

Data privacy:

R3V3RS3D

By

Jindrich Karasek
aka **4n6strider**

for UK
Rapid7 & PSU CAS

RAPID7



~% whoami

- Lead Security Researcher
- Serial hiker & forrest addict
- **Mind** hacker & AI cheater



#1 How do we generate the data in digital domain

#2 How are the data collected

#3 How are the data marketed -> Grey marketing, PR and politics

#4 Cognitive warfare

#5 NLP - Detection and analysis

#6 OSINT

Sharing is caring



#1 How we generate the data in digital domain

github.com/Lissy93/personal-security-checklist /
<https://digital-defense.io/>





Adversarial makeup & clothing

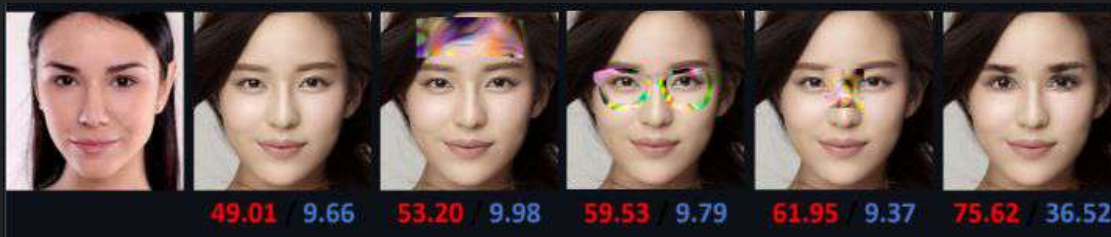
See also:

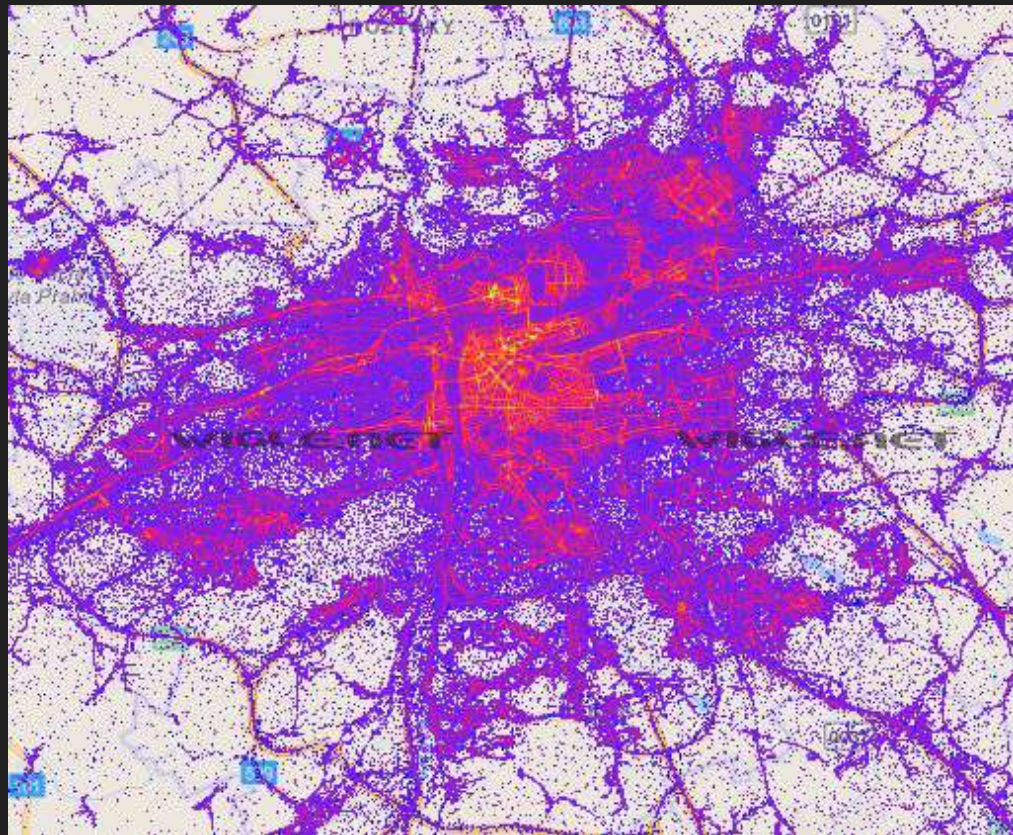
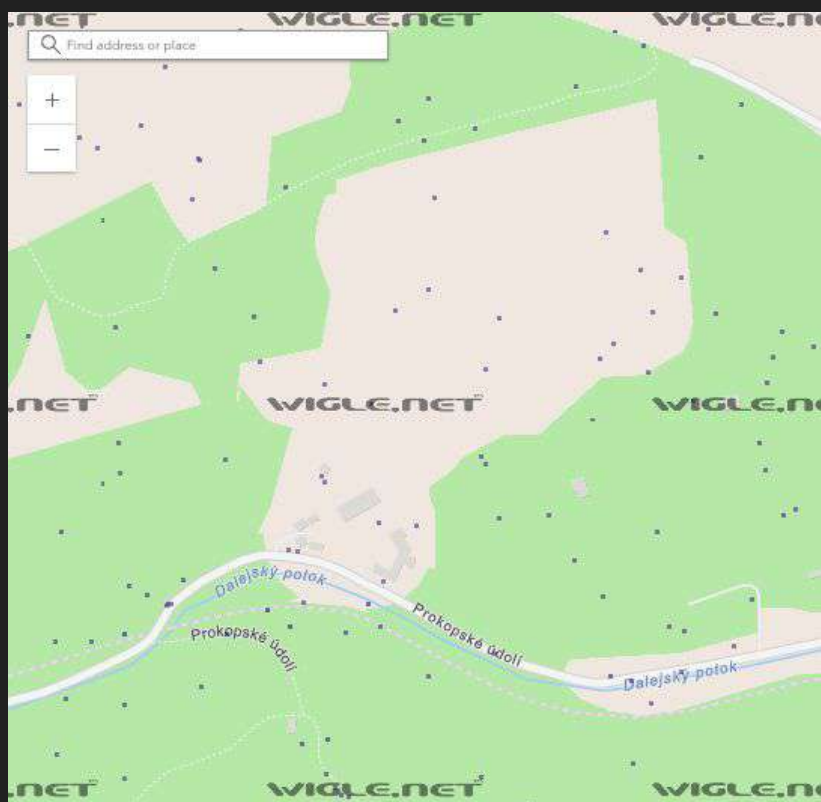
<https://github.com/TencentYoutuResearch/Adv-Makeup>

https://github.com/Eolas-bith/adversarial_patterns_generation/

<https://arxiv.org/abs/2109.03329>

<https://ieeexplore.ieee.org/document/8803269>





<https://wigle.net/>

What is Bluetooth® Beacon?



<https://www.minew.com/bluetooth-beacon/>



JOIN GROUP : <https://t.me/crewcomboteams>
JOIN GROUP : @crewcomboteams

[CrewComboTeams]

skulgar2@tiscali.cz:hydraulik
kicherer@email.cz:sagar12
stehlikjiri@tiscali.cz:dagdag
gate2me@tiscali.cz:Keli2kelI
javorbuk@seznam.cz:necumpico
marksniper@seznam.cz:casper134
stefka.daniel@tiscali.cz:StEfka
mirek.chocho@tiscali.cz:mchocho19
velamen@seznam.cz:uvidime103
vajinko@tiscali.cz:281206nl
lesany@tiscali.cz:bobina
xkupecx@seznam.cz:Hrabak1982
galdal@centrum.cz:reymysterio
p.madarova@worldonline.cz:certik
hornicek@chrudim.cz:Midget35
sisipech@email.cz:mazlinka

cas.cz

lukas.strasil@bcas.cz:Hurikan87
matlocha@ujf.cas.cz:modular
peterka@biomed.cas.cz:444444
radka.schneiderova@bcas.cz:Netopzr83

gmail








trdlo.t@gmail.cz:maminka445
iva.brandstetrova@gmail.cz:aftina46
nickygirl54@gmail.cz:70cflf7e
stenanxmas7@gmail.cz:stunakxmas7

seznam.cz

javorbuk@seznam.cz:necumpico
marksniper@seznam.cz:casper134
velamen@seznam.cz:uvidime103

Google

```
"endLocation" : {  
  "latitudeE7" : 500898931,  
  "longitudeE7" : 144598860  
},  
"duration" : {  
  "startTimestampMs" : "1580515888452",  
  "endTimestampMs" : "1580516682468"  
},  
"distance" : 2843,  
"activityType" : "IN_TRAM",  
"confidence" : "MEDIUM",  
"activities" : [ {  
  "activityType" : "IN_TRAM",  
  "probability" : 75.01339316368103  
}, {  
  "activityType" : "WALKING",  
  "probability" : 11.47935539484024  
}, {  
  "activityType" : "IN_PASSENGER_VEHICLE",  
  "probability" : 6.250264495611191  
} ],  
"transitPath" : {  
  "transitStops" : [ {  
    "latitudeE7" : 500793600,  
    "longitudeE7" : 144195000,  
    "placeId" : "ChIJveD7JPKUC0cRZcD30wrI4Cc",  
    "name" : "Lazarská"  
  } ],  
}
```

Name
 2021-02-08T08_34_00+01_00_PT0S_tcx
 2020-11-15T07_51_00+01_00_PT42M_Walking.tcx
 2020-12-27T10_49_00+01_00_PT8M_Walking.tcx
 2020-12-30T20_12_00+01_00_PT4M_Walking.tcx
 2019-10-31T13_50_00+01_00_PT4M_Walking.tcx
 2019-11-05T08_16_00+01_00_PT5M_Running.tcx
 2019-12-05T10_25_00+01_00_PT4M_Walking.tcx

Search

Visited <https://city-dog.cz/post/panska-eiketa-v-odivani/>

Mar 5, 2020, 12:33:08 PM CET

Products:
Search

Search

Searched for [vesta misto kravaty](#)

Mar 5, 2020, 12:33:01 PM CET

Products:
Search
Locations:
At [this general area](#) - From your device

```
<Activities>  
  <Activity Sport="Walking">  
    <Id>2020-11-15T06:51:00.000Z</Id>  
    <Lap StartTime="2020-11-15T06:51:00.000Z">  
      <Track>  
        <Trackpoint>  
          <DistanceMeters>0.0</DistanceMeters>  
          <Time>2020-11-15T06:51:00.000Z</Time>  
        </Trackpoint>  
        <Trackpoint>  
          <DistanceMeters>0.0</DistanceMeters>  
          <Time>2020-11-15T07:33:00.000Z</Time>  
        </Trackpoint>  
      </Track>  
      <DistanceMeters>0.0</DistanceMeters>  
      <TotalTimeSeconds>2520.0</TotalTimeSeconds>  
      <Calories>1.0</Calories>  
      <Intensity>Active</Intensity>  
      <TriggerMethod>Manual</TriggerMethod>  
    </Lap>  
  </Activity>
```

Google Photos

Used [Google Photos](#)

Feb 7, 2020, 8:07:33 PM CET

Products:
Android

Facebook

Used [Facebook](#)

Feb 7, 2020, 7:32:37 PM CET

Products:
Android

Spotify: Listen to podcasts & find music you love

Used [Spotify: Listen to podcasts & find music you love](#)

Feb 7, 2020, 7:11:00 PM CET

Products:
Android

Maps

[Viewed area around Czechia](#)

Mar 9, 2020, 1:21:32 PM CET

Products:
Maps

Maps

[Viewed area around Dubá](#)

Mar 9, 2020, 1:21:29 PM CET

Products:
Maps

Facebook



Messenger

Tajné konverzace

Zda jste využil tajné konverzace na Facebooku a případně seznam, kdy jste je využil.

Byly odeslány tajné zprávy?	Ano
Přišly tajné zprávy?	Ano

Seznam, kdy jste využil tajné konverzace v Messengeru

OnePlus 7

4. 1. 2021 13:16

Name

your_off-facebook_activity
ads_interests.html
advertisers_who_uploaded_a_contact_list_with_your_information.html
advertisers_you've_interacted_with.html
your_off-facebook_activity.html



Skupiny

Počet vašich interakcí se skupinami na Facebooku

Naděnci horské turistiky
469krát

Láska k šutrům
465krát

Geo Klub CZ/SK
290krát

Letenská parta
261krát

Cybor Security
257krát

Jindrich Karasek okomentoval(a) příspěvek uživatele Nadia Nolet.

because I can't speak or write french... So in english;-)
Thank you a lot:-P Lets make a toast to our good health and so on:-)

14. 12. 2009 10:54

Jindrich Karasek okomentoval(a) příspěvek uživatele Romina Ines Tyler.

Yea, I had:-) Sorry for my delay, I am not good oriented here in facebook. Greetings from the North, how are up to these days anyway?

19. 8. 2009 23:04

Jindrich Karasek okomentoval(a) příspěvek uživatele Neklan Kardza.

Ahoj,promin ja jsem v tom skotsku. A ikdyz se desateho vracim,asi se na chatu nedostanu-ikdyz bych rad aspon na chvilku treba na kole,ale fakt nevím,musím merit diplomku,po navratu.. Nemam tu moc pristup na web,pisu z mobilu. Jakteze mas volnej? Ja myslel ze jsi prave rikal ze toho mas hodne..

26. 7. 2009 23:03



Poslední poloha

Vaše nejaktuálnější poloha zaznamenaná vaším zařízením

(50.080946, 14.4597249)

13. 1. 2021 13:23

Name	Size
device_location.html	22.0 KiB
last_location.html	21.9 KiB
primary_location.html	22.7 KiB
primary_public_location.html	22.2 KiB
timezone.html	21.9 KiB

Facebook - pokr.

Typ zařízení	GM1903
ID zařízení	28176b84-5f8e-43ac-b3e9-b192faf2e1a3
ID reklamy	63c63b66-68b1-4f68-a399-0ec2159440f0

Použité IP adresy

86.49.119.204

Login

17. 9. 2020 16:21

62.245.75.120

Login

20. 9. 2020 20:55

37.188.177.124

Login

20. 9. 2020 20:41

37.188.147.121

Password Change












18. 9. 2020 20:20

37.188.151.192





Login

17. 9. 2020 16:31













Name

-  contact_verifications.html
-  authorized_logins.html
-  mobile_devices.html
-  used_ip_addresses.html
-  your_facebook_activity.html
-  where_you're_logged_in.html
-  logins_and_logouts.html
-  administrative_records.html
-  datr_cookie_info.html
-  login_protection_data.html
-  account_activity.html

Name

-  followed_pages.html
-  followers.html
-  following.html
-  unfollowed_pages.html

Name

-  anger.png
-  confused.png
-  dorothy.png
-  flame.png
-  haha.png
-  like.png
-  love.png
-  plane.png
-  selfie.png
-  sorry.png
-  toto.png
-  wow.png
-  yay.png

Support Correspondences

Interactions you've had with Facebook support

Funkci vytváření akcí protokolu Open Graph už jsme vám odblokovali.

Facebook

Dočasně jsme vám do 23. listopadu 2016 v 22:58 zablokovali vytváření akcí protokolu Open Graph.

22. 11. 2016 22:58




Facebook

Omezení bylo zrušeno.

Funkci vytváření akcí protokolu Open Graph už jsme vám odblokovali.

23. 11. 2016 22:58

Name

-  friends.html
-  received_friend_requests.html
-  rejected_friend_requests.html
-  removed_friends.html
-  sent_friend_requests.html



SNA - social network analysis

Complex systems analysis

Precise model of a social group
Backbone for behavioral analytics.

(Data source: My FB friend list
from the times when I had only
200 people in there)

<170 = Either fake or not so
social

Around 200 = usual number of
contacts

>200 = Something is going on

#2 How are the data collected &&

#3 How are the data marketed

Data Brokers

What They Collect

They gather an enormous range of data points, including:

- Basic identifiers: name, age, address history, phone numbers, email addresses
- Demographic details: gender, race/ethnicity estimates, income estimates, education level, marital status, children (ages/genders), political affiliation, religion estimates
- Financial data: credit headers (name + address + partial SSN from credit bureaus), purchase history, net worth estimates, “propensity to buy” scores
- Online/offline behavior: websites visited, apps used, search history, location history, vehicle owned, travel patterns, social media profiles and posts
- Health & lifestyle: inferred medical conditions (e.g., “diabetic buyer,” “cholesterol focus”), gym membership, dietary preferences, hobbies
- “Sensitive” categories: pregnancy status, sexual orientation estimates, ethnic affinity, political leanings



Major Data Brokers (2025)

Some of the biggest players still operating:

- Acxiom (now part of IPG, rebranded as “Acxiom LLC”)
- Oracle Data Cloud (absorbed BlueKai, Datalogix, AddThis)
- Experian Marketing Services
- Equifax (sells marketing data separately from credit reports)
- TransUnion (TLOxp, marketing lists)
- Epsilon (Publicis Groupe)
- Nielsen
- CoreLogic (real-estate-focused)
- LexisNexis Risk Solutions (owns Accurint, Seisint/Matrix)
- Thomson Reuters (owns CLEAR)
- LiveRamp (formerly Acxiom’s IdentityLink)
- Neustar (now part of TransUnion)
- Smaller/specialized brokers: BeenVerified, Spokeo, Intelius, PeopleFinders, TruthFinder, IDI (now part of Fluent), TowerData, FullContact, Pipl (now part of Near), etc.

How They Get the Data

Sources include:

1. Public records (property deeds, voter registration, court filings, DMV in some states)
2. Credit header data from the big three credit bureaus (legal loophole in FCRA)
3. Commercial sources (loyalty cards, warranty cards, surveys, magazine subscriptions, product registrations)
4. Online tracking (cookies, device fingerprinting, SDKs in apps, bidstream data from ad exchanges)
5. Data-sharing partnerships (retailers, banks, telcos, publishers)
6. Buying from other brokers (they trade datasets like baseball cards)

Who Buys It

- Marketers (targeted advertising)
- Advertisers & ad-tech companies (programmatic bidding)
- Employers (background checks)
- Insurance companies (risk scoring)
- Financial institutions (fraud detection, credit offers)
- Real-estate agents, landlords
- Law enforcement & government agencies (via specialized brokers like Thomson Reuters CLEAR or LexisNexis Accurint)
- People-search sites (whitepages, fastpeoplesearch, truepeoplesearch)
- **Political campaigns**
 - Stalkers, scammers, private investigators (big abuse vector)

Regulation (as of late 2025)

- United States: Patchwork. Vermont, California, and a few other states have data-broker registration laws. CCPA/CPRA lets Californians opt out of sale, but enforcement is spotty. DeleteMe/Optery-style removal services handle hundreds of opt-outs per client. No comprehensive federal law yet (ADPPA died again in 2024).
- EU/UK: GDPR severely restricted many brokers; most large ones either exited the European market or run heavily restricted “consent-based” models.
- Canada: PIPEDA + new Quebec law similar to GDPR.

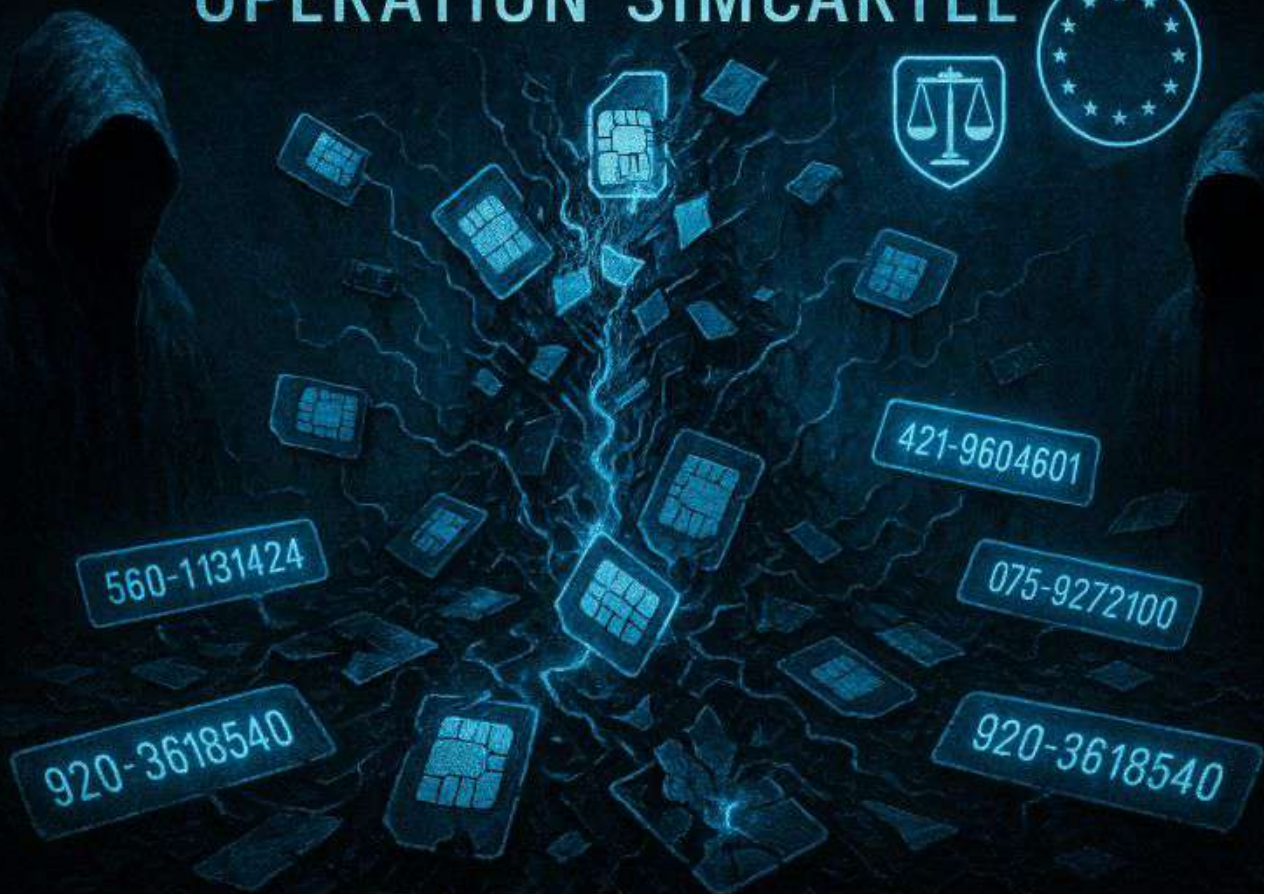
Current Trends (2025)

- Shift from cookies to probabilistic device graphs and hashed emails (post-cookie world)
- Rise of “identity resolution” companies stitching everything together
- Growing sale of location data (even after 2022 scandals)
- Political data brokers (e.g., i360, Catalist, L2) still extremely active
- Some brokers now offer “privacy-safe” clean rooms or synthetic data to get around regulation

In short, data brokers are one of the largest, least transparent parts of the surveillance economy. Most people have detailed dossiers held by dozens of companies they've never heard of, and full removal is extremely difficult even if you're willing to spend years on it

#4 Cognitive warfare

OPERATION SIMCARTEL



40.000 SIM-Karten konfisziert: Europol sprengt Betrügering

Strafermittler von Europol haben die IT-Infrastruktur von Cyberkriminellen lahmgelegt, die in der EU für Millionenschäden gesorgt haben.



<https://www.heise.de/news/40-000-SIM-Karten-konfisziert-Europol-sprengt-SIM-CARTEL-Betruegerring-10784925.html>

<https://de.euronews.com/2025/10/18/europol-lettland-polizei-cybercrime>

Europol: Lettische Polizei zerschlägt Cybercrime-Ring



Copyright EBU

An action day performed in Latvia on 10 October 2025 led to the arrest of five cybercriminals of Latvian nationality and the seizure of infrastructure used to enable crimes against thousands of victims across Europe. During the operation codenamed 'SIMCARTEL', law enforcement arrested two further suspects, took down five servers and seized 1 200 SIM box devices alongside 40 000 active SIM cards. Investigators from Austria, Estonia and Latvia, together with their colleagues at Europol und Eurojust, were able to attribute to the criminal network more than 1 700 individual cyber fraud cases in Austria and 1 500 in Latvia, with a total loss of several million euros. The financial loss in Austria alone amounts to around EUR 4.5 million, as well as EUR 420 000 in Latvia.

<https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested>



How Psy-Op Scammers Mass-Produce Fake Identities

- **Industrial fake-account factories:** A Latvian-run CaaS network operated 1,200+ SIM boxes and tens of thousands of SIM cards to create **~49 million online identities**.
- **Bypassing platform security:** Renting temporary numbers from **80+ countries** let criminals intercept SMS codes and **defeat SMS-based 2FA**, so platforms “trusted” the accounts.
- **Fuel for influence & fraud:** These anonymized accounts were then used to **bootstrap scams, phishing, investment fraud, pig-butcher, extortion and migrant-smuggling comms**.
- **Psychological angle:** With millions of “real-looking” accounts, actors can **amplify narratives, swarm targets, validate fake personas and run coordinated persuasion** without being tied to a real person.
- **Key takeaway: Account creation is the weakest link** — once identity checks are broken, psy-ops at scale become cheap, deniable, and global.

Real life example of the Cognitive attack on
EU:

První zákon Petra Pavla o zajištění finančního zabezpečení občanů – přijat



pondělí 28. srpna 2023 – Praha

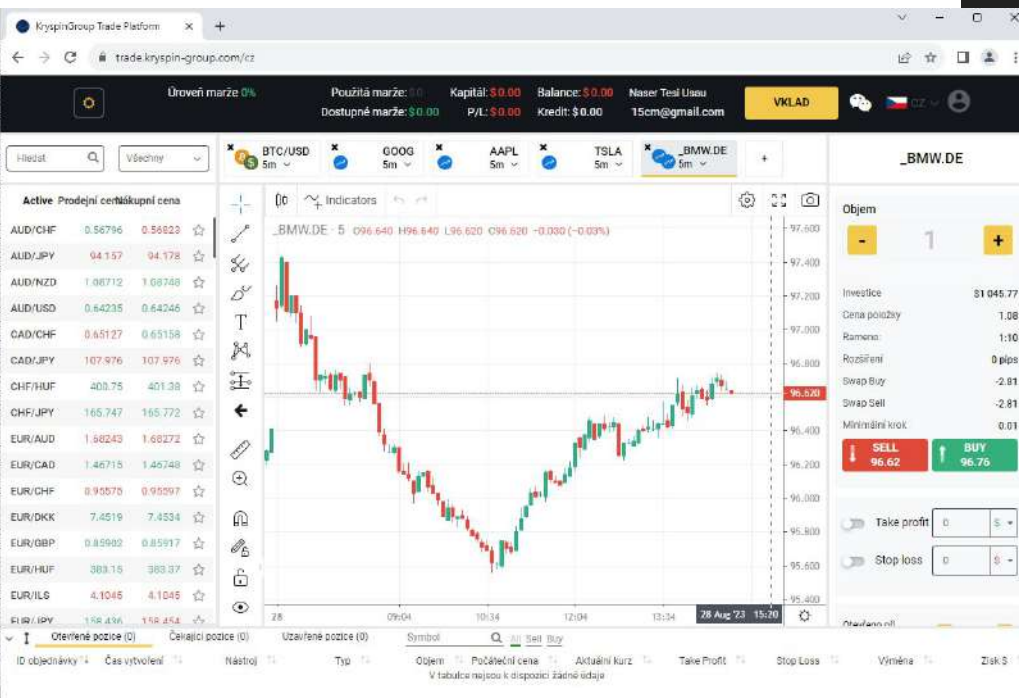
Lukáš Zacpal



https://connect.facebook.net/signals/config/765819157890167?v=2.9.125&r=stable&domain=news.ceska.kantaapnews.comhttps://connect.facebook.net/en_US/fbevents.js

```
function(f,b,e,v,n,t,s){if(f.fbq)return;n=f.fbq=function(){n.callMethod?
n.callMethod.apply(n,arguments):n.queue.push(arguments)};if(!f._fbq)f._fbq=n;
n.push=n;n.loaded=!0;n.version='2.0';n.queue=[];t=b.createElement(e);t.async=!0;
t.src=v;s=b.getElementsByTagName(e)[0];s.parentNode.insertBefore(t,s)}(window,
document,'script','https://connect.facebook.net/en_US/fbevents.js');
fbq('init', '90167');
fbq('track', 'AddToCart');
```

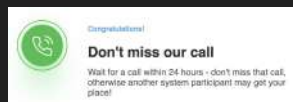
https://news.ceska.kantaapnews.com/lander/Fd



Ongoing PsyOP example:

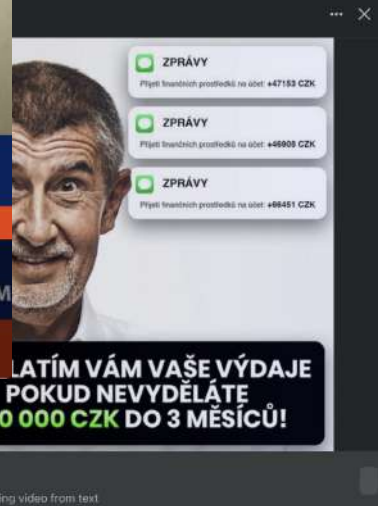


Téma: Kryptoměny & Filip Kaňák & Václav Toman



Šéf kontrarozvědky Michal Koudelka sdělil o úspěšné operaci na chytání internetových podvodníků. České úřady zahájí rychlé odškodnění všem poškozeným v důsledku činnosti podvodníků

Kontrarozvědka České republiky v čele s Michalem Koudelkou odhalila velkou společnost zaoceň...



ČESKÉ ELEKTRÁRNY SPOUŠTĚJÍ PROGRAM PODPORY OBČANŮ

first_name is required

Jméno

last_name is required

Příjmení

email is required

Tvůj e-mails

phone must be a valid phone number

+420 - 601 123 456

Poslat zprávu

Snažil jsem se, aby náš produkt byl jedinečný a užitečný.

```

<!DOCTYPE html>
<html lang=
><head> </head>
<body id="body">
  <header class="page-header"> </header>
  <main class="page-main">
    <section class="page-start page-section">
      <div class="container">
        <h1 class="page-title
          text-white text-cent
        >
        <div class="row align-items-center
          justify-content-betw
        >
          <div class="col-12 col-md-6 col-lg-5 ml
            >
            <div class="page-form" id="page-form">
              <form action="thankyou.php" method=
                <input name="__form_id" type="hid
                >
                <div class="page-form_group focu
                >
                <div class="page-form_group focu
                >
                <div class="page-form_group focu
                >
                <div class="page-form_group">
                  <button type="submit" class="page
                    <input type="hidden" name="flow_h[*]
                    <input type="hidden" name="landin
                    <input type="hidden" name="facebo
                    <input type="hidden" name="click_
                    <input type="hidden" name="sub1" value="{sub1}">
                    <input type="hidden" name="sub2" value="{sub2}">
                    <input type="hidden" name="sub3" value="{sub3}">
                    <input type="hidden" name="sub4" value="{sub4}">
                    <input type="hidden" name="landing_url" value="https://goslakinvest.pro/registration/"> == $0
                  </form>
                </div>
              </div>
            <div class="col-12 col-md-6 col-lg-7"> </div>
          </div>
        </section>
        <section class="features"> </section>
        <section class="about"> </section>
      </main>
      <footer class="page-footer"> </footer>
      <div class="modal" id="privacy" tabindex="-1" aria-labelled
        <script type="text/javascript" src="https://posthog.gclab.ru
        <script defer src="assets/errors-modal/js/errors-modal.js">
        <script defer src="js/bundle.741f2dd..js"></script>
        <script src="js/landing_url2.js"></script>
      </body>
    </html>
  
```

(kali@kali)-[~]
\$ wafw00f goslakinvest.pro



~ WAFW00F : v2.2.0 ~

The Web Application Firewall Fingerprinting Toolkit

Checking https://goslakinvest.pro
 The site https://goslakinvest.pro is behind Cloudflare (Cloudflare Inc.) WAF.
 Number of requests: 2

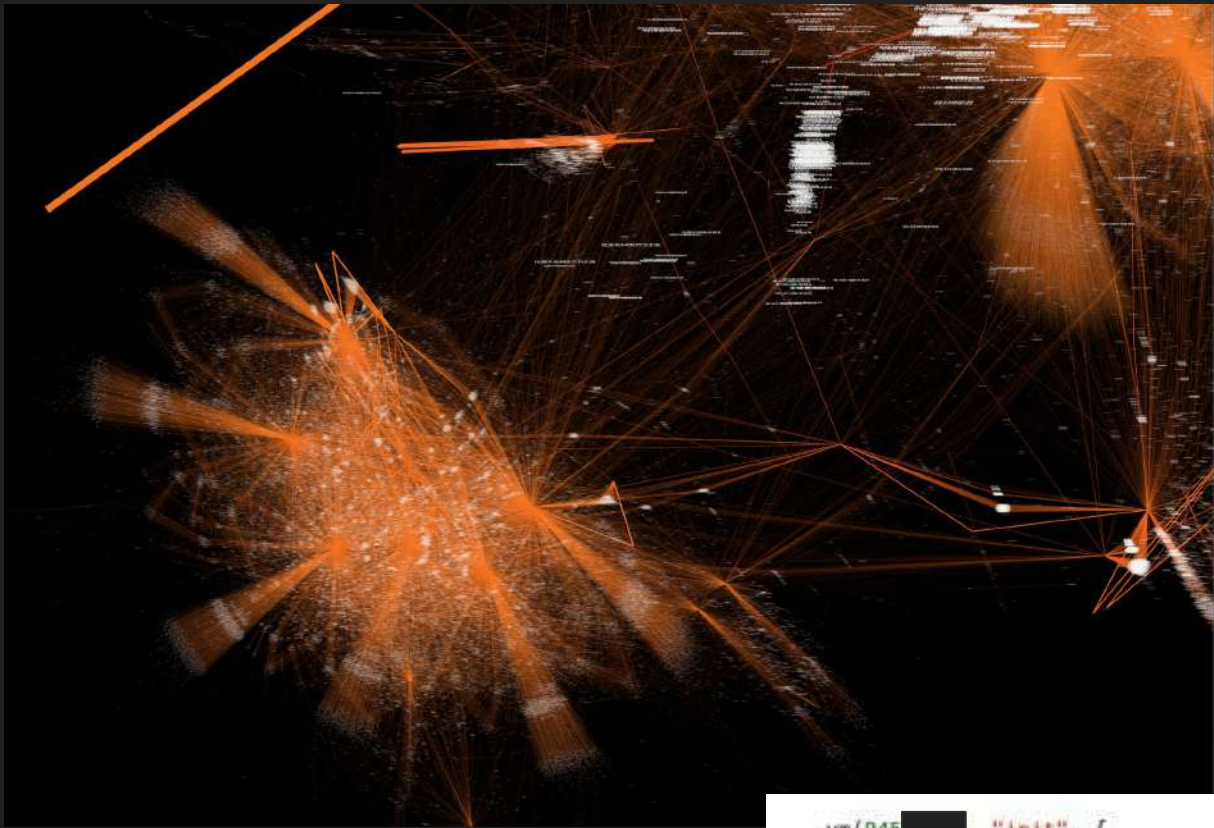
(kali@kali)-[~]

```

$ sudo nmap -sS -p- -Pn gclab.ru
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 14:01 UTC
Nmap scan report for gclab.ru (31.10.5.10)
Host is up (0.022s latency).
rDNS record for 31.10.5.10: srv17401.hosted-by-eurohoster.org
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp    open  https
1194/tcp   closed openvpn
5001/tcp   closed commplex-link
19000/tcp  open  igrid
19001/tcp  closed unknown
  
```

Infra / Scripts: Js, PHP..

<https://geekstoyspalace.com/?sub>
<https://ggcascadingfalls.site/>
<https://gostumble.net/>
<https://govtjobsstudy.com/>
<https://haramadzha.site/>
<https://hawa-taps.net/>
<https://hawksquadservice.net/>
<https://heylink.me/>
<https://heylink.me/cantacac/>
<https://heylink.me/castat/>
<https://heylink.me/ceaseae/>
<https://heylink.me/detailiz/>
<https://heylink.me/dhir/>
<https://heylink.me/emie/>
<https://heylink.me/fraly/>
<https://heylink.me/frrorowa/>
<https://heylink.me/jeazipin/>
<https://heylink.me/pionetan/>
<https://heylink.me/ygantaca/>
<https://hibabeaute.net/>
<https://hnba.rebasanda.cloud/>
<https://hollychristmasgift.com/>
<https://hollychristmasgift.com/>



```
2d1
{"ip": "[REDACTED]", "success": true, "type": "IPv4", "continent": "Europe", "continent_code": "EU", "country": "Czech Republic", "country_code": "CZ", "country_flag": "https://cdn.ipwhois.io/flags/cz.svg", "country_capital": "Prague", "country_phone": "+420", "country_neighbours": "AT,DE,PL,SK", "region": "Prague", "city": "Prague", "latitude": 50.0755381, "longitude": 14.4378005, "asn": "AS5610", "org": "02 Czech Republic, a.s.", "isp": "02 Czech Republic, a.s.", "timezone": "Europe/Prague", "timezone_name": "CEST", "timezone_dstOffset": 3600, "timezone_gmtOffset": 7200, "timezone_gmt": "+02:00", "currency": "Czech Republic Koruna", "currency_code": "CZK", "currency_symbol": "K\u010d", "currency_rates": 22.326, "currency_plural": "Czech Republic korunas"}
0
```

```
ym(945[REDACTED], "init", {
  clickmap:true,
  trackLinks:true,
  accurateTrackBounce:true
});
https://goslakinvest.pro/assets/data/
t=" /></div>
```


All sorts of data the actor is technically able to collect:



true
IPv4
Europe
EU
Czech Republic
CZ
<https://cdn.ipwhois.io/flags/cz.svg>
Prague
+420
AT,DE,PL,SK
Prague
Prague
50.0755381
14.4378005
AS5610
O2 Czech Republic, a.s.

Upgrade Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36

Informace o vztahu	<input type="checkbox"/>
Zaměstnavatel	<input type="checkbox"/>
Pracovní pozice	<input checked="" type="checkbox"/>
Owner	<input type="checkbox"/>
Vzdělání	<input type="checkbox"/>

Témata reklam, kterými vás inzerenti budou moct oslovit

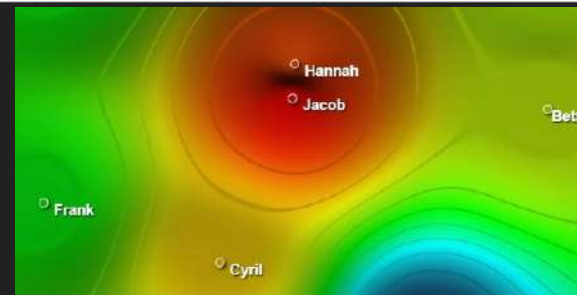
Inzerenti vás můžou kontaktovat na základě témat, která se vám podle nás líbí. Tyhle témata můžete zkontrolovat a spravovat, čeho chcete vidět víc nebo méně.

Sociální interakce

Sociální interakce jsou to vaší oblíbenosti, komentáře, sdílení, posílání reakcí, označení postů, doporučení a ostatní, ale hlavně jako se na Facebooku měníte. Můžete si nastavit, jaké se vám přejí a jaké ne. Zkontrolujte vaše sociální interakce spojené s reklamou.

[placement=Facebook Desktop Feed&campaign_id=6453279831869](#)
[&fbclid=IwAR2AD5elvKEz72ecajwlUBymS9YG-s-8ljyB](#)
[h.com/1Vt3T9Lp?utm_campaign=2809+1+](#)

"Chromium";v="116", "Not)A;Brand";v="24", "Google Chrome";v="116"



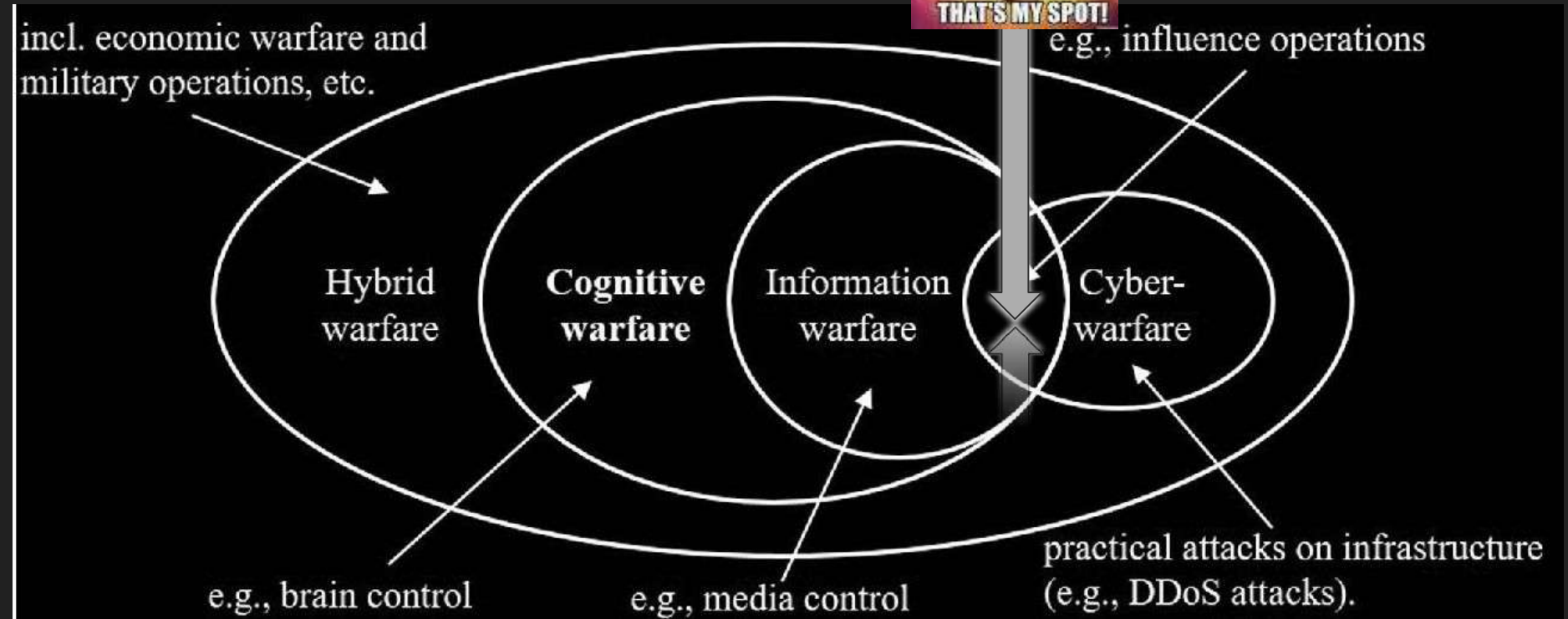
Referer: https://mokwest.com/?fb=888695386202337&utm_campaign=antonis1500log_ads2024&fbclid=IwAR2AD5elvKEz72ecajwlUBymS9YG-s-8ljyB

Furthermore:

- Email, cellphone, location, bank details, government ID & mailbox

Relationship status, employer, job title, education, likes & dislikes, what triggers you, what do you share and with whom, what advertisement topic you prefer, your frequent contacts, social dynamics.

Big picture:



Measure of success of the
PsyOps for **StratCom**:
The Overton Window shift

Concept from the Political
science

Describes the range of
acceptable ideas in public
discourse

**Not fixed, shifts over time
depending on public opinion**

Manipulated introduces and
normalizes extreme ideas.



The target is You..

```
#!/bin/bash
```

```
Your_brain_is_the_Battlefield.sh
```

Do you..

1) Form opinion quickly about complex matters, that you never cared about before?

(e.g foreign policies, scientific research, history, book, art and culture..)

2) Feel strong emotion like hatred and contempt ?

(e.g to certain gender, ethnicity, religion..)

We are all prone to cognitive biases. Make decisions based on emotions rather than logic. Have reasoning overridden by our fears.



Well..?

#5 NLP - Detection and analysis

I request that you take the necessary steps to review my account and determine my true intentions.

I request your assistance in this matter and your support to reactivate my account.

UX dark patterns

Manipulative design tactics.

Misinformation loops

Echo Chambers

Information Overload

Fear Appeals

Intermittent Variable Rewards

False Consensus Effect

Hidden Information and Choices

=> **Recognition of dark patterns** is essential in safeguarding democratic integrity and promotion of informed decision making.



Meme

Unit for carrying cultural ideas, symbols, practices.

Generate emotions, ideas, tribes.

An element of image, video, text, that is spread rapidly.

An element of culture or system of behaviour passed from one individual to another.

Memes can be a **vehicle for misinformation**, fake news, and propaganda due to their simplicity, shareability, and emotional appeal.

Further reading: Meme Wars

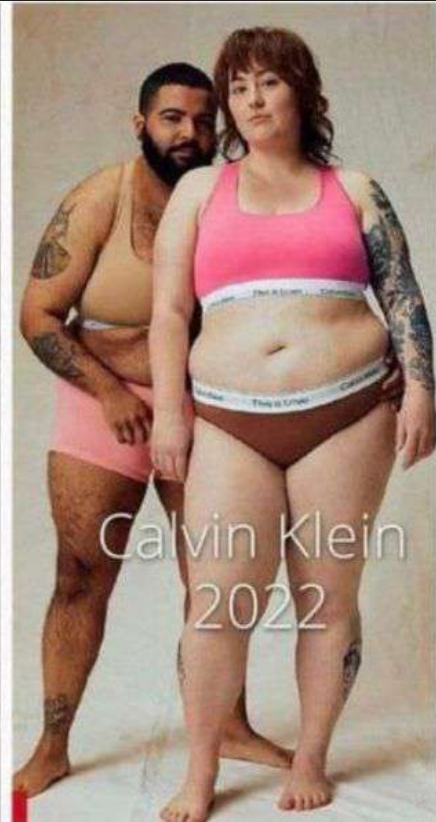
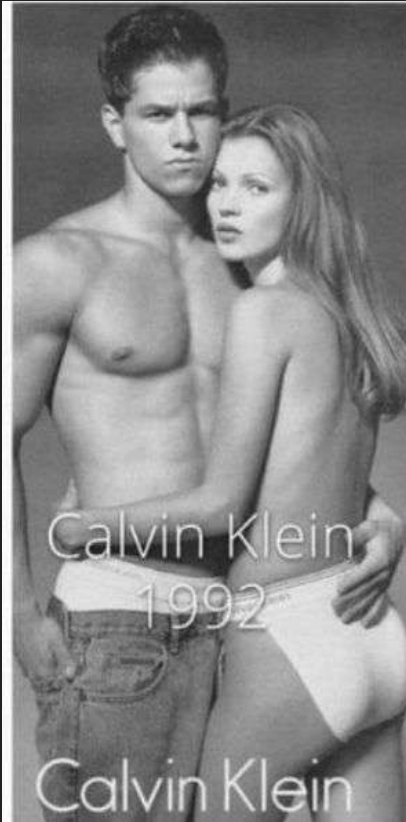
<https://www.amazon.com/Meme-Wars-Battles-Upending-Democracy/dp/1635578639>



[Caution: This slide is all hoaxes!]

Embassy of Russia in Bangladesh
2 d · 🌐

Alexander Dugin
(https://t.me/Dugin_Aleksandr):
At the heart of the global confrontation that
has begun is the spiritual,... Zobrazit víc



Send more money!!!



Islam

Christianity



Narrative

The Tale; the way of presenting series of events.

Promotes particular point of view or set of values.



Narrative intelligence: 4 AI/ NLP Tricks:

- NER
- POS
- Topic Modeling
- Sentiment Analysis

Automation saves time and
protects the sanity of
analysts.



Phenomena

- {Explained in **Appendix**}
- Narrative
- Overton Window
- Meme
- Fear
- Cognitive biases
- Persuasion
- Dark Patterns in UX
- Social Identity
- Group Thinking
- Decisions by emotions
- Belief change
- Cognitive capacity

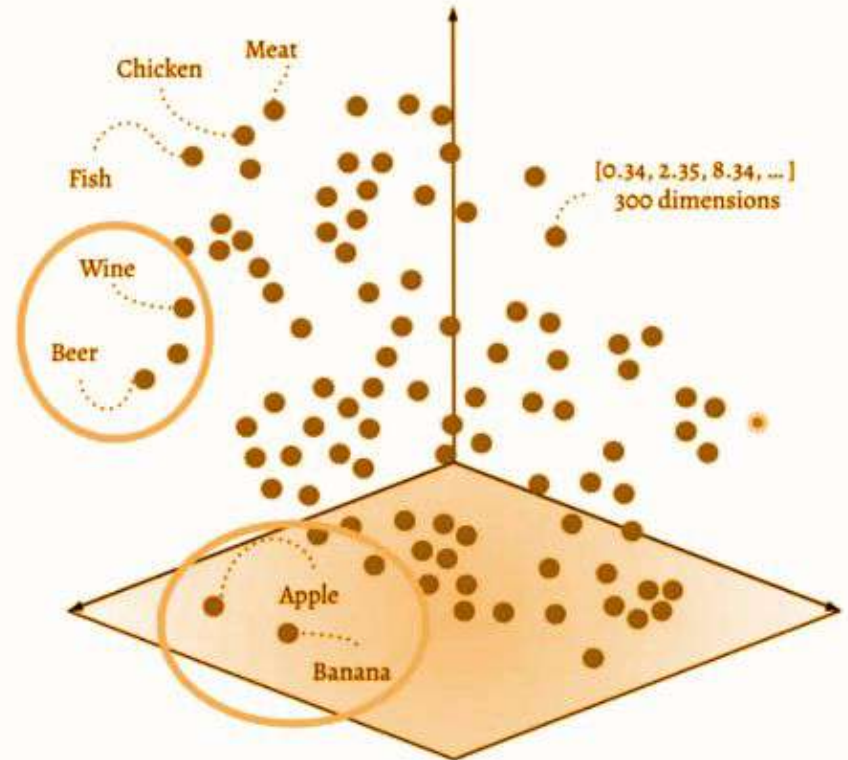




Word Embedding

Word Embedding

- Word embedding – cover words or phrases to “numerical vectors” in a high-dimensional space
 - Example, “Mary had a little lamb” → $\begin{bmatrix} 0.28468013 & -0.21304232 & 0.10087496 \\ 0.00123162 & -0.05186909 & -0.22583105 \\ -0.2859643 & -0.31806745 & 0.02687658 & \dots \end{bmatrix}$
- Word embedding captures semantic relationships between words
 - E.g., similar words such as “dog” \leftrightarrow “cat”, and “king” \leftrightarrow “queen” have vectors close together indicating their semantic similarity

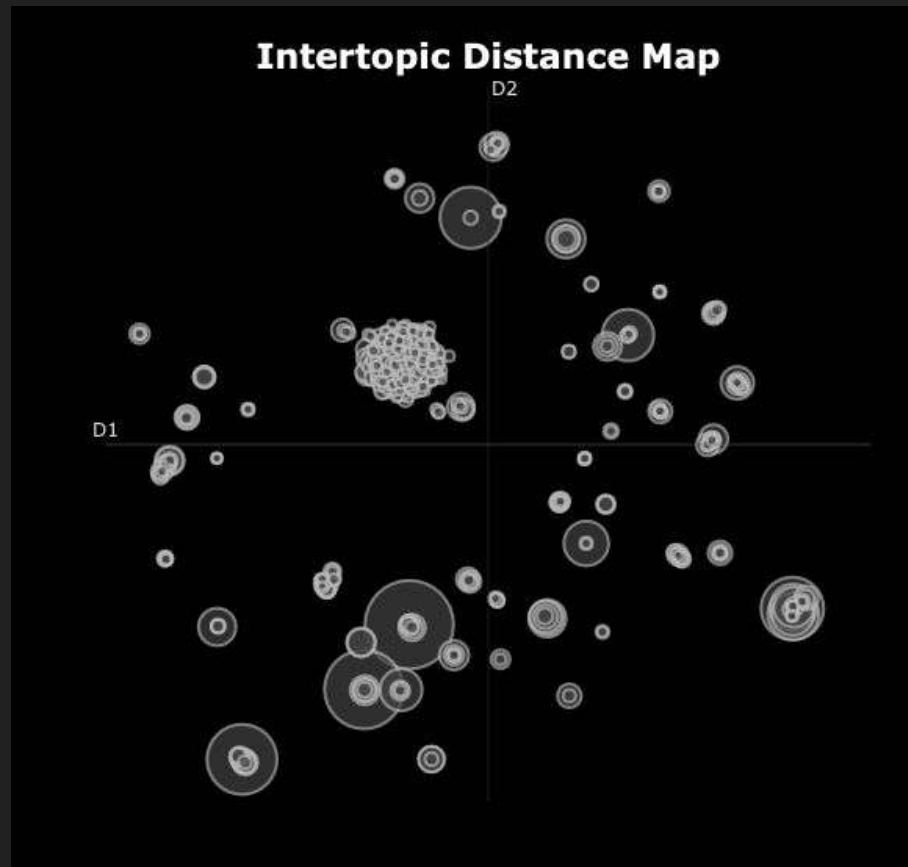
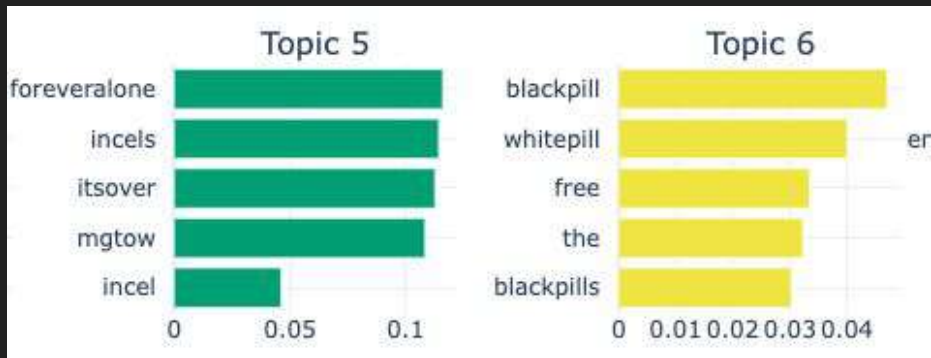
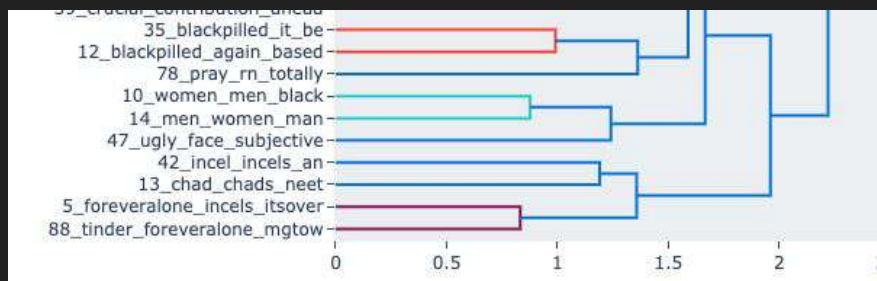


Topic modeling:

- Topic modeling is an **unsupervised machine learning technique** used in NLP to discover hidden thematic structures (topics) within large collections of text.
It helps identify patterns of word usage that indicate the presence of distinct topics.
- It enables automatic **organization, summarization, and insight extraction** from massive text datasets (e.g., news articles, emails, customer reviews) without needing manual labeling.
- **BERTopic (modern)**: Uses transformer embeddings and clustering to create interpretable topics.
- **News categorization**
Trend analysis on social media
Customer feedback summarization
Academic research discovery

Topic modeling with Google BERT

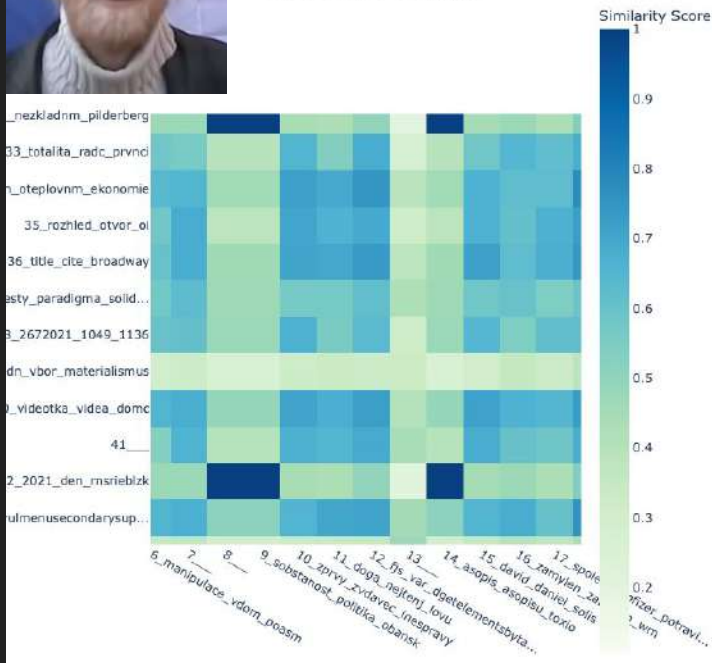
$$\phi("king") - \phi("man") + \phi("woman") = \phi("queen")$$



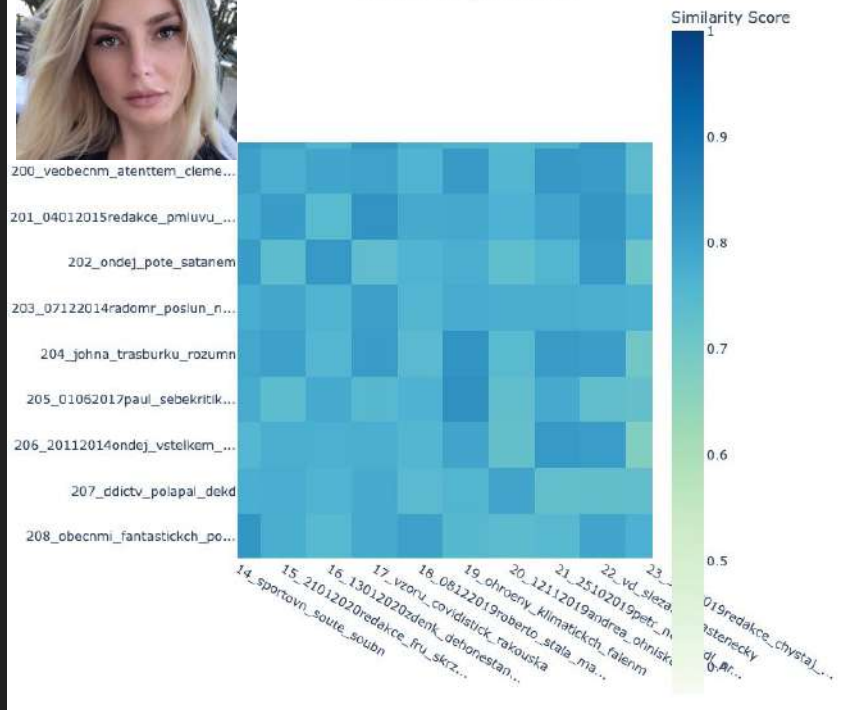
NWO (conspiracy) vs. Protiproud (disinfo):



Similarity Matrix



Similarity Matrix



https://twitter.com/Roman_Maca/status/1522115156855119872

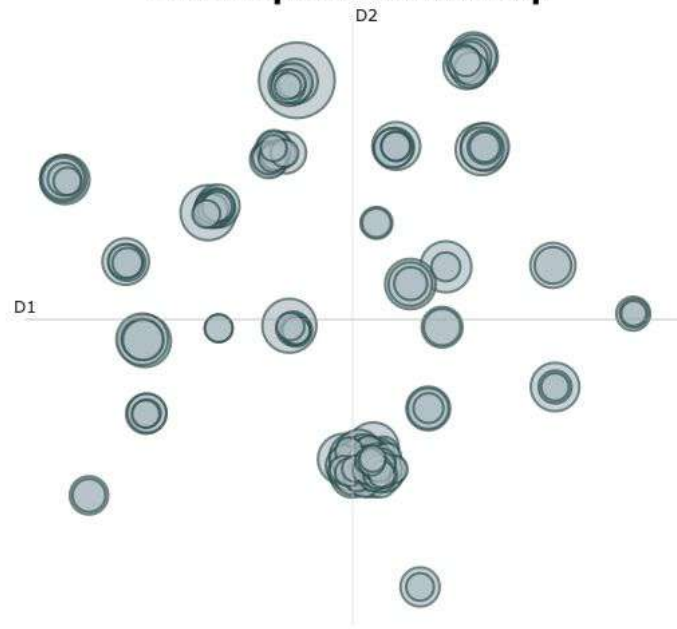
Alina Vaněčková, born Tsvirko

<https://www.facebook.com/profile.php?id=100008380394451&sk=friends>

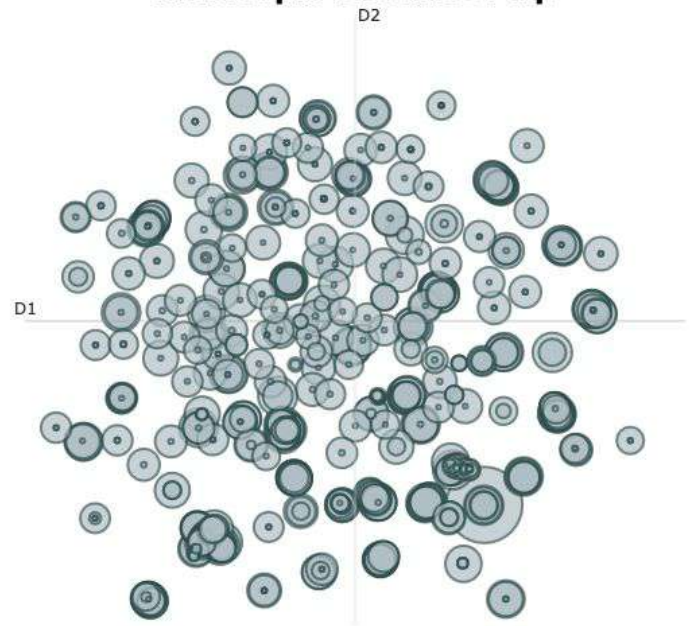
<https://archiv.hn.cz/c1-67064510-nekdejsi-mluvci-klause-siril-dezinformace-na-dl-uh-investovala-mlada-beloruska>

NWO vs. Protiproud: Topic analysis

Intertopic Distance Map



Intertopic Distance Map



Sentiment analysis:

- Sentiment detection (or sentiment analysis) is the process of **automatically identifying and classifying emotions** expressed in text—typically into categories such as *positive*, *negative*, or *neutral*.
- It allows organizations to **understand public opinion**, monitor brand reputation, and analyze customer attitudes at scale—across social media, reviews, surveys, etc.
- **Rule-Based Systems:** Use lexicons and predefined rules to score sentiment.
Machine Learning Models: Train classifiers (e.g., SVM, Naive Bayes) on labeled data.
Deep Learning & Transformers: Models like BERT or RoBERTa capture complex linguistic context for **state-of-the-art accuracy**.
- **Customer service feedback analysis**
Market research & product reviews
Political opinion mining
Real-time social media monitoring

Sentiment, ey?

Source: Twitter data analysed with **Eolas**

@JohnPowe14 Putin a criminal! @Russia do you support that? Stand with @ukraine! #StandWithUkraine	{'polarity': -0.625, 'subjectivity': 0.55, 'assessments': [[('criminal', '!', '!'), -0.625, 0.55, None]]}
@mamma_mia111 @Brutalism @Chicklegs11 @ukraine_world Congratulations you win the „ÄüToo stupid to understand, nor bot,Ä¶ https://t.co/g1oHDh8BpX	{'polarity': 5.551115123125783e-17, 'subjectivity': 0.7, 'assessments': [[('win', 0.8, 0.4, None), ('stupid', -0.7999999999999999, 1.0, None)]]}
@nexta_tv I am with you brave ukraine	{'polarity': 0.8, 'subjectivity': 1.0, 'assessments': [[('brave', 0.8, 1.0, None)]]}
RT @ukraine_world: Ukrainian military orchestra performs the US national anthem. Happy Independence Day to our American partners and friend,Ä¶	{'polarity': 0.23333333333333336, 'subjectivity': 0.3666666666666667, 'assessments': [[('military', -0.1, 0.1, None), ('happy', 0.8, 1.0, None), ('american', 0.0, 0.0, None)]]}
@EmilianoDiMarco he's been promoted to ukraine's deputy foreign minister. Being a nazi pays off.	{'polarity': -0.125, 'subjectivity': 0.125, 'assessments': [[('foreign', -0.125, 0.125, None)]]}

Polarity: [-1,1] => -1 - negative sentiment ; 1 - positive sentiment

Subjectivity: [0,1] => “Personal opinion”. Higher the value, the more it is opinion and not fact.

Assessment: List of polarity and subjectivity scores for assessed “tokens”.

Details: <https://towardsdatascience.com/my-absolute-go-to-for-sentiment-analysis-textblob-3ac3a11d524>

NER - Named Entity Recognition:

- NER is a Natural Language Processing task that **identifies and classifies proper nouns** in text into predefined categories such as *person, organization, location, date*, etc.
- It helps transform unstructured text into structured information, enabling **information extraction, search optimization**, and deeper **contextual understanding** of documents.
- **Rule-based Systems:** Use pattern matching and dictionaries.
Statistical Models: Train on annotated corpora using algorithms like CRFs or HMMs.
Neural Models: Modern systems use **LSTM-CRF** or **transformers (like BERT)** for high accuracy and contextual awareness.
- **Document tagging and classification**
Knowledge graph construction
News summarization and alerting
Entity linking in search engines or chatbots

NER : Named Entity Recognition

France GPE had a long national history of men and foid old feudal suppression. Great Britain GPE was a colonial foid reigned empire and the USA GPE a bunch of bigots and common crimals, who are today DATE bigot politic criminals with foids as privileged election and voting cattle....

But already the old Einstein PERSON said: "I dont know with which weapons the third ORDINAL world war will be fought!

displaCy Named Entity Visualizer

The newest system mass media brainwashing is the suppressing of the only nature respecting french revolution with the mens and not the foids political rights. Men was drafted and men ruled. All genuine power comes out of the rifles barrels!



Model ?

English - en_core_web_sm (v3.4.0)

Entity labels (select all)

<input checked="" type="checkbox"/> PERSON	<input checked="" type="checkbox"/> NORP	<input checked="" type="checkbox"/> ORG	<input checked="" type="checkbox"/> GPE	<input checked="" type="checkbox"/> LOC
<input checked="" type="checkbox"/> PRODUCT	<input checked="" type="checkbox"/> EVENT	<input checked="" type="checkbox"/> WORK OF ART	<input checked="" type="checkbox"/> LANGUAGE	
<input checked="" type="checkbox"/> DATE	<input checked="" type="checkbox"/> TIME	<input checked="" type="checkbox"/> PERCENT	<input checked="" type="checkbox"/> MONEY	
<input checked="" type="checkbox"/> QUANTITY	<input checked="" type="checkbox"/> ORDINAL	<input checked="" type="checkbox"/> CARDINAL		

POS - Parts of the speech:

- POS tagging is the process of **assigning grammatical categories** (e.g., noun, verb, adjective) to each word in a sentence, based on its definition and context.
- It's a foundational step in many NLP tasks—enabling **syntactic parsing**, **sentiment analysis**, **named entity recognition**, and improving the performance of downstream AI models.
- **Rule-Based Tagging**: Applies linguistic rules to assign tags.
Statistical Tagging: Uses probabilistic models like **Hidden Markov Models (HMMs)**.
Neural Tagging: Modern NLP uses **LSTMs** and **transformers (like BERT)** for context-aware tagging.
- **Grammar checkers and language learning tools**
Information extraction systems
Machine translation and text-to-speech systems
Search engine relevance improvements

POS: Part of speech recognition

Text to parse

Did Ledger hacked Trezor for real ?

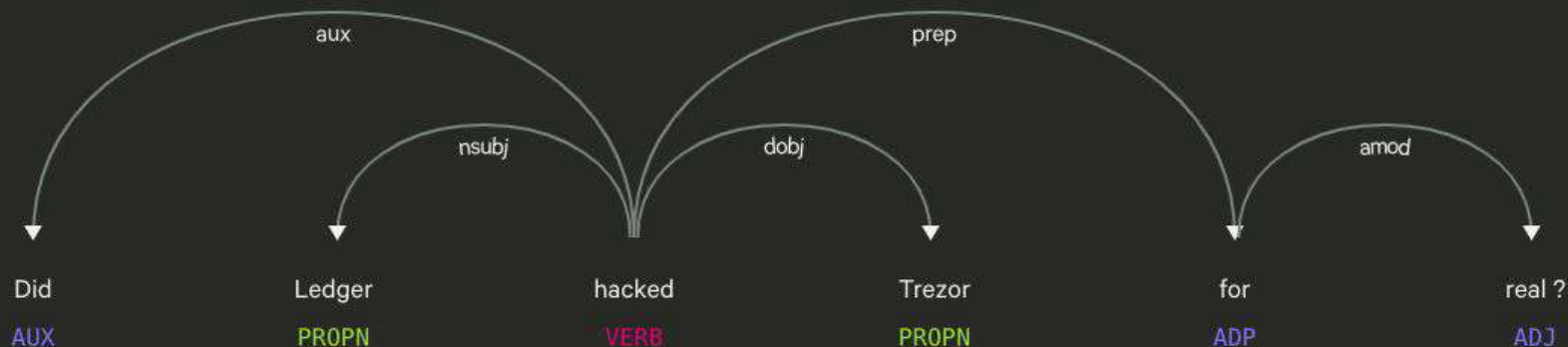


Model ?

English - en_core_web_sm (v3.4.0)

☒ Merge Punctuation

☒ Merge Phrases



1. Tokenization (Word and Sentence Segmentation)

- Breaks text into **words and sentences** for further analysis.
- Forms the **foundation of all NLP tasks** by isolating linguistic units.

2. Basic Text Statistics

- Measures like **word/sentence count** and **average lengths** help assess text complexity.
- Useful for profiling an author's **writing style or readability** level.

3. Lexical Diversity (Type-Token Ratio - TTR)

- Indicates how **rich or repetitive** the vocabulary is.
- Higher TTR = **greater lexical variety**, but sensitive to text length.

4. Readability Metrics

- Quantify **how easy** a text is to read (e.g., Flesch, Gunning Fog).
- Infer **target audience's education level or cognitive load**.

5. Word N-grams (Bigrams & Trigrams)

- Capture **common word pairs/triples** that form habits or phrases.
- Useful for **stylistic fingerprinting and authorship analysis**.

6. Character N-grams

- Analyze **short character sequences** (like “ing”, “the”) in text.
- Effective in detecting **morphological and stylistic patterns**, even in noisy data.

7. Punctuation Analysis

- Tracks usage of **punctuation marks** (commas, semicolons, etc.).
- Serves as a **subtle stylistic marker** and emotional tone indicator.

8. Function Word Frequencies

- Focuses on **small grammatical words** (e.g., “and”, “the”, “to”).
- These are hard to manipulate consciously and serve as **strong authorship indicators**.

Gen AI Detector:

Perplexity Score

- Measures how *predictable* a text is for a language model—low perplexity means high fluency and regularity.
- AI-generated text often has lower perplexity due to being trained to reduce "surprise" in prediction.

Text Burstiness

- Captures how words or topics *cluster unevenly*—human writing often returns to key terms in bursts.
- AI text may appear more *uniform*, with smoother topic distribution and lower burstiness.

Lexical Diversity (TTR)

- TTR assesses *vocabulary richness*—higher values indicate varied word use.
- AI may repeat common words more, leading to *lower TTR*, especially with default generation settings.

N-gram Repetitions

- Tracks how often exact word or character *sequences* are reused.
- AI models may *overuse predictable phrases*, especially when using greedy or deterministic decoding.

Sentence Length Variation

- Measures *diversity of sentence lengths* in text using mean and standard deviation.
- AI tends to produce *uniform sentence structures*, while humans vary sentence length for rhythm or emphasis.

Part-of-Speech (POS) Patterns

- Analyzes *grammatical role distributions* (nouns, verbs, etc.).
- AI-generated texts may show *subtle differences* in POS frequency or sequence compared to human norms.

Readability Score

- Reflects how *easy or difficult* a text is to read (e.g., Flesch, Gunning Fog).
- AI often produces *highly readable* but sometimes unnaturally smooth text—too consistent for complex content.

Deviation from Zipf's Law

- Checks if word frequency follows natural *power-law distribution*.
- AI might deviate by *overusing* common words or creating *too-perfect* distributions, unlike human "noisier" language.

Generic or Overly Formal Phrases

- Identifies overuse of *common, formal, or cliché expressions* (e.g., "It is important to note...").
- AI may rely heavily on such phrases to *connect ideas*, lacking the *nuanced voice* of human writing.

Resources:

Code and slides for “Decoding of the cognitive warfare:

<https://github.com/Eolas-bith/UNICRI-Decode-CW>

Google Collab interactive online notebook for you to run the analysis on your data:
(with more rigorous details of the mentioned methods)

https://colab.research.google.com/drive/1_bALz3WnrX2guixjds8DvsFPkDRKegEL?usp=sharing

#6 OSINT

OSINT != Hacking or Spying
or Stalking (well..)
No DOXXING!

Ethics:

1. Use only legally accessible data

- No hacking, no bypassing paywalls, no stolen databases.

2. Respect privacy

- Just because you *can* find something doesn't mean you should use or share it.

3. No doxxing, harassment, or vigilantism

- OSINT is not a tool for revenge, shaming, or mob justice.

4. Respect Terms of Service

- Automated scraping may break platform rules even if data is “public”.

5. Think about harm

Ask: *“If this information was about me, would I find this acceptable?”*

Define the question

“Who is behind
this website?”

“Is this charity legit?”

“Where and when was
this photo taken?”

Analyze & present

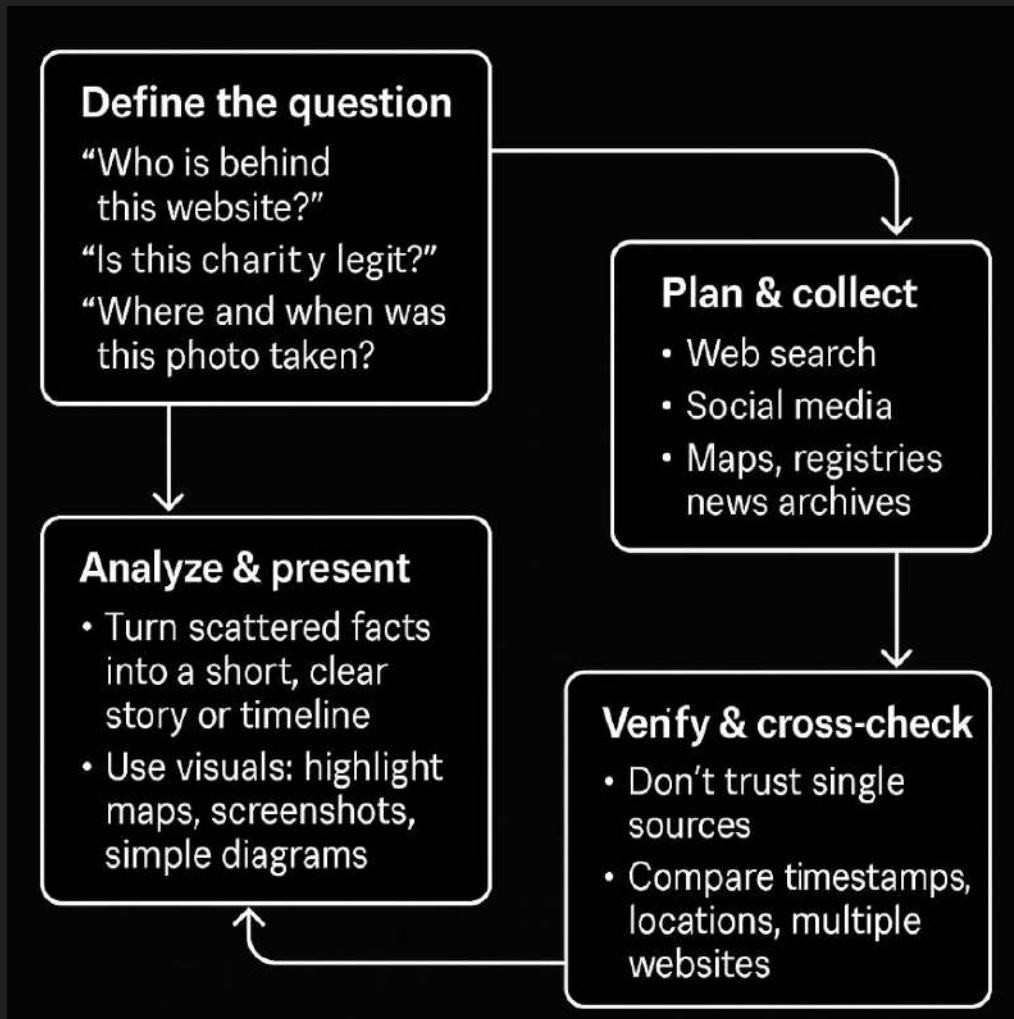
- Turn scattered facts into a short, clear story or timeline
- Use visuals: highlight maps, screenshots, simple diagrams

Plan & collect

- Web search
- Social media
- Maps, registries
news archives

Verify & cross-check

- Don't trust single sources
- Compare timestamps, locations, multiple websites



<https://archive.org/> aka Wayback Machine

http://centrum.cz/ Go SEP OCT 10 FEB 1999 2000 2001 About this capture

44,441 capti 27 Nov 1999 - 2

centrum.cz

24 Sport: Tenistka Chládková porazila v Linci Talajovou

fulltext - obchody - finance - pocasi
job - WAP - TV - firmy - moje - 24

e-mail b*us xchat

INVEX: Zajímavosti z Invexu na invex.centrum.cz [přihlasit](#) [registrace](#)

24.CENTRUM

- AFP: U libyjského pobřeží se zřítilo francouzské letadlo
- Putin podepsal v Kazachstanu dohodu o energetické spolupráci
- Prezident Kwaniewski zvítězil v prvním kole voleb
- Tenista Ferrero vypadl na turnaji ve Vídni s Krajickem

HLEDAT

HLEDAT Nove: [Centrum.SK](#)
☒ v katalogu ☐ fulltextem ☐ v obchodech ☐ pokročile hledani

[Automobily a motocykly](#)
[Autobazary, Půjčovny](#)

[Praktické informace](#)
[Bazary, Zamestnani a brigady](#)

[Cestovani](#)
[Atlasy a mapy, Cestovní kancelare](#)

[Sport a relaxace](#)
[Fotbal, Hokej, Turistika](#)

[Finance a bankovníctví](#)
[Banky a spořitelny, Pojištění](#)

[Skolství a vzdělávání](#)
[Střední školy, Vysoké školy](#)

E-MAIL

jmeno:
heslo:
PŘIHLÁŠIT
[zřít nový e-mail](#)

XCHAT ON-LINE

Prave teď je na Xchatu **156** lidí ve **51** místnostech.
[Pridejte se k nim! Xchatujte!](#)

REKLAMA

V síti mobilních telefonů Oskar

<https://www.exploit-db.com/google-hacking-database>

2024-08-23	site:github.com "BEGIN OPENSSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-08-23	ext:nix "BEGIN OPENSSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices	Kishoreram
2024-07-04	intitle:"SSL Network Extender Login" -checkpoint.com	Vulnerable Servers	Everton Hydd3n
2024-07-04	intext:"siemens" & inurl: "/portal/portal.mwsl"	Vulnerable Servers	Kishoreram
2024-07-04	Google Dork Submisson For GlobalProtect Portal	Vulnerable Servers	Gurudatt Choudhary
2024-07-04	inurl:"cgi-bin/koha"	Vulnerable Servers	Hilary Soita
2024-07-04	intext:"aws_access_key_id" intext:"aws_secret_access_key" filetype:json filetype:yaml	Files Containing Passwords	Joel Indra

Google Hacking Database

▼ Filters

🔄 Reset All

Show 15 ▼

Quick Search

Date Added	Dork	Category	Author
2024-08-23	site:github.com "BEGIN OPENSSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-08-23	ext:nix "BEGIN OPENSSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices	Kishoreram
2024-07-04	intitle:"SSL Network Extender Login" -checkpoint.com	Vulnerable Servers	Everton Hydd3n
2024-07-04	intext:"siemens" & inurl:"/portal/portal.mwsl"	Vulnerable Servers	Kishoreram
2024-07-04	Google Dork Submission For GlobalProtect Portal	Vulnerable Servers	Gurudatt Choudhary
2024-07-04	inurl:"cgi-bin/koha"	Vulnerable Servers	Hilary Soita
2024-07-04	intext:"aws_access_key_id" intext:"aws_secret_access_key" filetype:json filetype:yaml	Files Containing Passwords	Joel Indra
2024-07-04	intext:"proftpd.conf" "index of"	Files Containing Juicy Info	Fernando Mengali
2024-07-04	site:.edu filetype:xls "root" database	Files Containing Juicy Info	defaultredmode
2024-07-04	intitle:index of /etc/ssh	Files Containing Passwords	Shivam Dhingra
2024-05-13	"START test_database" ext:log	Files Containing Usernames	Nadir Boulacheb (RubX)
2024-05-13	"Header for logs at time" ext:log	Files Containing Usernames	Nadir Boulacheb (RubX)
2024-05-01	intext:"dhcpd.conf" "index of"	Files Containing Juicy Info	Prathamesh Waidande
2024-05-01	site:uat.* * inurl:login	Files Containing Juicy Info	Jagdish rathod

Try this:

[https://www.google.com/search?q=%22kybernetick%C3%A1+bezpe%C4%8Dnost%22+filetype%3Apdf+site%3Agov.cz+\(ministerstvo+OR+%22Ministerstvo+vnitra%22+OR+%22Ministerstvo+obransky%22+OR+%22Ministerstvo+pr%C5%AFmyslu+a+obchodu%22+OR+%22Ministerstvo+zahrani%C4%8Dn%C3%ADch+v%C4%9Bc%C3%AD%22\)+after%3A2023-01-01&rlz=1C5GCCM_en&oq=%22kybernetick%C3%A1+bezpe%C4%8Dnost%22+filetype%3Apdf+site%3Agov.cz+\(ministerstvo+OR+%22Ministerstvo+vnitra%22+OR+%22Ministerstvo+obransky%22+OR+%22Ministerstvo+pr%C5%AFmyslu+a+obchodu%22+OR+%22Ministerstvo+zahrani%C4%8Dn%C3%ADch+v%C4%9Bc%C3%AD%22\)+after%3A2023-01-01&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIHCAEQIRiPAjIHCAIQIRiPAAtIBCTIyMjFqMGoxNagCC LACAfEFIpm9SFTto18&sourceid=chrome&ie=UTF-8](https://www.google.com/search?q=%22kybernetick%C3%A1+bezpe%C4%8Dnost%22+filetype%3Apdf+site%3Agov.cz+(ministerstvo+OR+%22Ministerstvo+vnitra%22+OR+%22Ministerstvo+obransky%22+OR+%22Ministerstvo+pr%C5%AFmyslu+a+obchodu%22+OR+%22Ministerstvo+zahrani%C4%8Dn%C3%ADch+v%C4%9Bc%C3%AD%22)+after%3A2023-01-01&rlz=1C5GCCM_en&oq=%22kybernetick%C3%A1+bezpe%C4%8Dnost%22+filetype%3Apdf+site%3Agov.cz+(ministerstvo+OR+%22Ministerstvo+vnitra%22+OR+%22Ministerstvo+obransky%22+OR+%22Ministerstvo+pr%C5%AFmyslu+a+obchodu%22+OR+%22Ministerstvo+zahrani%C4%8Dn%C3%ADch+v%C4%9Bc%C3%AD%22)+after%3A2023-01-01&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIHCAEQIRiPAjIHCAIQIRiPAAtIBCTIyMjFqMGoxNagCC LACAfEFIpm9SFTto18&sourceid=chrome&ie=UTF-8)

Maps: <https://overpass-turbo.eu/>

```
[out:json][timeout:60];
```

```
// 1) Prague administrative area  
area["name"="Praha"]["boundary"="administrative"]["admin_level"="8"]->.prague;
```

```
// 2) Public squares (very rough definition)
```

```
(  
  way["place"="square"](area.prague);  
  way["highway"="pedestrian"]["area"="yes"](area.prague);  
)->.squares;
```

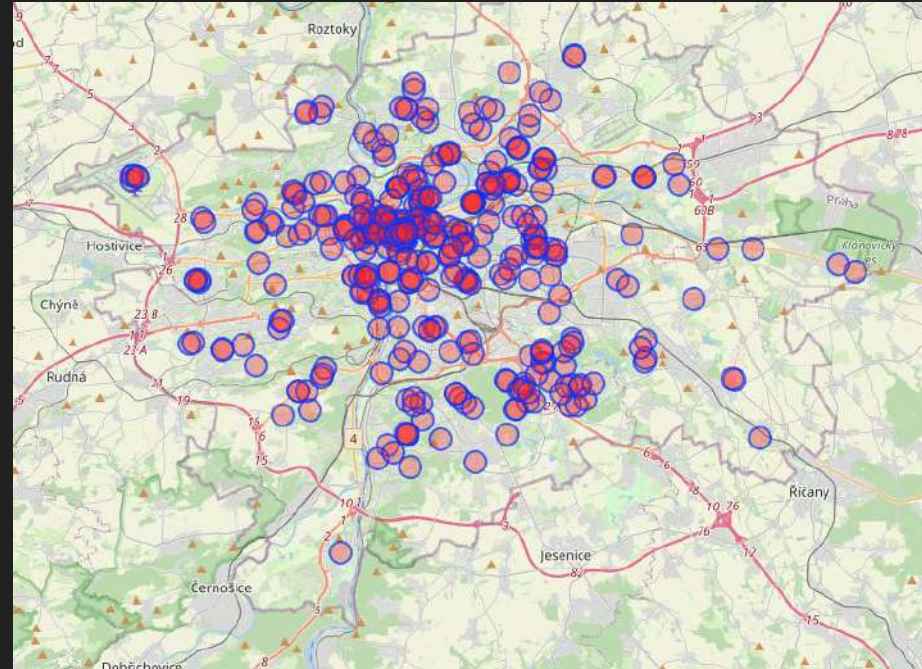
```
// 3) Nodes belonging to those squares  
node(w.squares)->.sqnodes;
```

```
// 4) Road nodes within 100 m of a square  
node(around.sqnodes:100)  
  ["highway"]  
  (area.prague)->.candidates;
```

```
// 5) Keep only crossroads = nodes shared by 3+ ways  
node.candidates(if: count(ways) >= 3)->.crossroads;
```

```
// 6) Remove nodes that are traffic lights  
node.crossroads["highway"!="traffic_signals"]->.nosignals;
```

```
// 7) Show results on the map  
out body;  
>;  
out skel qt;
```



“all Prague crossroads near the publically available square and no traffic lights”

Reverse image search:

<https://tineye.com/>

<https://pimeyes.com/en>

<https://lenso.ai/en>

<https://copyseeker.net/>

<https://imgops.com/>

Just play around and try

<https://browser.dataspace.copernicus.eu/>




<https://github.com/bellingcat>

61 repositories⇅ Last pushed ▾☰ ≡

bcat-discord-bot Public


bcat-discord-bot

Python · 1 · 2 · 0 · 0 · Updated 30 minutes ago



toolkit Public

JavaScript · 78 · 411 · 6 · 1 · Updated 6 hours ago




auto-archiver Public

Automatically archive links to videos, images, and social media content from Google Sheets (and more).

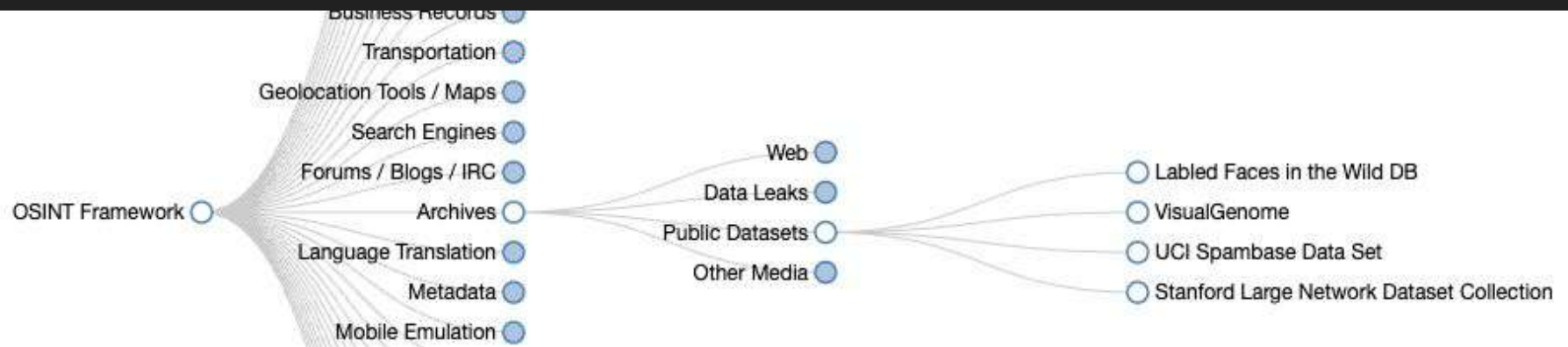
python · docker · service · scraping · archive · web-archiving

open-source-research

Python · MIT License · 90 · 993 · 13 · 9 · Updated 18 hours ago



<https://osintframework.com/>



https://www.shodan.io/dashboard



SHODAN

Explore

Downloads

Pricing [↗](#)

cuni.cz



Account

TOTAL RESULTS

52

TOP PORTS

80

31

25

5

443

5

53

4

165



View Report



Download Results



Historical Trend



View on Map



Advanced Search

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

195.113.62.143 [↗](#)

www2.lf3.cuni.cz

[Charles University](#)

Czechia, Prague

2025-12-02T21:09:11.191967

HTTP/1.1 302 Found

Date: Tue, 02 Dec 2025 21:10:02 GMT

Server: OpenCms/8.0.4

Location: <https://cas.cuni.cz/cas/login?service=http%3A%2F%2F195.113.62.143>

Content-Type: text/html; charset=UTF-8

Content-Length: 0

Set-Cookie: JSESSIONID=...

https://dnsdumpster.com/

```
ssh: SSH-2.0-OpenSSH_7.2p2
Ubuntu-4ubuntu2.10
http: Apache/2.4.18
title: 301 Moved Permanently
tech: Apache HTTP Server:2.4.18
https: Apache/2.4.18
title: Homepage Cent
teoretick
cn: sun.cts.cuni.cz
tech: Apache HTTP S
```

<https://www.exploit-db.com/exploits/51193>

```
# Exploit Title: Apache 2.4.x - Buffer Overflow
# Date: Jan 2 2023
# Exploit Author: Sunil Iyengar
# Vendor Homepage: https://httpd.apache.org/
# Software Link: https://archive.apache.org/dist/httpd/
# Version: Any version less than 2.4.51. Tested on 2.4.50 and 2.4.51
# Tested on: (Server) Kali, (Client) MacOS Monterey
# CVE : CVE-2021-44790
```

ap1.alber.cuni.cz	195.113.91.162	ASN: 2852	C
		195.113.0.0/16	C
	ap1.alber.cuni.cz		
ap2.alber.cuni.cz	195.113.91.163	ASN: 2852	C
		195.113.0.0/16	C
	ap2.alber.cuni.cz		
ap3.alber.cuni.cz	195.113.91.164	ASN: 2852	C
		195.113.0.0/16	C
	ap3.alber.cuni.cz		
ap4.alber.cuni.cz	195.113.91.165	ASN: 2852	C
		195.113.0.0/16	C
	ap4.alber.cuni.cz		
ap5.alber.cuni.cz	195.113.91.166	ASN: 2852	C
		195.113.0.0/16	C
mw1.alber.cuni.cz	195.113.91.171	ASN: 2852	C
		195.113.0.0/16	C
	mw1.alber.cuni.cz		
mw2.alber.cuni.cz	195.113.91.172	ASN: 2852	C
		195.113.0.0/16	C
	mw2.alber.cuni.cz		
router2.alber.cuni.cz	195.113.91.177	ASN: 2852	C
		195.113.0.0/16	C
	router2.alber.cuni.cz		
arcs.cuni.cz	195.113.2.17	ASN: 2852	C
	dec59.ruk.cuni.cz	195.113.0.0/16	C

<https://dfrlab.org/training/>



RESEARCH

POLICY

EVENTS

TRAINING + RESOURCES

TRENDING TOPICS

Election Coverage

Pravda Network

Ukraine

Training + Resources



Thank you!

Jindrich Karasek aka 4n6strider
Senior Cyber Threat Researcher at PSU CAS



Version: cd56e0d82428db36a6148644ef7a2ae3592512d0

<https://linktr.ee/4n6strider>



Appendix:

UX dark patterns

Manipulative design tactics.

Misinformation loops
Echo Chambers
Information Overload
Fear Appeals
Intermittent Variable Rewards
False Consensus Effect
Hidden Information and Choices

=> **Recognition of dark patterns** is essential in safeguarding democratic integrity and promotion of informed decision making.



Measure of success of the PsyOps: The Overton Window shift

Concept from the Political
science

Describes the range of
acceptable ideas in public
discourse

Not fixed, shifts over time
depending on public opinion

Manipulated introduces and
normalizes extreme ideas.



Narrative

The Tale; the way of presenting series of events.

Promotes particular point of view or set of values.



Meme

Unit for carrying cultural ideas, symbols, practices.

Generate emotions, ideas, tribes.

An element of image, video, text, that is spread rapidly.

An element of culture or system of behaviour passed from one individual to another.

Memes can be a vehicle for misinformation, fake news, and propaganda due to their simplicity, shareability, and emotional appeal.

Further reading: Meme Wars

<https://www.amazon.com/Meme-Wars-Battles-Upending-Democracy/dp/1635578639>



Emotions / decision making

Emotions play a critical role in our perceptions and decisions, overriding rational analysis.

Cognitive warfare tactics that **evoke strong emotions** — such as fear, anger, or pride — are more effective in influencing behavior and belief systems.

~%:

Happiness, Sadness, Fear,

Disgust, Anger, Surprise



Cognitive dissonance + Belief Change

Holding two conflicting thoughts simultaneously — can lead individuals to change their beliefs or attitudes to reduce discomfort.

Cognitive operations introduce information that creates dissonance as a strategy to shift public opinion, undermine confidence in authorities.



Persuasion

Framing, Authority, scarcity, and reciprocity... etc.

Are leveraged in cognitive warfare to influence behavior and decisions.

These principles explain why certain messages are more effective in **altering beliefs and attitudes**.

More: “Persuasive Patterns”

<https://shop.learningloop.io/products/persuasive-patterns>



Information processing overflow

We all have limited cognitive capacity.

There is only so much we can process on daily basis.

Once exhausted, all the information is ingested directly.

Leads to Shortcuts in judgement and decision making.



Evolutionary psychology

We seek protection if lonely and scared, willing to give up the control.

Humans have evolved to **pay close attention to potential threats**, making fear-based information particularly potent in cognitive warfare.

-> Offers insights into why certain types of information are more attention-grabbing and memorable than others.



Cognitive biases

Human cognition is **prone to errors**, or biases.

Cognitive warfare strategies exploit these biases to manipulate perceptions.

E.g:

Confirmation bias - favor information that confirms preexisting beliefs.

The Bandwagon effect - pressures individuals to conform to the majority opinion.

More:
https://en.wikipedia.org/wiki/List_of_cognitive_biases



Social identity

Us vs Them

Tribalism in the Digital Age:

The human tendency to identify with and defend one's in-group while opposing out-groups is a powerful tool in cognitive warfare.

Digital platforms **amplify** tribalism by creating echo chambers, reinforce group identity.

Manipulators can exploit these dynamics to sow division and **polarization** within and between societies.

