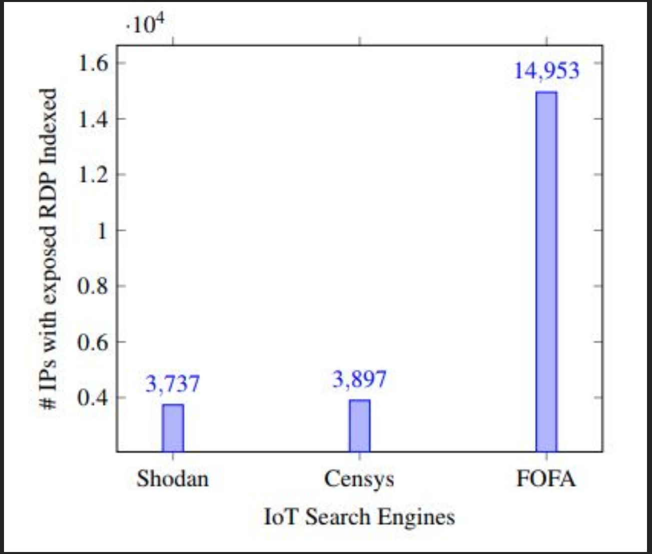
Organization

Tencent cloud computing (Beijing) Co....	325,183
Google LLC	297,102
Tencent Cloud Computing (Beijing) Co....	268,827
Microsoft Corporation	185,559
Amazon Technologies Inc.	118,613

Useful Toolset

Western Europe, 17/05/2023 20:30 | Snapchat Maps

- Red Team tools that automate repeated processes and tasks of the enumeration/reconnaissance phase:
  - Amass
  - Gitleaks
  - Spiderfoot
  - Linkedint
- Internet Search Engines
  - Shodan
  - Censys
  - FOFA
  - LeakIX
- Social Media
  - Snapchat (Maps)
  - Instagram (Patterns, social relationships)
  - Twitter (Following, using alerts, Analytics)



Ethics

Personal Data | Generated by Stable Diffusion 2

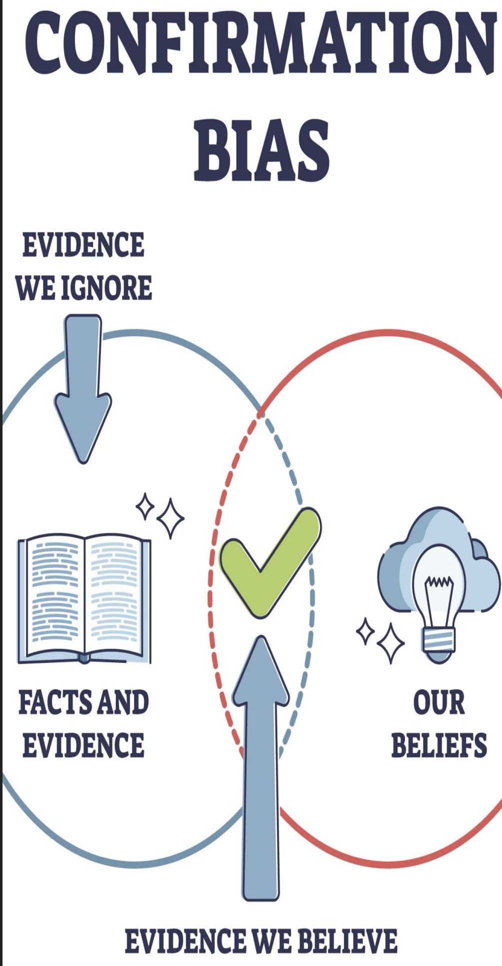
Prompt: “Illustration of the personal data of someone, investigation, osint, transparency, big data, fantasy, intricate, elegant, highly detailed, digital painting, artstation, concept art, matte, sharp focus”

Doxing and Swatting

- Doxing
  - Personal information disclosure publicly
  - Vigilante “justice”
  - doxing can have detrimental effects on a person
- Swatting
  - ”Swatting” is derived from the United States’ Special Weapons and Tactics (SWAT) team
  - Incidents
    - a home address was shared to a Discord channel and someone from that channel ”swatted” the address, resulting in the victim having a heart attack
    - a 20 year old man being shot on sight after a hostage 911 call

Biases

- Data found can be inaccurate for the following reasons:
    - To promote certain beliefs
    - To spread fake news
    - Human error
- 3rd party biases cause:
    - Incompleteness
    - Inaccuracy
- Personal bias can affect the accuracy of an investigation
- Combatting Biases?
    - 3rd party biases
        - Cross referencing sources
        - Find information that backs the original data
    - Own biases
        - Being aware of own biases
        - Make an effort to convey information in an unbiased and objective fashion



Confirmation Bias | Simply Psychology

Transparency in investigations | Generated by DALLE Mini

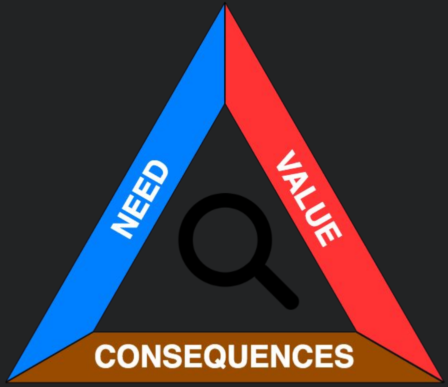
Transparency

- Transparency is critical:
  - Reliability
  - Credibility
  - Nests accuracy and trustworthiness
  - The investigation can be verified by a 3rd party
- The researchers should be open and honest about
  - What Information is gathered
  - Their goal
  - If and what unnecessary information was processed
  - Their sources
  - Their methods

Prompt (GPT-2): “Illustration of someone doing an investigation and being transparent about the results and methods. This is for a presentation about open source intelligence, osint. big data are utilized and privacy could be breached”

Judgement Criteria

- What is morally correct to use as a source?
  - Leaked documents are considered part of Open Source Intelligence
    - They may contain sensitive information such as:
      - Patient information
      - Passwords
      - Company financial data
  - Social media expose great amounts of information online about a person:
    - General behavior
    - Preferences
    - Interests
    - Relationships
    - Political beliefs
- Ethical guidelines must be followed
  - **NEED**
  - **VALUE**
  - **CONSEQUENCES**



Judgement Criteria | OSINT Essentials - Medium.com

Personal Data on the Cloud | Generated by Stable Diffusion 1.5

Conclusion

- More Data will increasingly be uploaded
- Social Networking will probably closely follow and integrate the newly introduced VR and AR technologies
- Digitization of governmental documents and services
- The problem:
  - a new stream of personal data will undoubtedly be uploaded
  - Advertising based on data provided
  - The cyber attack surface of legislative organizations will increase
- What can be done?
  - Need for ethical guidelines
    - personal privacy of people not involved in an investigation should not be compromised
    - certain people should only be targeted when an issue of public importance is raised
  - Privacy campaigns should be launched
  - Practise privacy and have a proper cyber security posture

Thank you for your time!

Sources are available in the thesis
Images from various sources
Presentation template by Slidesgo

Information Gathering via Open Source Intelligence
Lazarakis Dimitrios