

# Tech Tuesday Zurich:

## Internet Security, Infrastructure & POTUS

### Mindsets and Methods of Mass Surveillance and application in Switzerland

Hernâni Marques (@vecirex), CCCZH / CCC-CH

hernani@{{cccti,ccczh,ccc-ch}.ch,vecirex.net}  
0EE4 679E 7198 7A66 37D0 3395 D425 5D18 53C9 182C

Impact Hub @Viadukt, Feb 7th 2017, 7pm+

# Overview

- 1 Problem: Mass Surveillance
- 2 Mindsets
- 3 Methods
- 4 Application in Switzerland
- 5 Solution: Mass Encryption
- 6 \$myInput

# Disclaimer

- **Chaos Computer Club (CCC)**: member.
- **Chaos Computer Club Ticino (CCCTI)**: *in foundation*.
- **Chaos Computer Club Zurich (CCCZH)**: board member.
- **Chaos Computer Club Switzerland (CCC-CH)**: board member.
- **Digitale Gesellschaft Schweiz (Digiges)**: member.
- **p≡p foundation** (non-commercial, tax-free): council member.
- **p≡p security** (commercial): Dev(Ops) & misc. employee.
- **VICE Switzerland**: contributing writer.
- Strategy when in contact with police, secret services, data-collecting firms: full-disclosure, including media escalations. → “Light on them!”

# Nature of Mass Surveillance

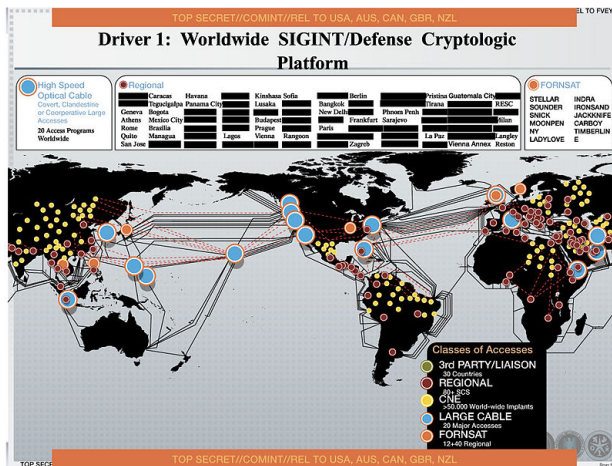
- Mass Surveillance is given when data flows (permanently saved or not) are searched for a needle (like in a haystack).
- It's not necessary to save the data permanently: you can also just buffer data for a while in RAM.
- Mass Surveillance AFK is comparable to airport situations where people are randomly picked out or being searched based on “suspicions” (=needles or selectors); also searching all postal letters, opening and eventually copying them for further processing is Mass Surveillance.
- Even if no results (hits) occur, still Mass Surveillance was carried out: like in web searching for public data when way too specific search terms are used.

# Types of needles or selectors

Different types of needles (=selectors) exist:

- **Hard selectors** (focussed on metadata): phone numbers, email addresses, chat nicknames, IP addresses etc.
  - Usually used when you basically know who your “targets” are, like phone numbers of diplomats, journalists, CEOs, Angela Merkel ...
- **Soft selectors** (focussed on content): word combinations in text or (transcribed) voice, pattern matches in text, graphics, videos etc.
  - Not seldomly used when you basically have no clue what you are searching for, like in cases of “terrorists”, where not enough “training data” exists ...
- Combinations of both selector types are also possible: not always can they even be distinguished.

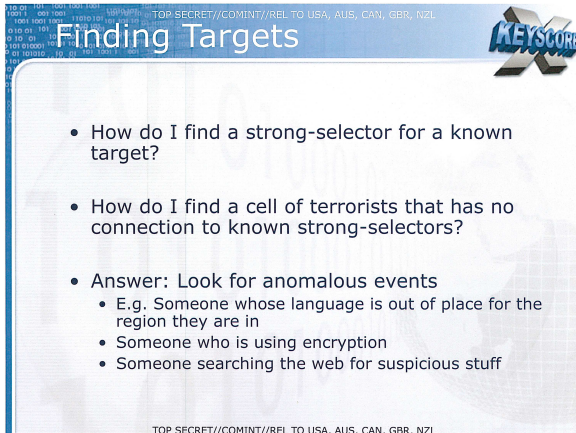
# Example in a general (NSA-led) global context



# Example in a general (Swiss) local context



# Needle creationism for Five-Eyes analysts



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## Finding Targets

KEYSCORE

- How do I find a strong-selector for a known target?
- How do I find a cell of terrorists that has no connection to known strong-selectors?
- Answer: Look for anomalous events
  - E.g. Someone whose language is out of place for the region they are in
  - Someone who is using encryption
  - Someone searching the web for suspicious stuff

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



# No Hollywood movies needed – INDECT showtime!

INDECT = “**I**ntelligent information system supporting observation, searching and **d**etection for security of **c**itizens in urban environment”



## Project Indect (EU Surveillance Programme)

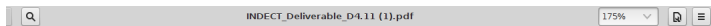
Topics [EU](#), [Project Indect](#), [leak](#), [Leaked](#), [surveillance](#), [state](#), [totalitarianism](#), [civil rights](#), [privacy](#),

INDECT-400px.ogvâ (Ogg multiplexed audio/video file, Theora/Vorbis, length 5m41s, 400Ã222 pixels, 962kbps overall)  
[edit] Summary

### DOWNLOAD OPTIONS

<a href="#">H.264</a>	1 file
<a href="#">OGG VIDEO</a>	1 file
<a href="#">TORRENT</a>	1 file

# INDECT: Detect suspicious (web) texts



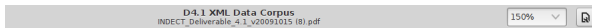
## 6. Pattern Matching

In this step we select patterns which show high association to suspicious websites than to normal websites. In many suspicious websites, the sentences containing messages to influence criminal activities are generally grouped within other normal sentences. For example, a suspicious websites can have many factual information and few suspicious lines. Thus, the patterns extracted from such suspicious websites are not all indicative of criminal activities. Most of these patterns will also occur in normal websites. To filter out such normal patterns we use a very simple approach. Once we generate patterns from both suspicious websites and normal websites. The patterns indicative of criminal activities are only those which are not present in normal websites. Thus, we select only patterns which are present in suspicious websites but not in normal websites. For exam-

Patterns from suspicious websites	Patterns from normal website
hand-package-boss	everest-mountain
everest-mountain	tall-mountain-world
tall-mountain-world	temperature-cold-winter

Table 4: Possible patterns generated from suspicious and normal websites

# INDECT: Named Entity Recognition in a “terrorist” chat



## 4.4.3 Terrorist chat<sup>7</sup>

**Shazad Tanweer** [PER.Individual]: Any extra risks getting into **Pakistan** [GPE.NAT] ?

**Omar Khyam** [PER.Individual]: We had five **Bengalis** [GPE.NAT] last year. Guess how **we** [PER.Group] got **them** [GPE.NAT] in. From **Bangladesh** [GPE.NAT] all the way across **India** [GPE.NAT] into **Pakistan**[GPE.NAT]... **we** [PER.Group] bribed the guy [PER.Individual]. You know when you [PER.Individual] go to the check-in, it would all be set up.

**Mohammed Siddique Khan** [PER.Individual]: Going through the airport - normal tickets.

**Omar Khyam**[PER.Individual]: Yeah, just walk straight through bruv normal, just act as if you are a **Pakistani** [GPE.NAT].

**Shazad Tanweer** [PER.Individual]: I live in **Faisalbad** [GPE.NAT]

**Omar Khyam** [PER.Individual]: That's not a problem

**Omar Khyam** [PER.Individual]: All right **bruv** [PER.Individual]. Get your parents to pick you up. Or your family ... And that way you will breeze through the airport seriously. Even if **they** [ORG.GOV] are following **you** [PER.Individual] - it doesn't really count. Chill out, proper chill out ... until **we** [PER.Group] contact you and then we'll pick **you** [PER.Individual] up.

# Soft selectors (thematic search) in email contexts

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## Example 4

- **\$acwitems** = 'machine gun' or 'grenade' or 'AK 47'
- **\$acwpositions** = 'minister of defence' or 'defense minister'
- **\$acwcountries** = 'somalia' or 'liberia' or 'sudan'
- **\$acwbrokers** = 'south africa' or 'serbia' or 'bulgaria'
- **\$acwports** = 'rangoon' or 'albasra' or 'dar es salam'

```
topic('wmd/acw/govtorgs') =  
  email_body($acwitems and $acwpositions and  
    ($acwcountries or $acwbrokers or $acwports));
```

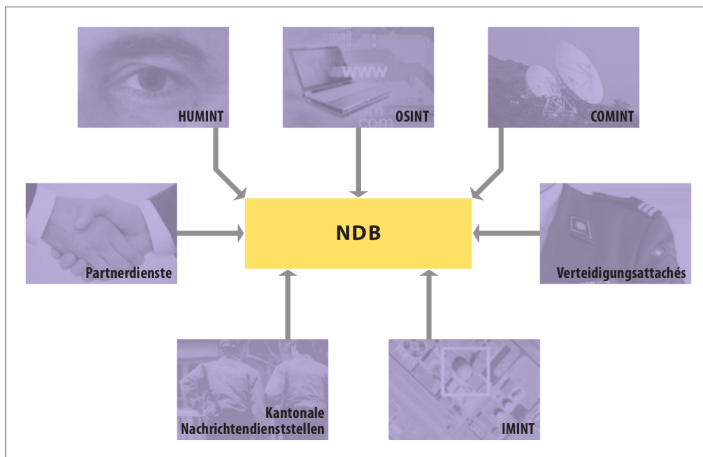
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

# Selector searches for just everything digitally written

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL	
<h2>Communication Based Contexts</h2>	
email_body(expr)	The UTF-8 normalized text of all email bodies. <code>email_body('how to' and 'build' and ('bomb' or 'weapon'))</code>
chat_body(expr)	The UTF-8 normalized text of all chat bodies. <code>chat_body('how to' and 'build' and ('bomb' or 'weapon'))</code>
document_body(expr)	The UTF-8 normalized text of the Office document. – Office documents include (but are not limited to) Microsoft Office, Open Office, Google Docs and Spreadsheets. <code>document_body('how to' and 'build' and ('bomb' or 'weapon'))</code>
calendar_body(expr)	The UTF-8 normalized text of all calendars. An example is Google Calendar. <code>calendar_body('wedding')</code>
archive_files(expr)	Matches a list of files from within an archive. For example is a ZIP file is transmitted, all names of files within are passed to this context. <code>archive_files('bad.dll' or 'virus.doc')</code>
http_post_body(expr)	The UTF-8 normalized text HTTP url-encoded POSTs. <code>http_post_body('action=send' and 'badguy@yahoo')</code>
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL	

# Swiss secret service (NDB) sensors

Die Sensoren des NDB



# Data retention for LI purposes: BÜPF / LSCPT

- **Today:** Data retention of 6 months for **access providers** (including mobile phones).
- **2018:** Data retention of 6 months *additionally* for **service providers**; private providers of Internet access (firms, schools, associations etc.) must give at least access to their infrastructure, such that the state can install implants  
...
- **Sep 2017:** Also the Swiss secret service (NDB) can access all data accessible by the BÜPF law, i.e. (mis)using law-enforcement. (Today the NDB can “just” query through BÜPF / LSCPT law whom a hard selector belongs to (e.g., a phone number or IP address)).

# More Mass Surveillance & Data retention for the NDB: ZNDG / VEKF / NDG

- **Before 2013:** *Onyx* was built as of 1999 illegally and passed in parliament under the military budget as “multi-purpose building” for CHF 45 millions. *Onyx* works in full operation since 2005 – for 7 years (!) illegally.
- **Today:** As of 2012 legal basis (ZNDG / VEKF) was created for *Onyx* to operate: data from mass surveillance on SAT-based communications can be retained for 1.5 (content) and 5 (!) years (metadata).
- **Sep 2017:** The secret service law NDG *additionally* introduces cable-based mass surveillance. In the corresponding executive order NDV, once again, the same data retention rules are imposed: 1.5 and 5 years for content and metadata, respectively.



# Some more novelties introduced by NDG / NDV

- Mass Surveillance is not carried out by the NDB, but by the Swiss Military (unit: Zentrum für Elektronische Operationen (ZEO)). The NDB “just” gets the results.
- Search categories must be accepted by three instances (court, administrative & political control), *but* by the executive order NDV the Swiss Military can add further selectors on its own if the results are not satisfying . . .
- The NDB is not allowed to search for “Swiss” Named Entities like person or firm names, but this can be circumvented by means from Computational Linguistics / Information Retrieval or by cooperating with the German BND . . .

# Not enough NDG / NDV novelties? Let's go on!

- Swiss **access** and **service providers** must allow the ZEO (for purposes of the NDB) to “install equipment”, i.e. **Swiss Military can install implants in Swiss ICT infrastructure.**<sup>i</sup>
- The NDB can use drones (IMINT) to carry out Mass Surveillance from the sky . . . at least they're not supposed to be armed.
- The NDB has the right to collect data from video surveillance actors (both, state-run and privately owned ones) → Switzerland is INDECT-ready.
- The NDB does not have to get permission to carry out “cyberwar” (or install trojan horses) on a device-by-device basis: just on a per-case (or “case complex”) basis. In theory, wide-scale attacks could be carried out.<sup>ii</sup>

---

<sup>i</sup>There's at least a remuneration of CHF 150 / hour. In cases of disputes, it's the NDB to decide how much it costs. :)

<sup>ii</sup>XKeyscore allows to show all vulnerable machines matching certain criteria, like countries, device types etc.

# Which personal data might be collected?

What's to be collected with the NDG is in no way less than was done in times of the "Fichenaffäre", where it was revealed by the end of the 1980s that Swiss Federal Police had collections of data on persons and groups in around 900k cases.

vice.com/alps/article/ein-hacker-erklart-wie-dich-der-schweizer-staat-bald-ausspionieren-ki

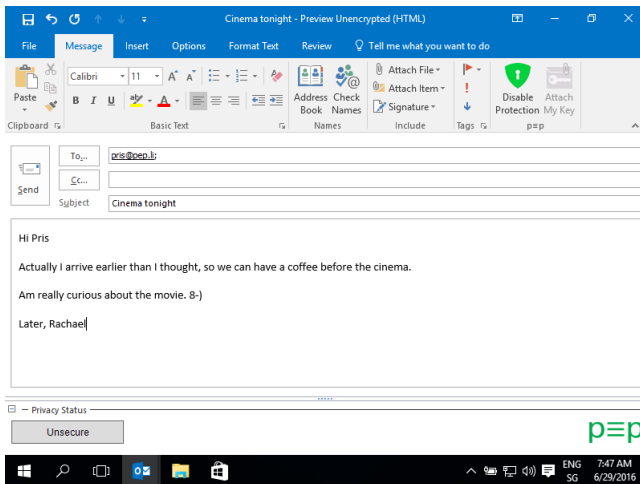
VICE

- Etwas versteckt im Anhang 17 der VIS-NDB wird auch die Intensität der sogenannten "genehmigungspflichtigen Überwachungsmassnahmen", zu denen die Instrumente der Massenüberwachung wie Funk- und Kabelaufklärung gehören, deutlich: Adressen, Augen-, Haar- und Hautfarbe, Beruf, Fotografien, Geburtsdatum und -ort, Finanzverhältnisse, Grösse, Kontaktnetze, Medizindaten, Namen, Religion, politische Ausrichtung und Ideologie, Staatsangehörigkeit oder schlichtweg alles, dem man habhaft wird – das ist eine regelrechte Erfassung eines Menschen, wie sie der Ende der 1980er aufgeflogenen **Fichenaffäre** in nichts nachsteht.

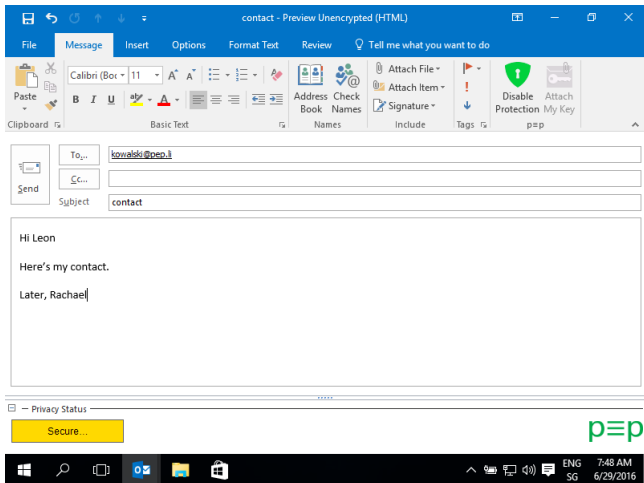
# Some requirements for a safe, privacy-friendly Internet

- Fully decentralized (peer-to-peer) or at least federated infrastructures anyone can participate in (similar to Blockchain technology, Bittorrent, email or XMPP/Jabber).
- Free choice of identity (unlike in Signal or WhatsApp with fixed, hard selectors (i.e., cell phone numbers)).
- End-to-end cryptography for all services with private keys saved solely on the end-users' devices and peer-to-peer distribution of public keys (no keyservers or other key storage locations: avoid re-encryption (MITM) attacks).
- Full-disk encryption on all devices.
- Strong passwords (=easy memorable passphrases) to login / use devices.
- Backdoor-free soft- and hardware (Free / Open Source Software + Open Hardware with audits on every release).

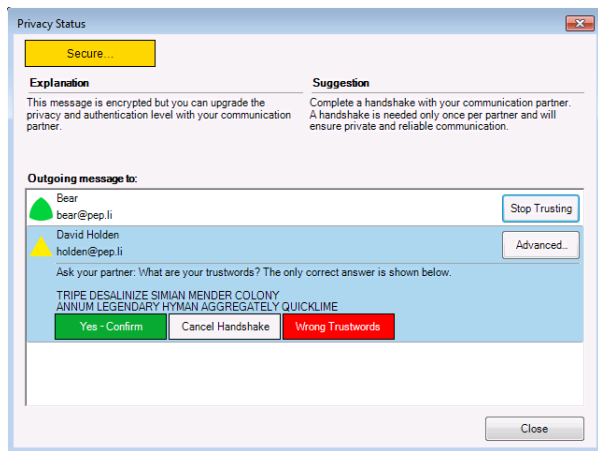
# p≡p for Outlook: First email (unsecure)



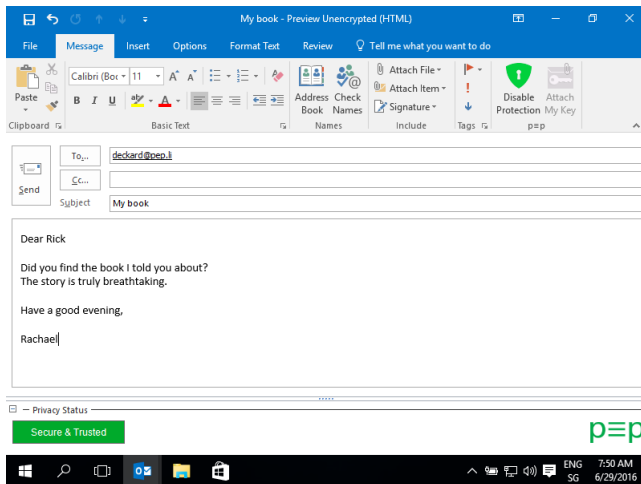
# p≡p for Outlook: second email (secure)



# $p \equiv p$ for Outlook: Handshaking process



# p≡p for Outlook: third email (secure & trusted)





# Rants & Questions :)

