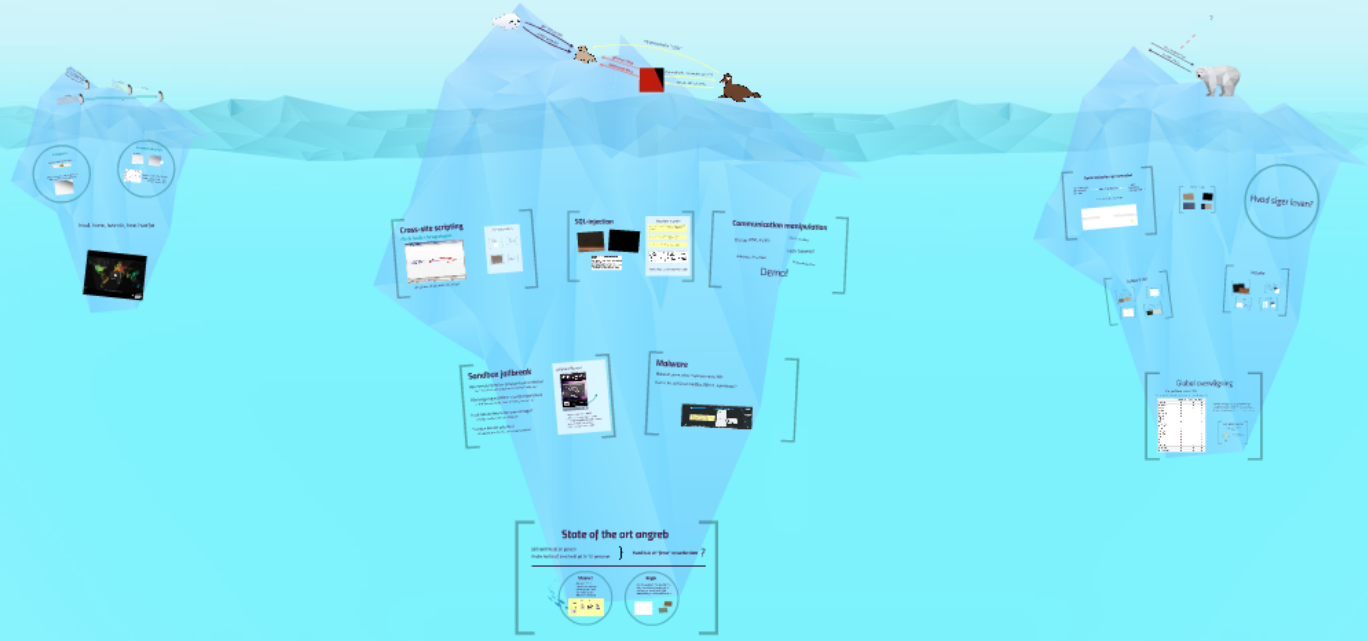
# Angreb / overvågning

Michael Nørkjær

Information

Angreb

Overvågning

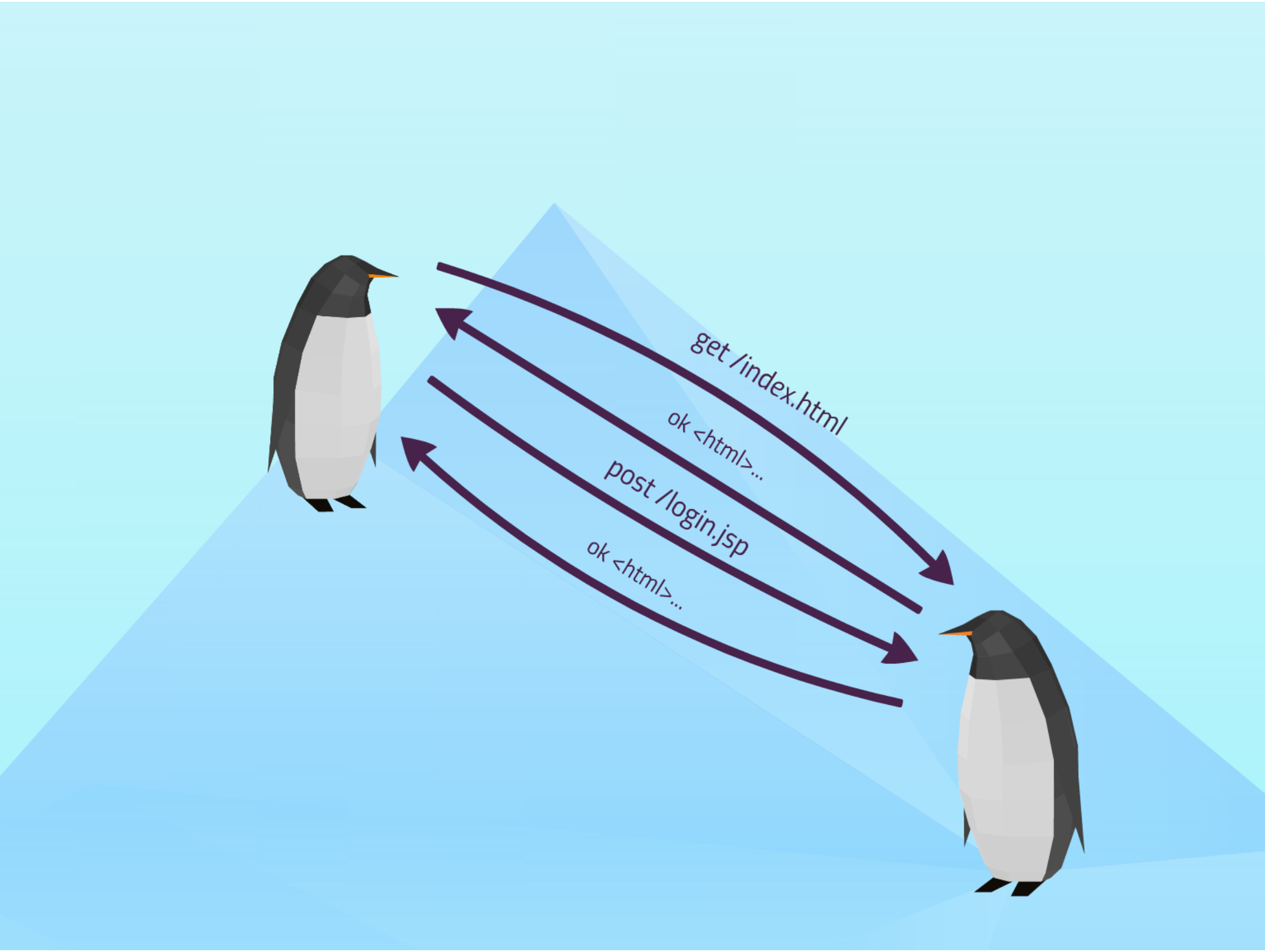


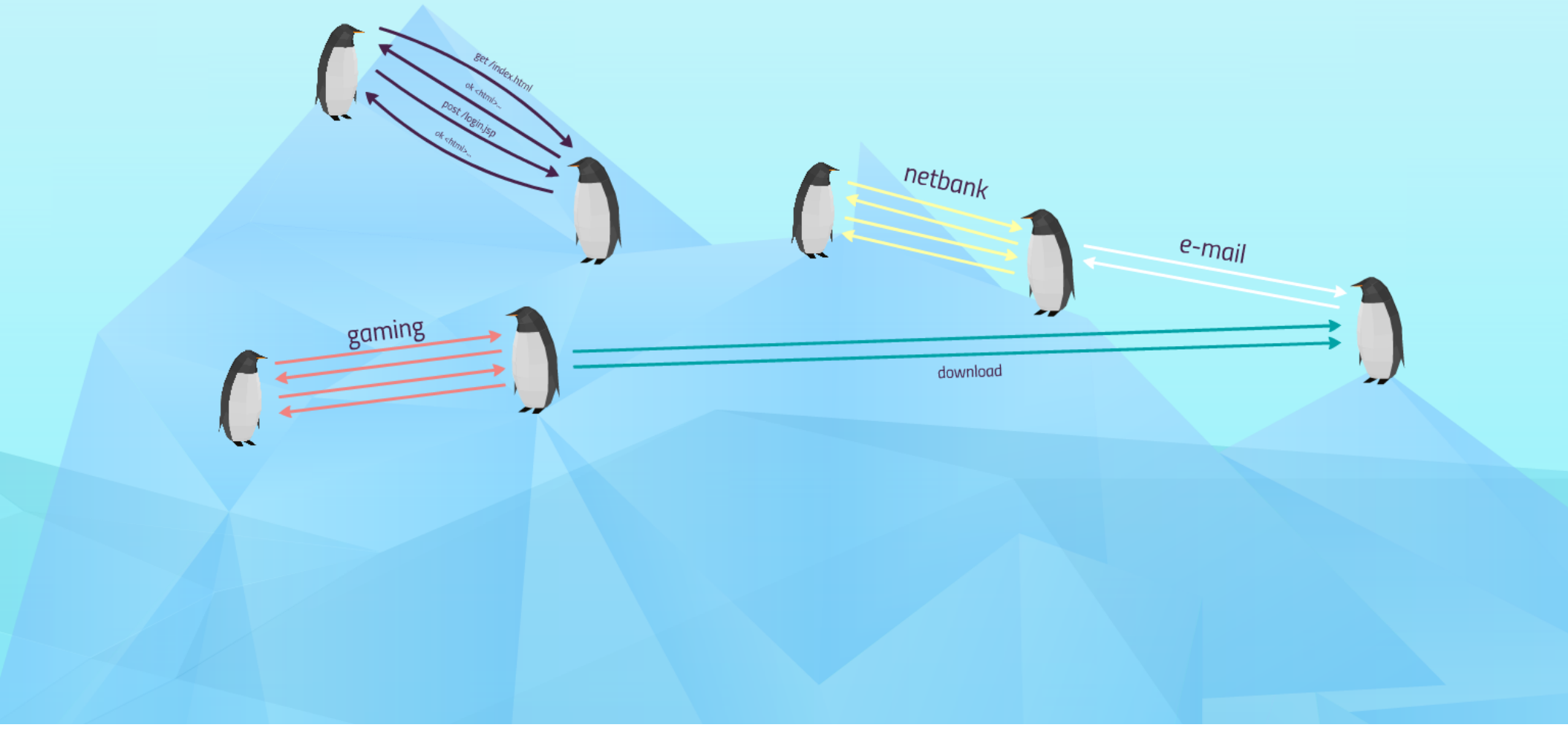
# Angreb / overvågning

Michael Nielsen

… husk ansvarlighed …

# Information


get /index.html
ok <html>...
post /login.jsp
ok <html>...


get /index.html
ok <html>...
post /login.jsp
ok <html>...
netbank
e-mail
gaming
download

# Computer

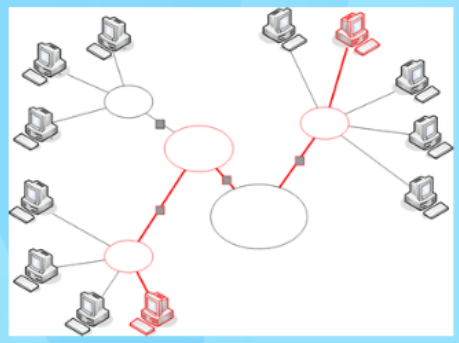
Modelleres af fx Turing Maskine


Samme udtrykskraft som hvad du kan udføre logisk med papir og blyant!

# Kommunikation

Beregninger

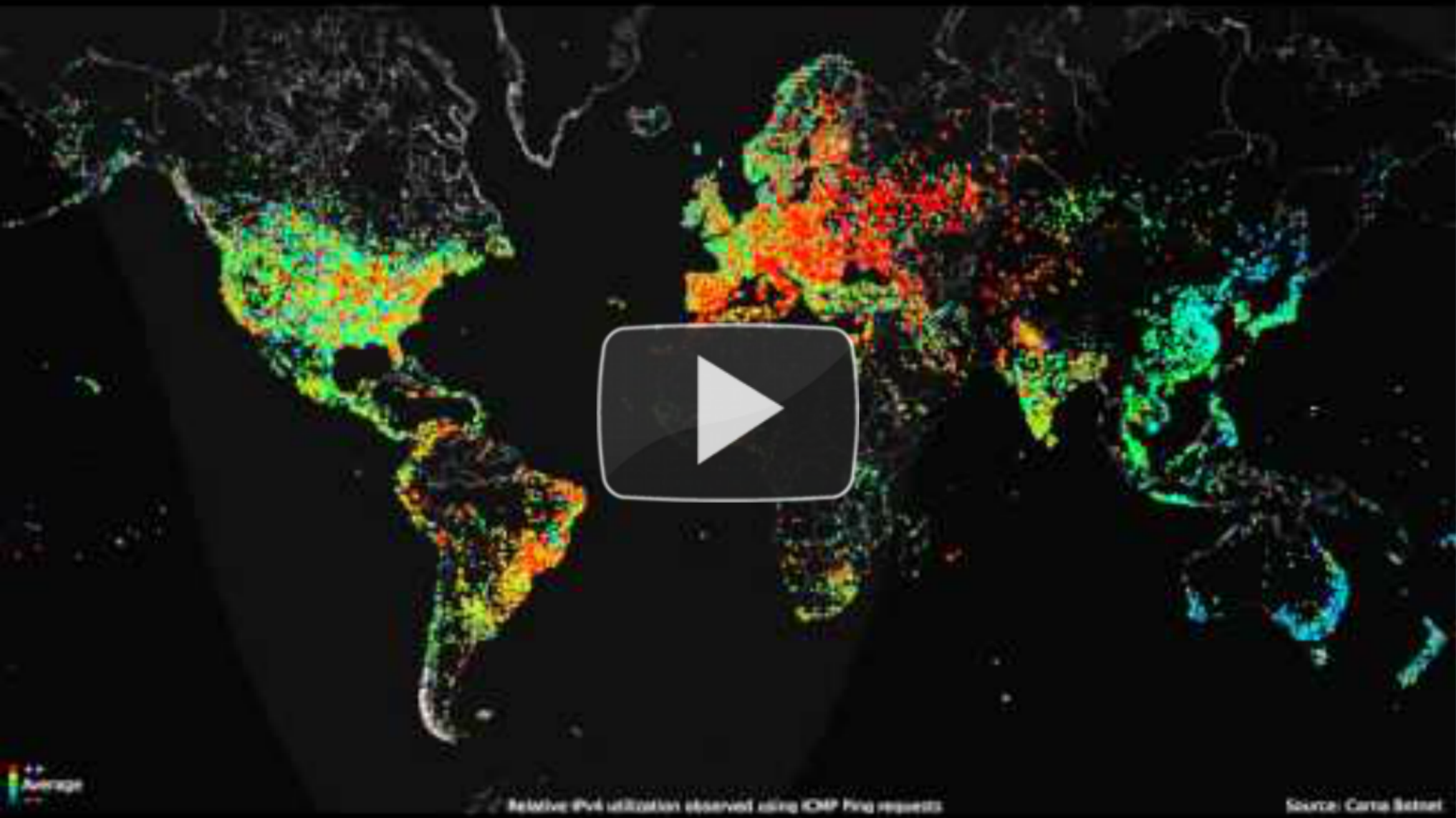
Kommunikation

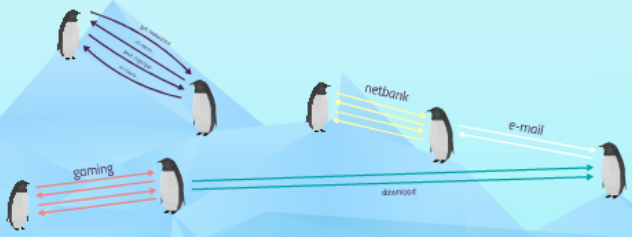


**Ideelt:** snak med vilkårlig anden

**Reelt:** send besked vh.a. hop gennem mellemmænd

hvad, hvem, hvornår, hvor, hvorfor


Average
Relative IPv4 utilization observed using ICMP Ping requests
Source: Carna Botnet




## Computer

Modelleres af fx Turing Maskine

Samme udtrykskraft som hvad du kan udføre logisk med papir og blyant!

## Kommunikation

Beregninger

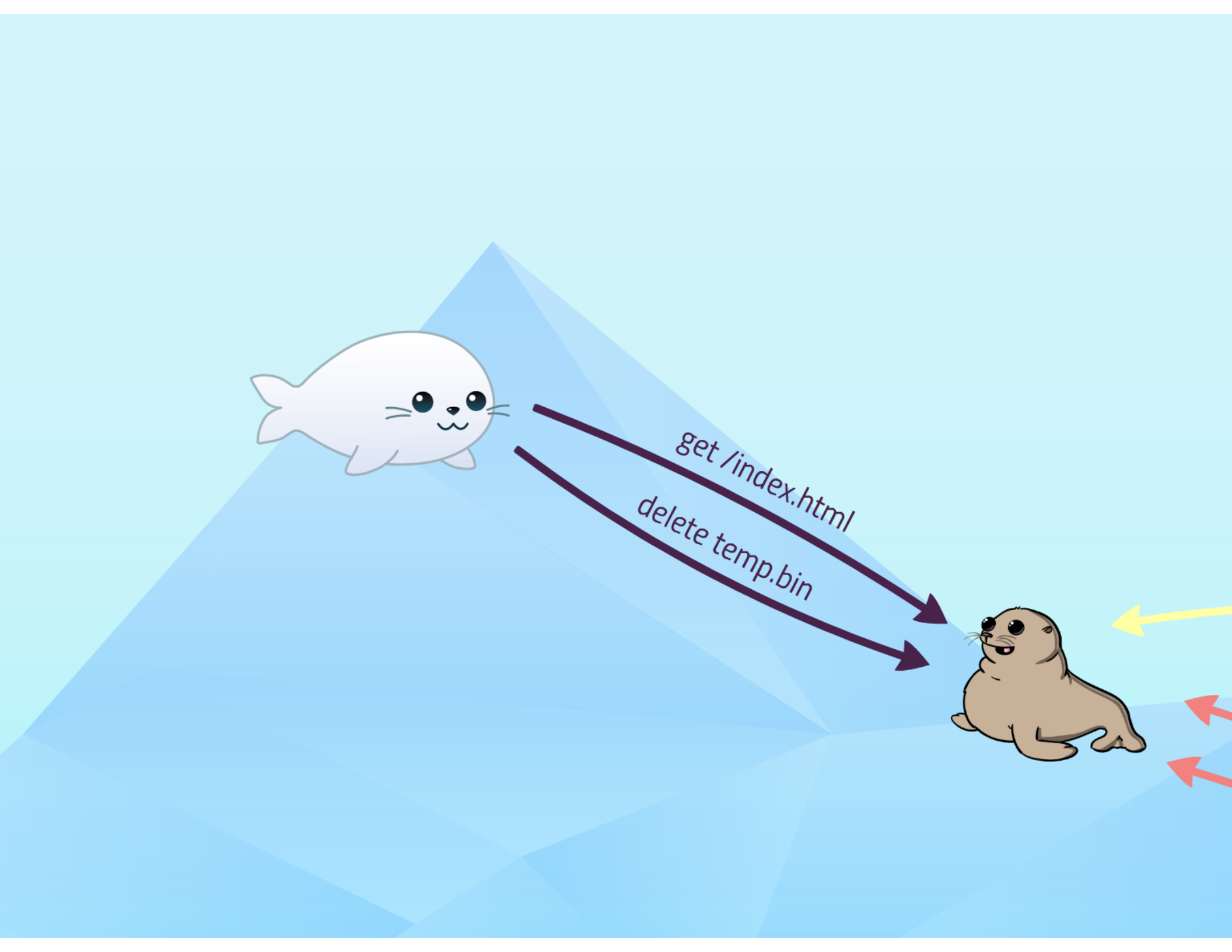
Kommunikation

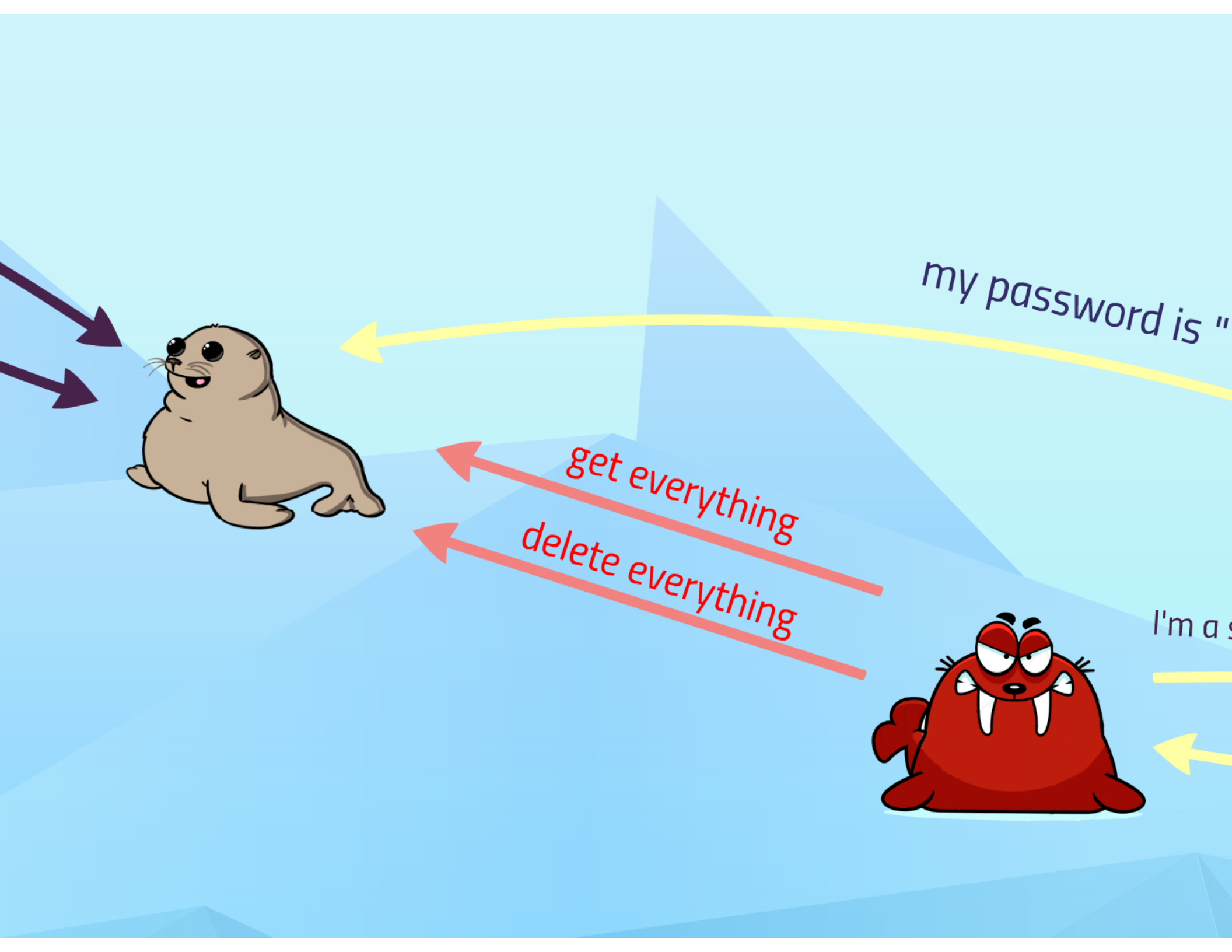
**Ideelt:** snak med vilkårlig anden

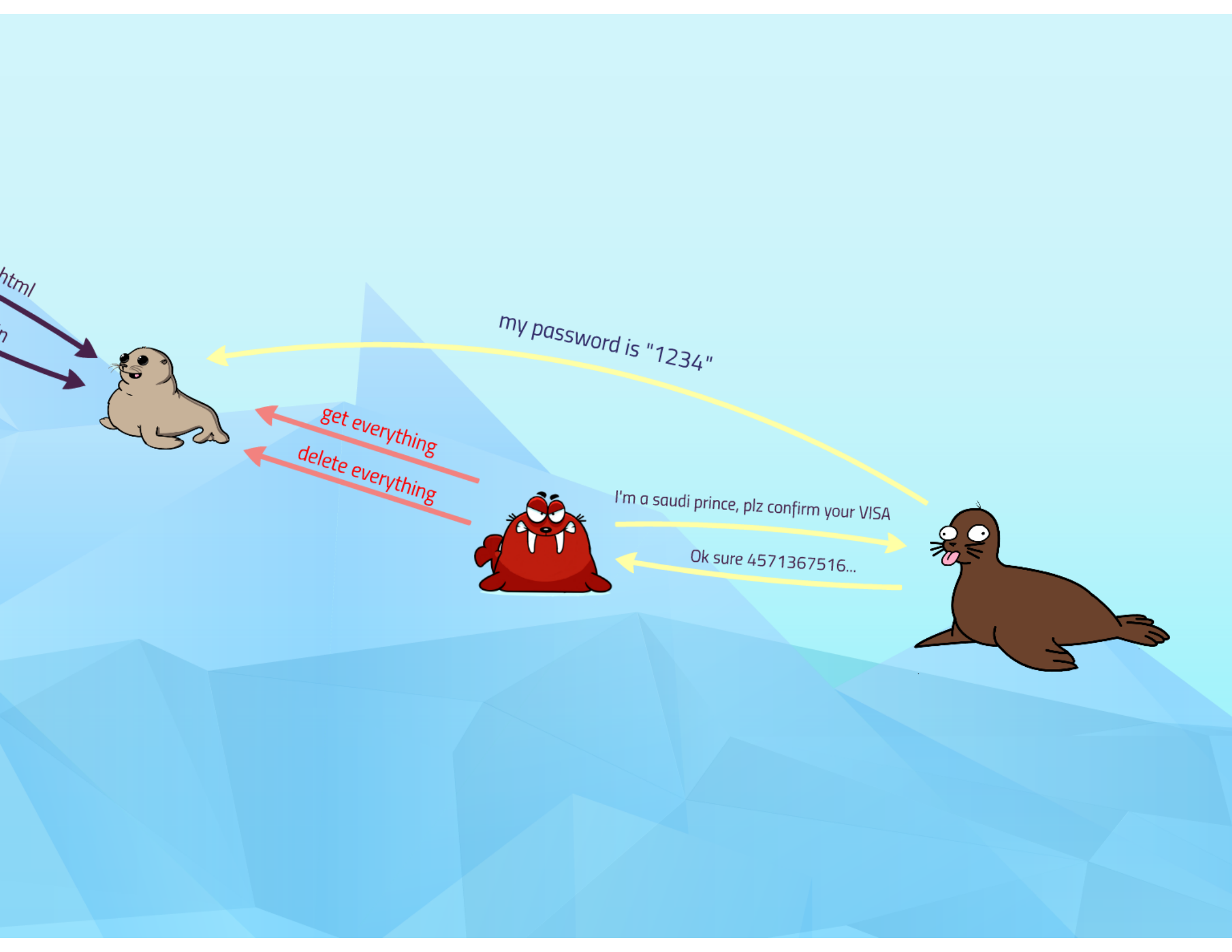
**Reelt:** send besked vh.a. hop gennem mellemmænd

hvad, hvem, hvornår, hvor, hvorfor

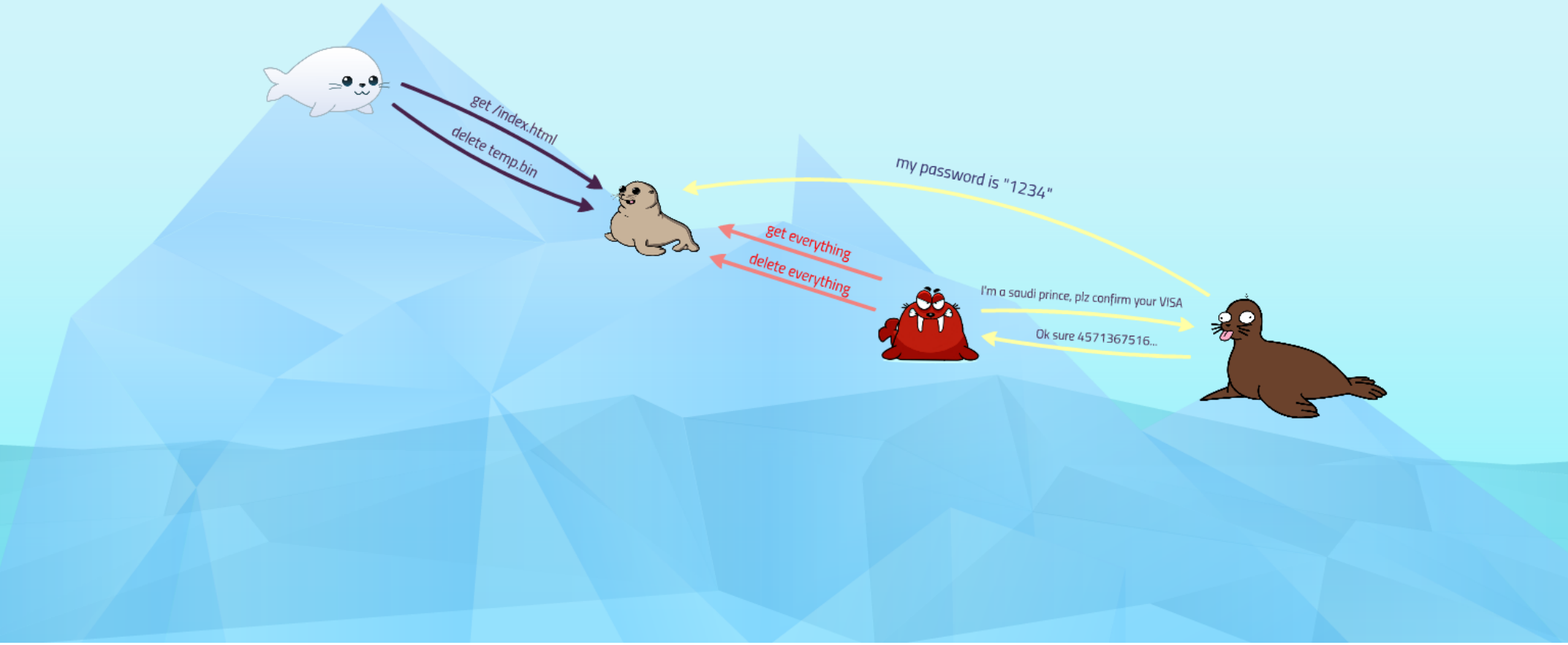
Angreb


get /index.html
delete temp.bin


my password is "
get everything
delete everything
I'm a

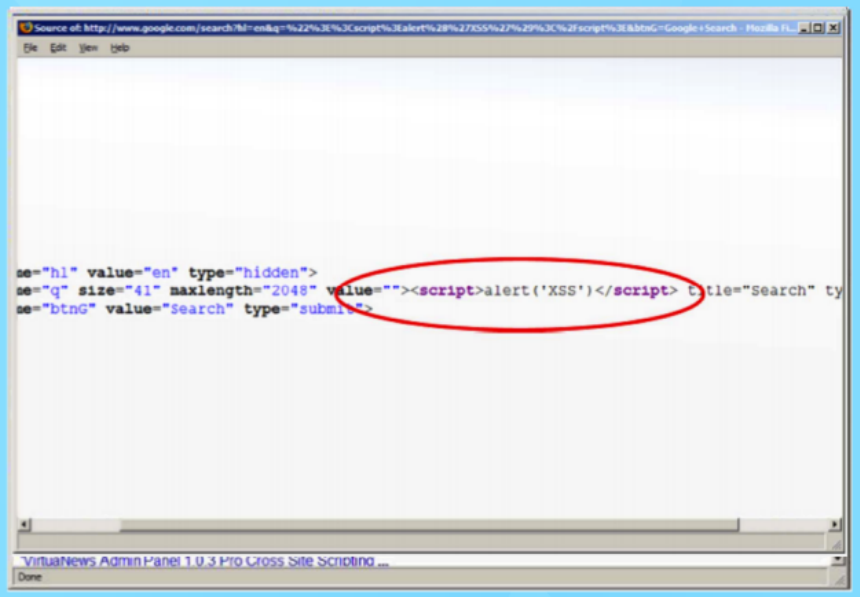

html
n
my password is "1234"
get everything
delete everything
I'm a saudi prince, plz confirm your VISA
Ok sure 4571367516...

# Angreb

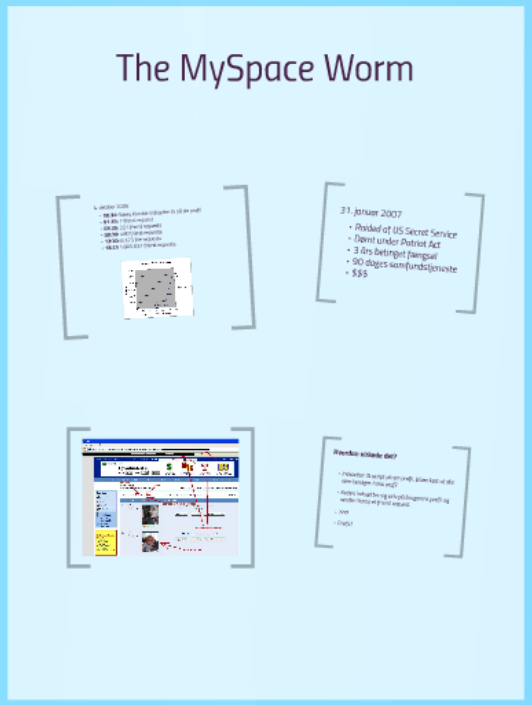

get /index.html
delete temp.bin
my password is "1234"
get everything
delete everything
I'm a saudi prince, plz confirm your VISA
Ok sure 4571367516...

# Cross-site scripting

## Skriv kode i brugerinput

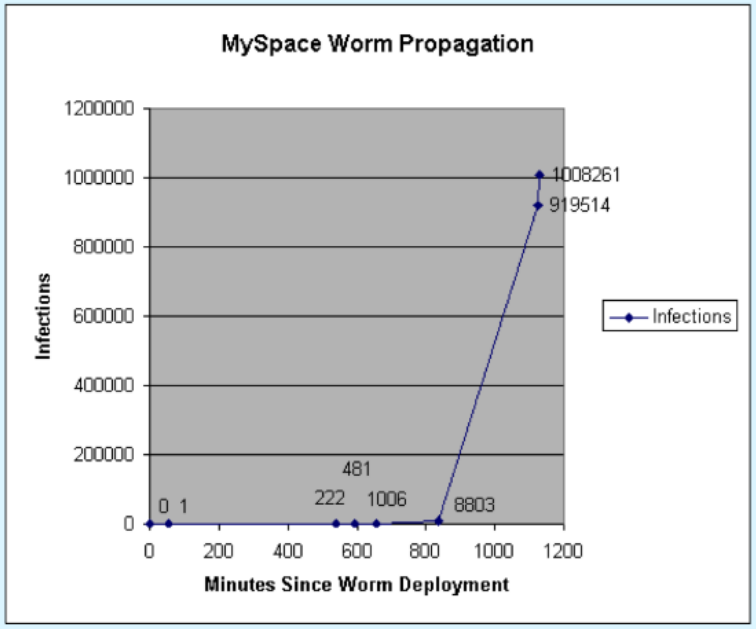



Undgå ved at tjekke well-formed input!



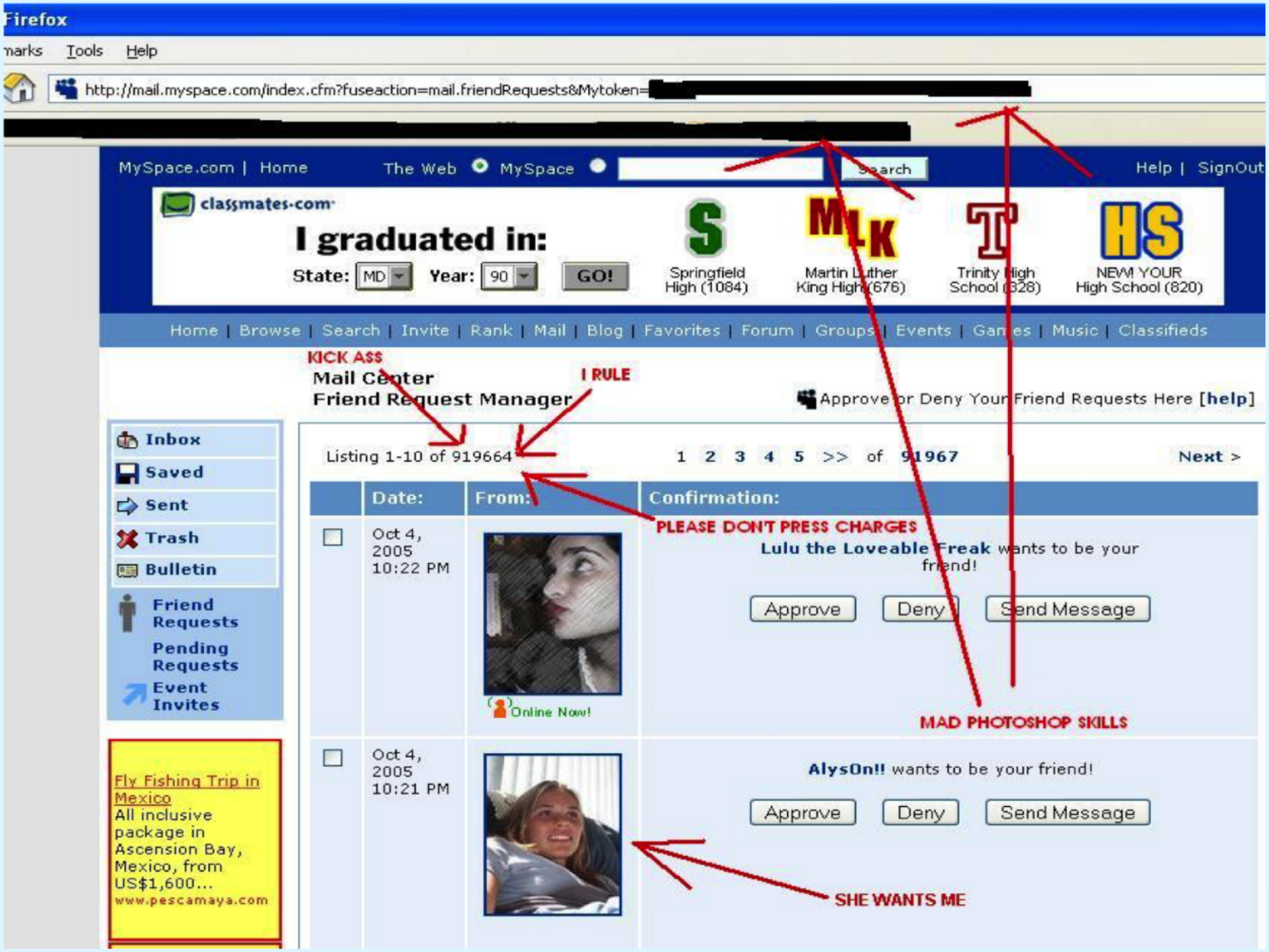
4. oktober 2005

- **00.34:** Samy Kamkar indsætter JS på sin profil
- **01.30:** 1 friend request
- **08.35:** 221 friend requests
- **09:30:** 480 friend requests
- **13:30:** 6.373 frie requests
- **18:25** 1.005.831 friend requests



31. januar 2007

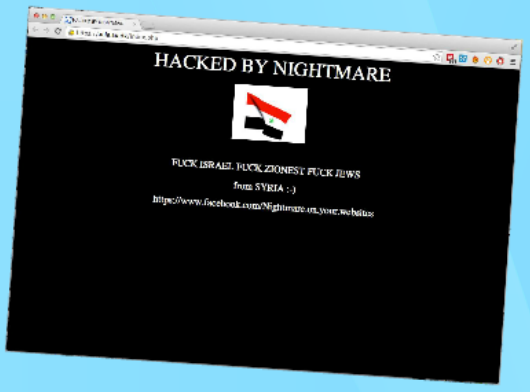
- Raided af US Secret Service
- Dømt under Patriot Act
- 3 års betinget fængsel
- 90 dages samfundstjeneste
- $$$


Firefox
marks Tools Help
http://mail.myspace.com/index.cfm?fuseaction=mail.friendRequests&Mytoken=[redacted]
MySpace.com | Home
The Web
MySpace
Search
Help | SignOut
classmates.com
I graduated in:
State: MD
Year: 90
GO!
Springfield High (1084)
Martin Luther King High (676)
Trinity High School (328)
NEW! YOUR High School (820)
Home | Browse | Search | Invite | Rank | Mail | Blog | Favorites | Forum | Groups | Events | Games | Music | Classifieds
KICK ASS
Mail Center
Friend Request Manager
I RULE
Approve or Deny Your Friend Requests Here [help]
Inbox
Saved
Sent
Trash
Bulletin
Friend Requests
Pending Requests
Event Invites
Listing 1-10 of 919664
1 2 3 4 5 >> of 91967
Next >
Date:
From:
Confirmation:
PLEASE DON'T PRESS CHARGES
Oct 4, 2005 10:22 PM
Online Now!
Lulu the Loveable Freak wants to be your friend!
Approve
Deny
Send Message
MAD PHOTOSHOP SKILLS
Oct 4, 2005 10:21 PM
AlysOn!! wants to be your friend!
Approve
Deny
Send Message
SHE WANTS ME
Fly Fishing Trip in Mexico
All inclusive package in Ascension Bay, Mexico, from US$1,600...
www.pescamaya.com

# Hvordan virkede det?

- Indsætter JS script på sin profil, bliver kørt af alle som besøger hans profil
- Koden indsætter sig selv på brugerens profil og sender Samy et friend request
- ????
- Profit!

# SQL-injection


## Mistænkt CSC-hacker idømt to års fængsel i Sverige

Gottfrid Svartholm Warg er blevet idømt to års fængsel for sammen med en bekendt at have hacket sig ind i blandt andet Nordeas systemer på en mainframe hos it-leverandøren Logica.

*Af Jesper Stein Sandal* Følg @jespersandal *Torsdag, 20. juni 2013 - 12:00*

Pirate Bay-medstifter Gottfrid Svartholm Warg er blevet idømt to års fængsel for hacking ved en domstol i Sverige. Det oplyser de svenske domstole ifølge en pressemeddelelse.

Gottfrid Svartholm Warg er også én af de hovedmistænkte i sagen om hackingen af en mainframe hos CSC i Danmark, hvor hackere fik adgang til blandt andet politiets kørekortsregister.

## How does it work?

```
sql = "SELECT * FROM users WHERE username = ' "+param.user+" ' AND
                                 password = ' "+param.pass+" '
execute(sql);
...
```

```
sql = "SELECT * FROM users WHERE username = ' mik ' AND
                                 password = ' 1234 '
```

```
sql = "SELECT * FROM users WHERE username = ' mik ' AND
                                 (password = ' ' OR '1'='1')
```


## How to avoid? Do now allow raw input!

UNITED NATIONS

# Secretary-General Ban Ki-moon


- Home
- Secretary-General Ban Ki-moon
- Biography
- On the job
- Daily schedule
- All statements
- Major speeches
- "Off the Cuff" Remarks
- Reports/articles
- Ethical standards
- Travel
- The Team
- Deputy Secretary -General
- Management group
- Representatives & envoys


Secretary General Ban Ki-Moon speaks on the stage of the Herbst Theater, San Francisco, where the Charter of the United Nations was signed on 26 June 1945. William Luers, President of the UNA-USA stands in background - 26 July 2007.

"I feel honoured and very humbled when I think of all our founding fathers wise enough and courageous enough to save this world from the scourge of war who have negotiated, drafted and finally signed the Charter of the United Nations, which has shaped the future of the whole international community."

Secretary-General Ban Ki-moon in remarks at San Francisco War Memorial, 26 July 2007

## LATEST HEADLINES

### Ban Ki-moon hails Security Council resolution on strengthened UN role in Iraq

*10 August 2007* – Secretary-General Ban Ki-moon said today that a new Security Council resolution on

## Latest speeches

- HACKED BY KEREM125 M0STED AND GSY THAT IS CYBERPROTEST HEY ÝSRAIL AND USA DONT KILL CHILDREN AND OTHER PEOPLE PEACE FOR EVER NO WAR
- HACKED BY KEREM125 M0STED AND GSY THAT IS CYBERPROTEST HEY ÝSRAIL AND USA DONT KILL CHILDREN AND OTHER PEOPLE PEACE FOR EVER NO WAR

HACKED BY NIGHTMARE

https://aula.au.dk/index.php

# HACKED BY NIGHTMARE

FUCK ISRAEL FUCK ZIONEST FUCK JEWS

from SYRIA :-)

https://www.facebook.com/Nightmare.on.your.websites

# Mistænkt CSC-hacker idømt to års fængsel i Sverige

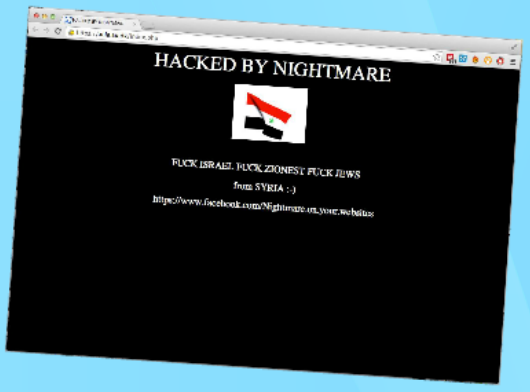
Gottfrid Svartholm Warg er blevet idømt to års fængsel for sammen med en bekendt at have hacket sig ind i blandt andet Nordeas systemer på en mainframe hos it-leverandøren Logica.

*Af Jesper Stein Sandal* Følg @jespersandal *Torsdag, 20. juni 2013 - 12:00*

Pirate Bay-medstifter Gottfrid Svartholm Warg er blevet idømt to års fængsel for hacking ved en domstol i Sverige. Det oplyser de svenske domstole ifølge en pressemeddelelse.

Gottfrid Svartholm Warg er også én af de hovedmistænkte i sagen om hackingen af en mainframe hos CSC i Danmark, hvor hackere fik adgang til blandt andet politiets kørekortsregister.

# SQL-injection


## Mistænkt CSC-hacker idømt to års fængsel i Sverige

Gottfrid Svartholm Warg er blevet idømt to års fængsel for sammen med en bekendt at have hacket sig ind i blandt andet Nordeas systemer på en mainframe hos it-leverandøren Logica.

*Af Jesper Stein Sandal* Følg @jespersandal *Torsdag, 20. juni 2013 - 12:00*

Pirate Bay-medstifter Gottfrid Svartholm Warg er blevet idømt to års fængsel for hacking ved en domstol i Sverige. Det oplyser de svenske domstole ifølge en pressemeddelelse.

Gottfrid Svartholm Warg er også én af de hovedmistænkte i sagen om hackingen af en mainframe hos CSC i Danmark, hvor hackere fik adgang til blandt andet politiets kørekortsregister.

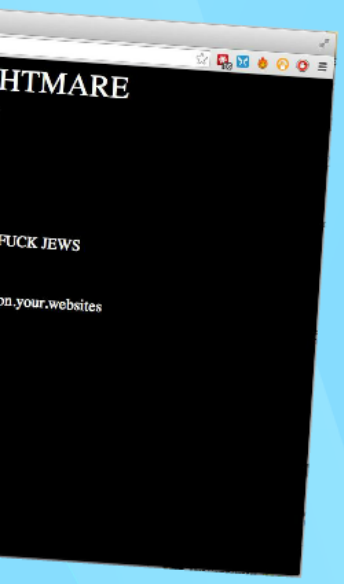
## How does it work?

```
sql = "SELECT * FROM users WHERE username = ' "+param.user+" ' AND
                                 password = ' "+param.pass+" '
execute(sql);
...
```

```
sql = "SELECT * FROM users WHERE username = ' mik ' AND
                                 password = ' 1234 '
```

```
sql = "SELECT * FROM users WHERE username = ' mik ' AND
                                 (password = ' ' OR '1'='1')
```


## How to avoid? Do now allow raw input!

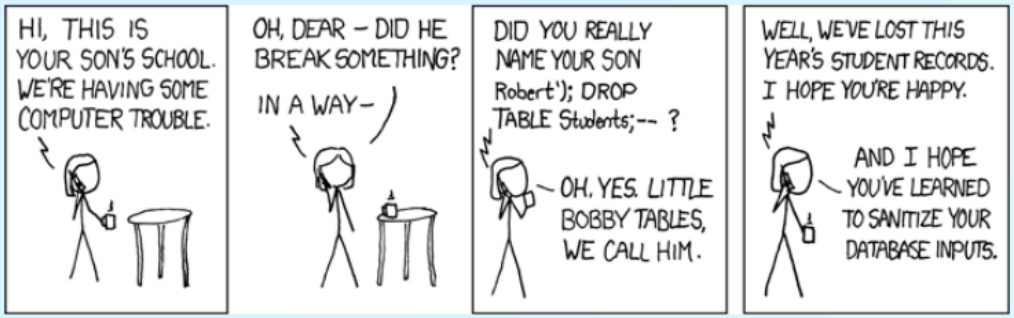



# How does it work?

```
sql = "SELECT * FROM users WHERE username = ' "+param.user+" ' AND
                                 password = ' "+param.pass+" '
execute(sql);
...
```

```
sql = "SELECT * FROM users WHERE username = ' mik ' AND
                                 password = ' 1234 '
```

```
sql = "SELECT * FROM users WHERE username = ' mik ' AND
                                 (password = ' ' OR '1'='1')
```




## How to avoid? Do now allow raw input!

# Communication manipulation

Change HTML-inputs

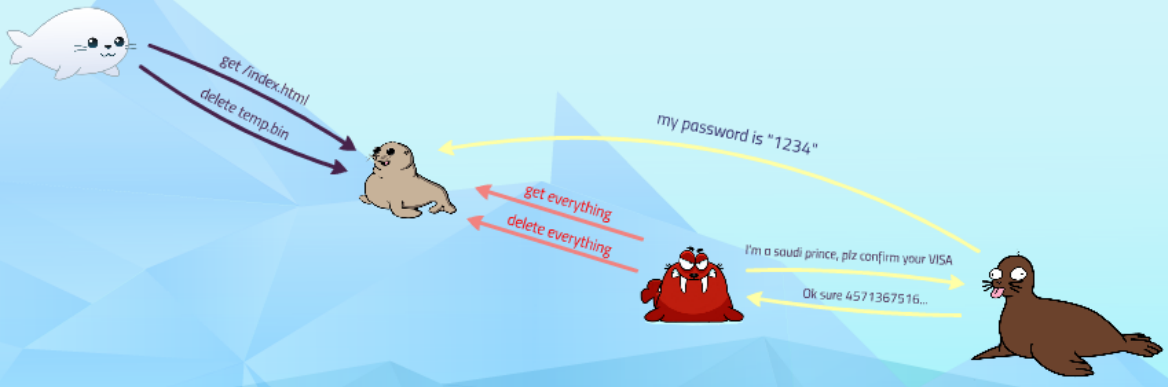
Cookie-stealing

Path traversal

Malicious file-upload

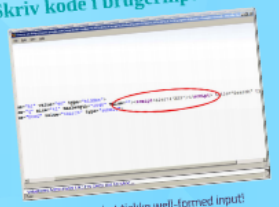
Protocol injection

Demo!



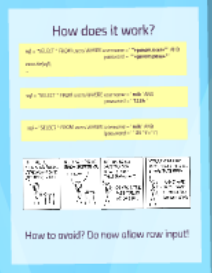

## Cross-site scripting

Skriv kode i brugerinput



Undgå ved at tjekke well-formed input!


## SQL-injection




## Communication manipulation

Change HTML-inputs

Cookie-stealing

Path traversal

Malicious file-upload

Protocol injection

Demo!

# Sandbox jailbreak

## Hjemmesider fortolker browser-kommunikation

I har selv skrevet Tomcat-kode, måske lavet en "nåå ja ups"

## Ofte bruger og installerer vi programfortolkere

i.e. PDF, Java, JavaScript, Flash, Silverlight, browser, spil

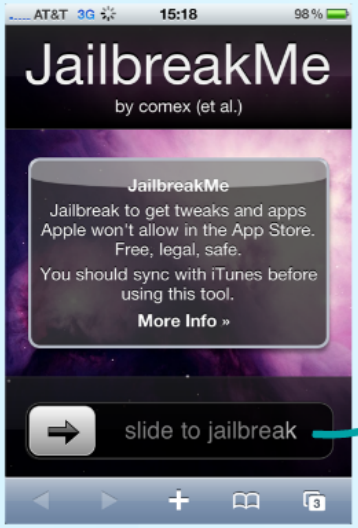
## Hvad hvis udviklerne har overset noget?

Fx buffer-overflow eller bare dårlig kode

## Hvordan kan det udnyttes?

Kør eget program direkte, som hvis kørt af **admin**!

## JailbreakMe.com

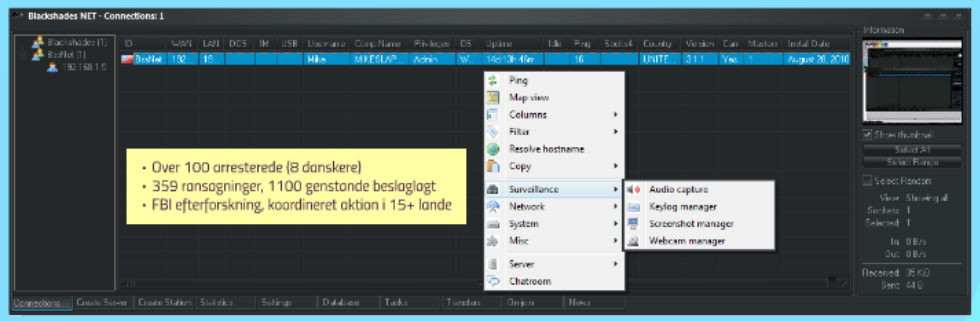


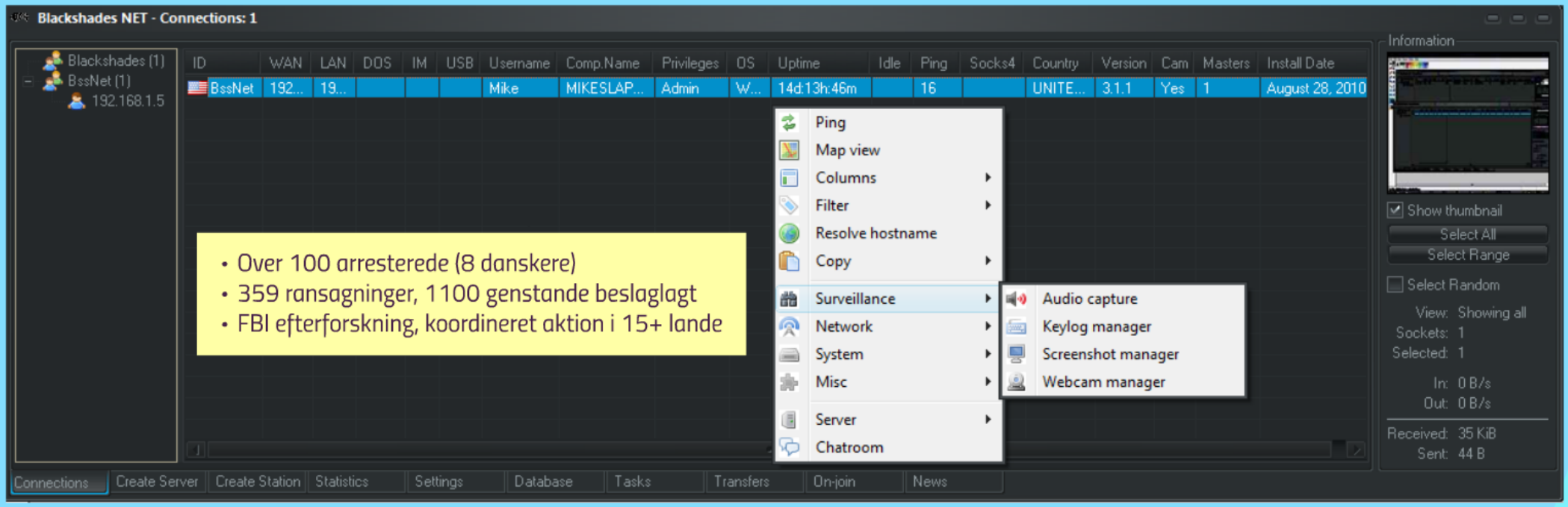

- Brugeren sendes til en .pdf-fil
- PDF-fil indeholder custom skrifttype
- Skrifttype er ugyldig, laver buffer-overflow
- Jailbreak-app (Cydia) installeres
- Retter bug i Safari, nu vi er igang

# Malware

Malware, orme, virus, trojanske heste, RAT

Poison Ivy, SubSeven, NetBus, Bifrost, TeamViewer?






- Over 100 arresterede (8 danskere)
- 359 ransagninger, 1100 genstande beslaglagt
- FBI efterforskning, koordineret aktion i 15+ lande

# State of the art angreb

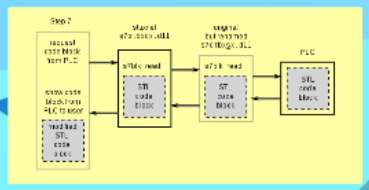
JailbreakMe af en person

Andre hacks af små hold på 5-10 personer

} Hvad hvis et "firma" ansætter 600 ?

## Stuxnet

- Opdaget i 2010
- Specialiseret malware
- Spredt af spion (USB)
- 4 ZeroDay exploits
- Mål: Irans atomkraft

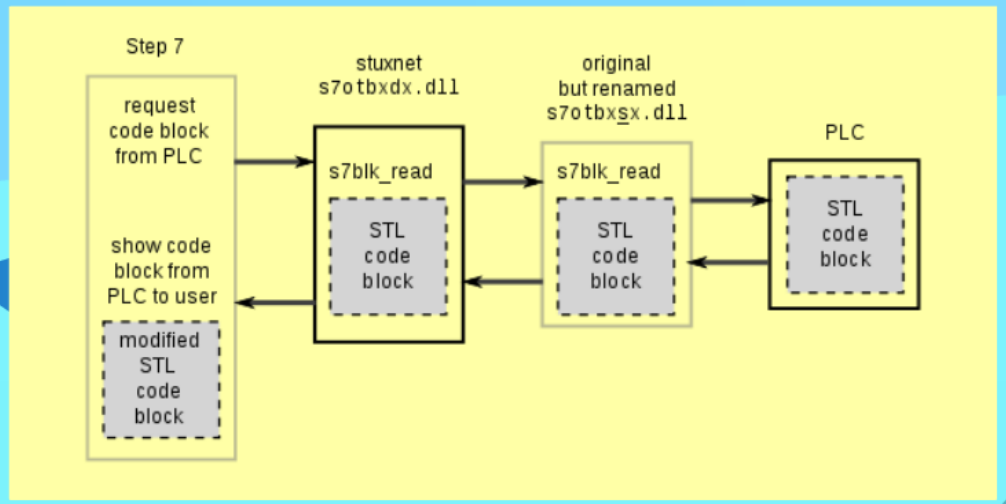


## Regin

- Fra '04, opdaget i '12, offentligt '14
- Meget modulært og kryptografisk
- Der Spiegel: lavet af USA og UK
- Mål: private personer/virksomheder

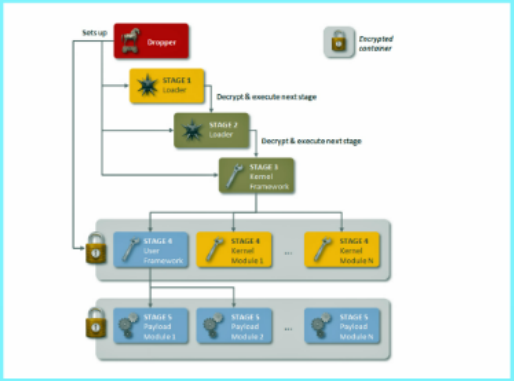
# Stuxnet

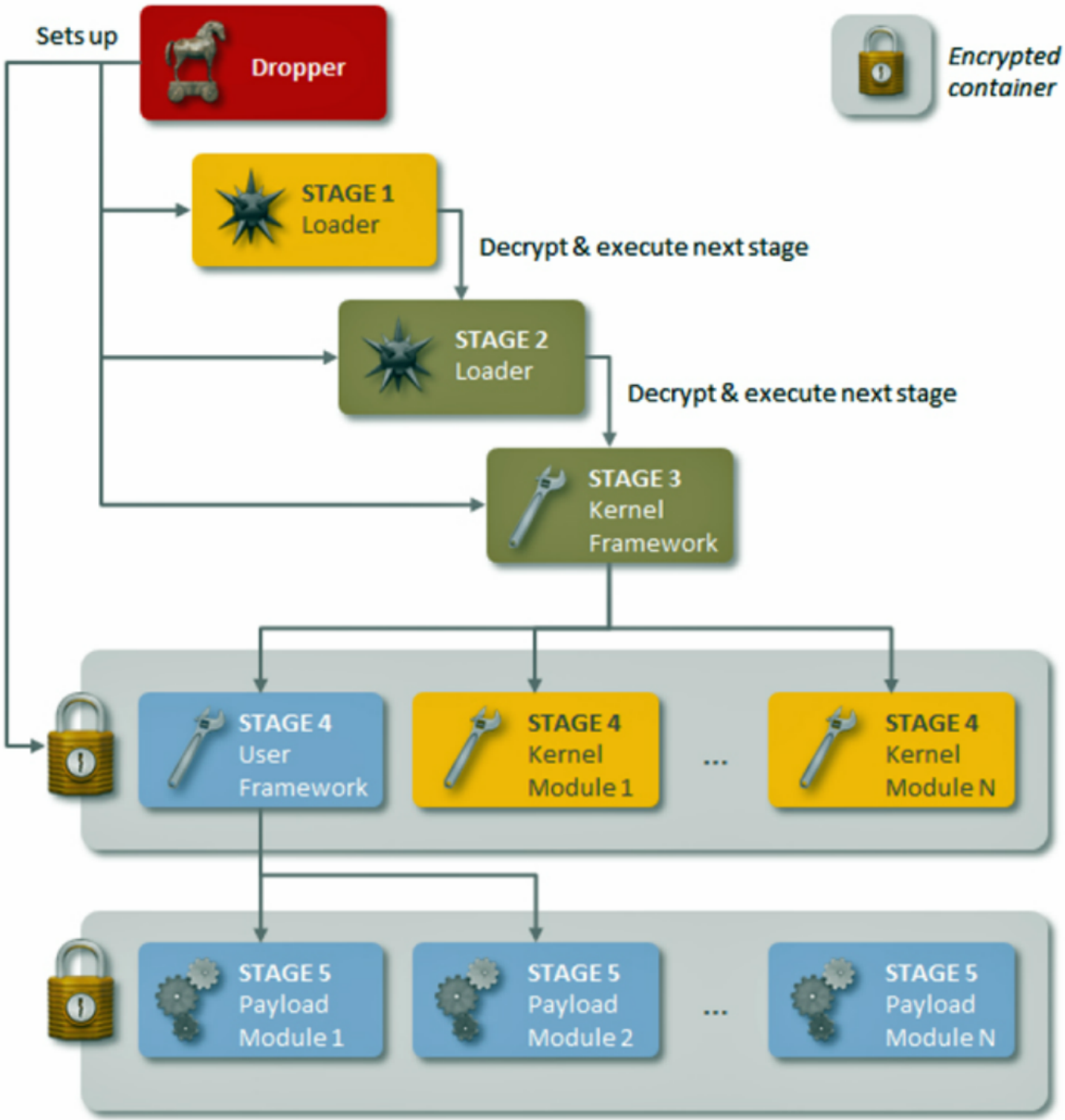
- Opdaget i 2010
- Specialiseret malware
- Spredt af spion (USB)
- 4 ZeroDay exploits
- Mål: Irans atomkraft



# Regin

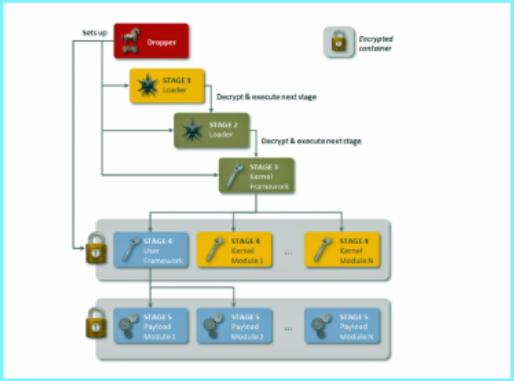
- Fra '04, opdaget i '12, offentligt '14
- Meget modulært og kryptografisk
- Der Spiegel: lavet af USA (NSA) og UK (GCHQ)
- Mål: private personer/virksomheder



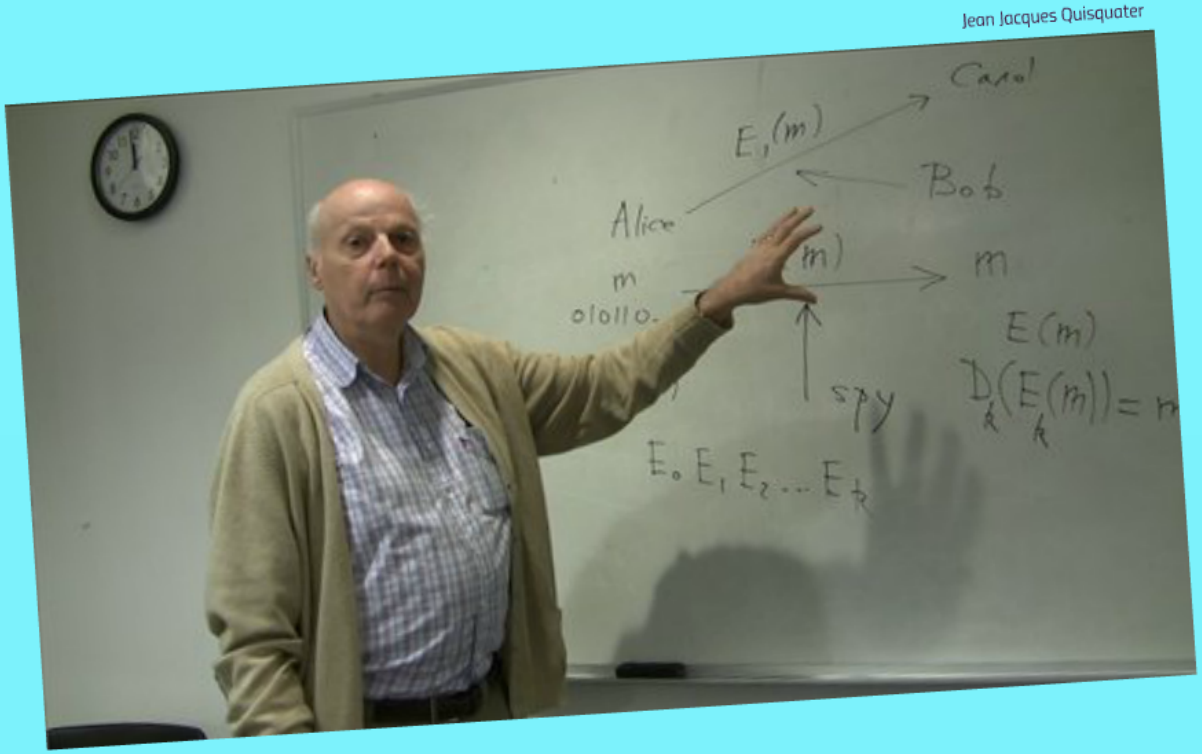


Sets up
Dropper
Encrypted container
STAGE 1
Loader
Decrypt & execute next stage
STAGE 2
Loader
Decrypt & execute next stage
STAGE 3
Kernel
Framework
STAGE 4
User
Framework
STAGE 4
Kernel
Module 1
...
STAGE 4
Kernel
Module N
STAGE 5
Payload
Module 1
STAGE 5
Payload
Module 2
...
STAGE 5
Payload
Module N

# Regin

- Fra '04, opdaget i '12, offentligt '14
- Meget modulært og kryptografisk
- Der Spiegel: lavet af USA (NSA) og UK (GCHQ)
- Mål: private personer/virksomheder




belgacom




Jean Jacques Quisquater

# State of the art angreb

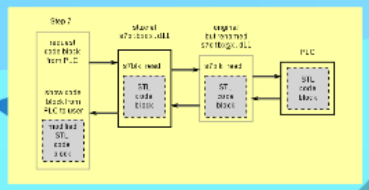
JailbreakMe af en person

Andre hacks af små hold på 5-10 personer

} Hvad hvis et "firma" ansætter 600 ?

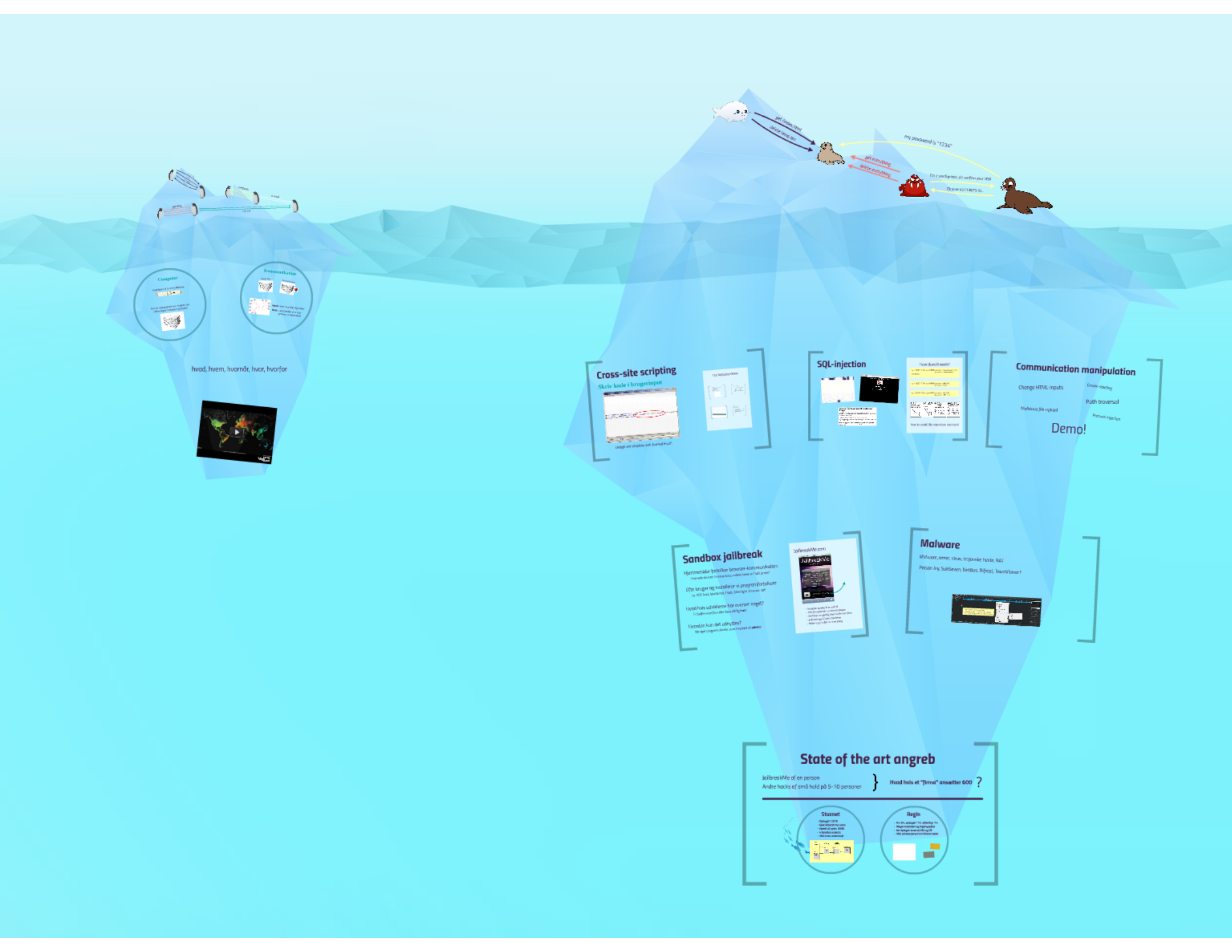
## Stuxnet

- Opdaget i 2010
- Specialiseret malware
- Spredt af spion (USB)
- 4 ZeroDay exploits
- Mål: Irans atomkraft

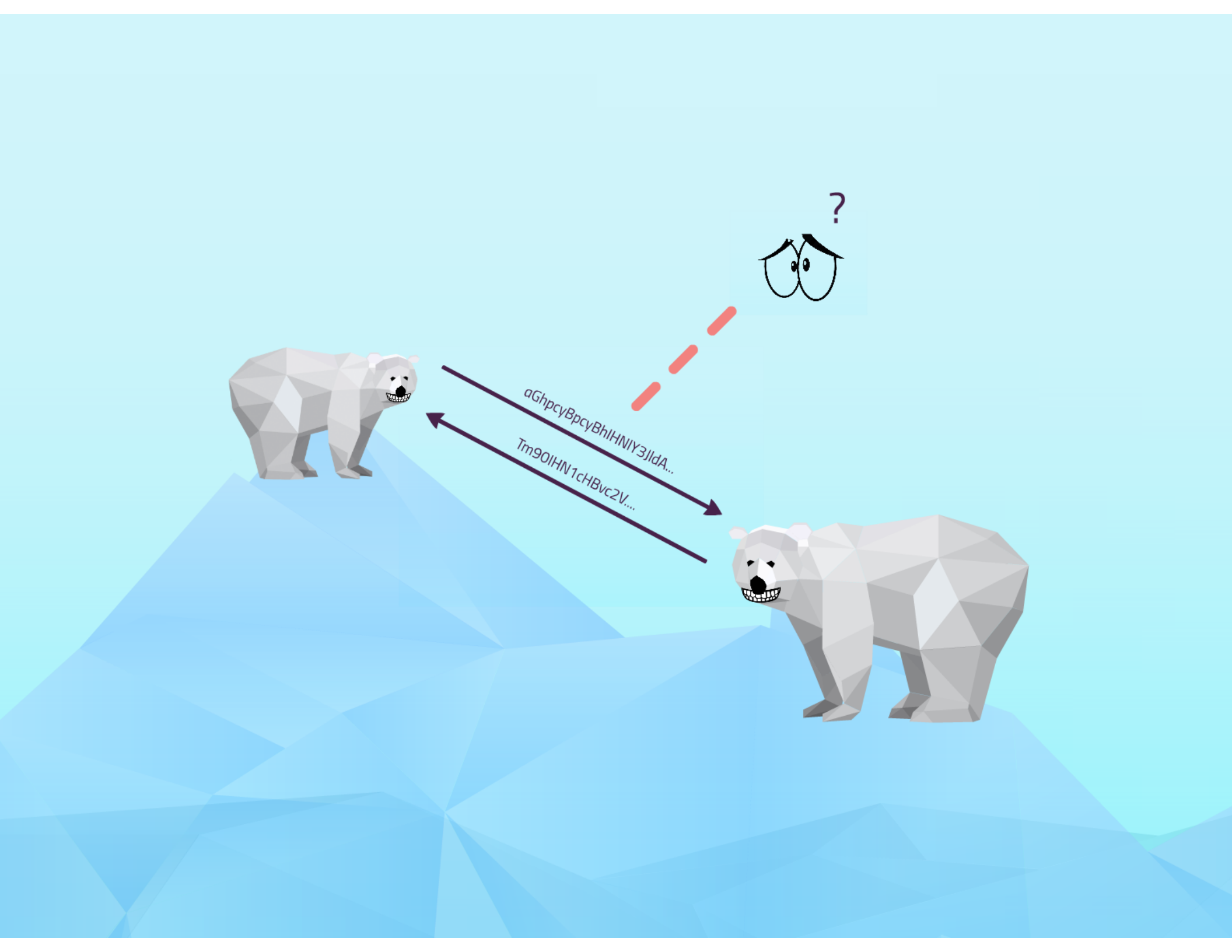


## Regin

- Fra '04, opdaget i '12, offentligt '14
- Meget modulært og kryptografisk
- Der Spiegel: lavet af USA og UK
- Mål: private personer/virksomheder


Cross-site scripting
Skriv kode i brugerinput
SQL-injection
Communication manipulation
Change HTML-inputs
Malicious file upload
Session stealing
Path traversal
Request injection
Demo!
Sandbox jailbreak
Malware
State of the art angreb
Stuxnet
Regin

# Overvågning


?
aGhpcyBpcyBhIHNlY3JldA...
Tm90IHN1cHBvc2V....

# Kommunikation og mennesket

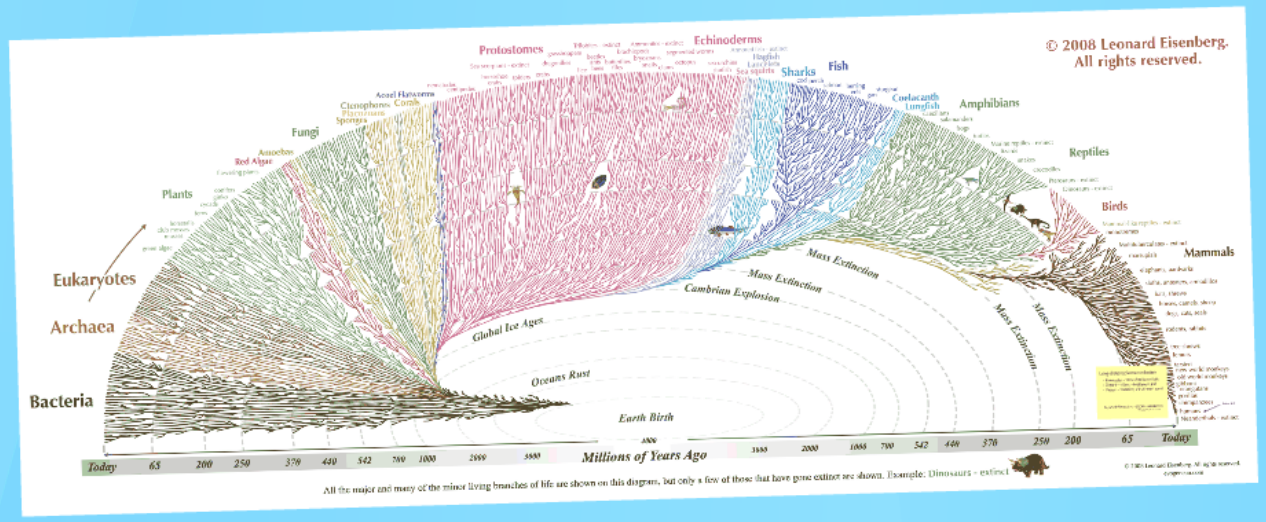
Enkelt forbindelse
Lokalt netværk
Internettet

→ Kommunikation ←

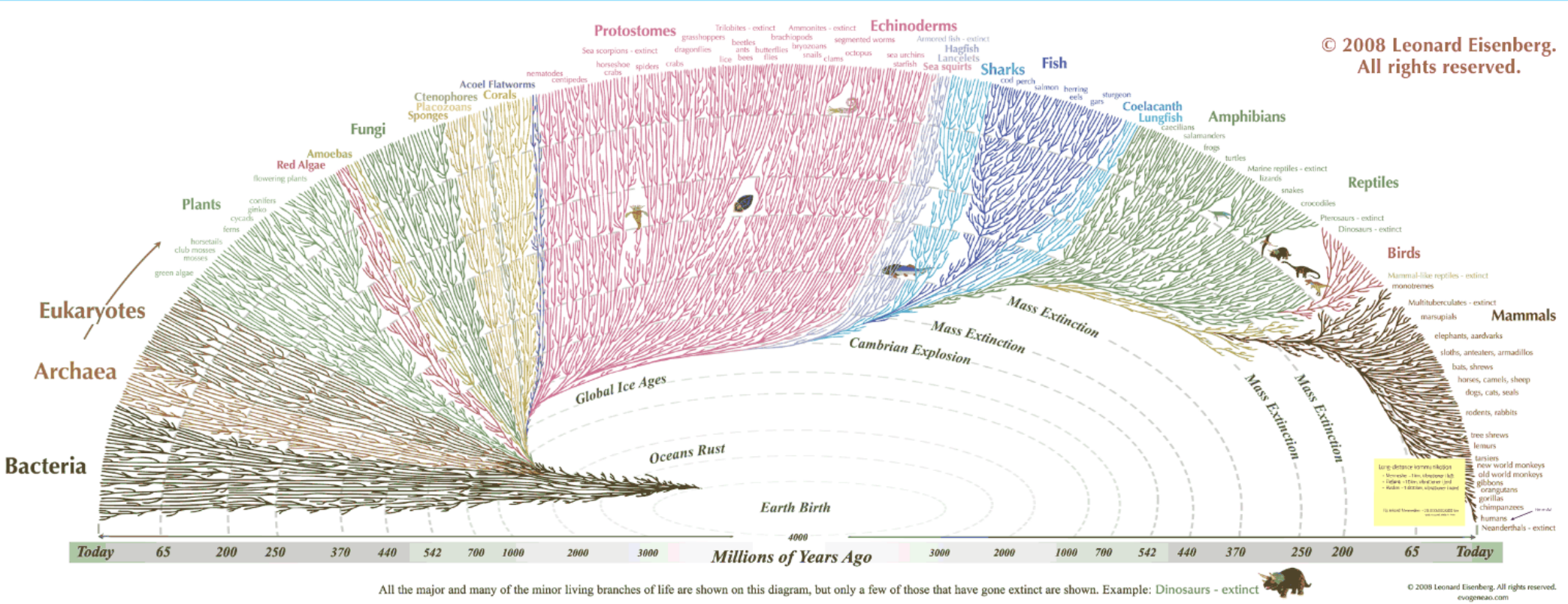
Samtale
Forsamling
Lydbølger / EM / ...

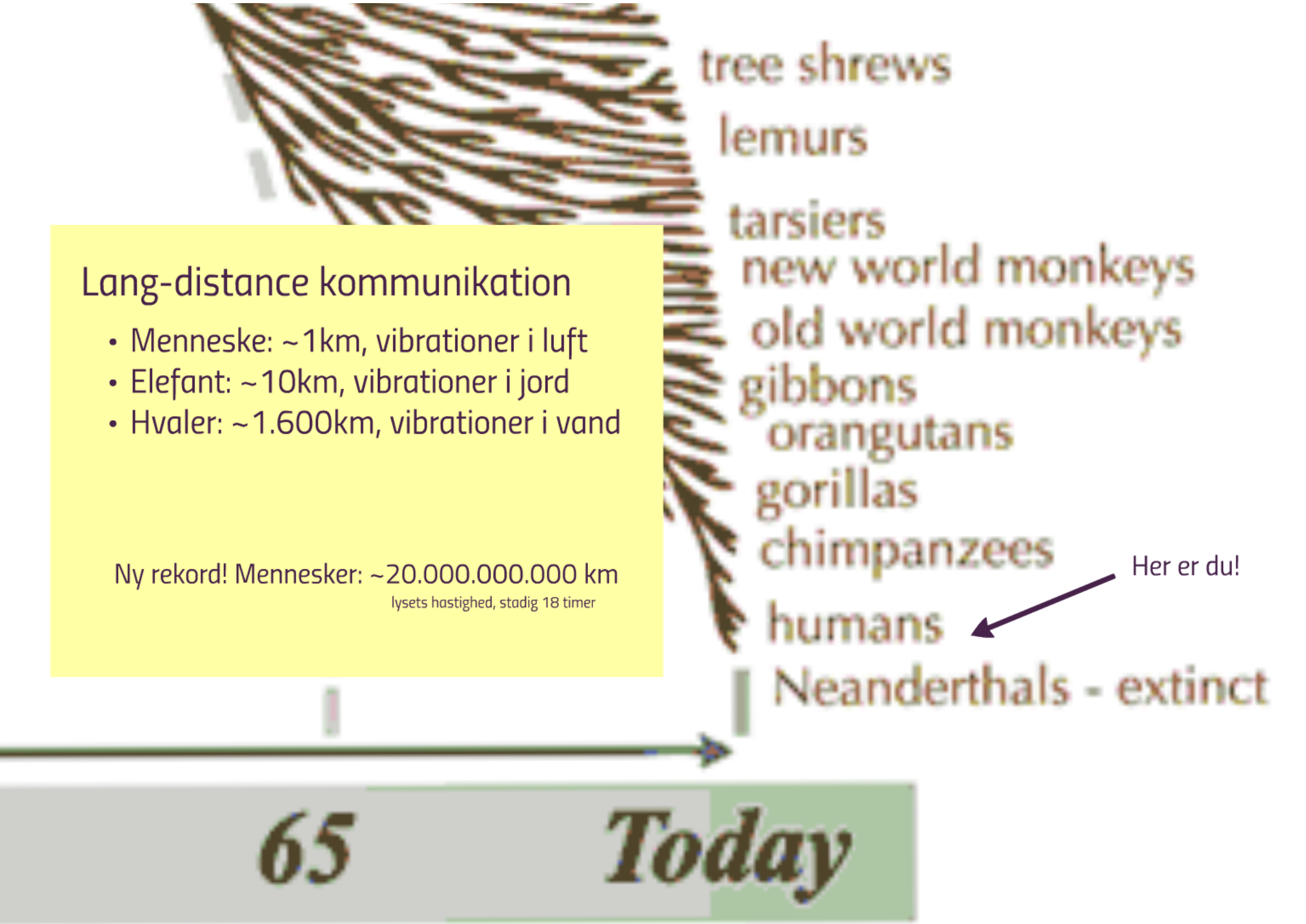
↓

hvad, hvem, hvornår, hvor, hvorfor



# hvad, hvem, hvornår, hvor, hvorfor






## Lang-distance kommunikation

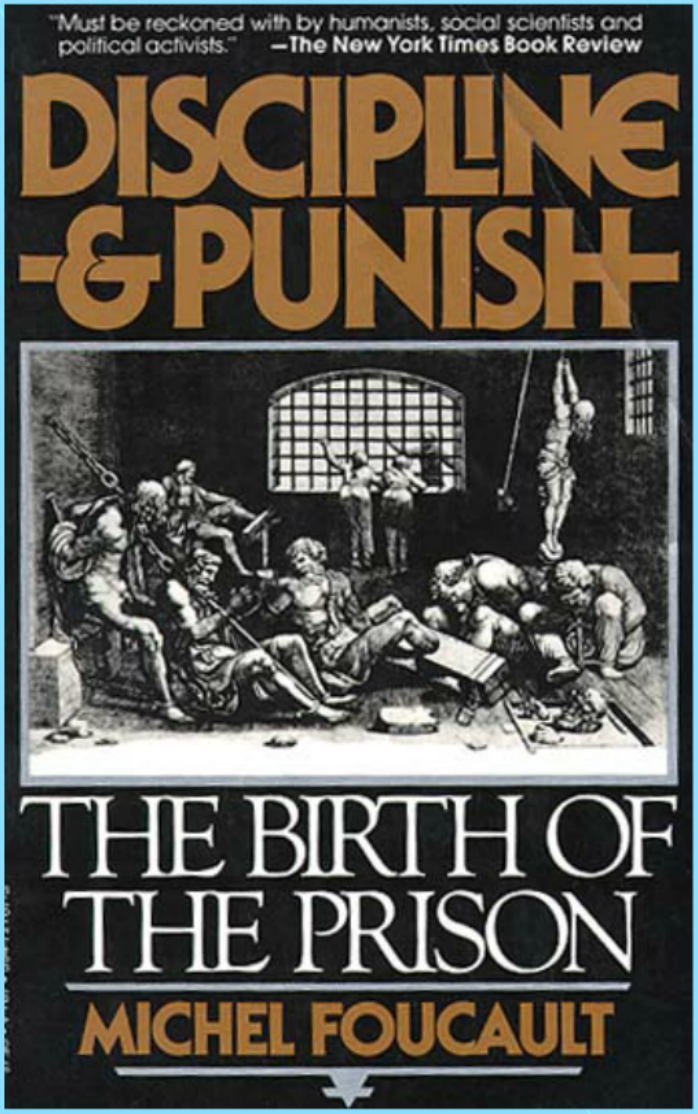
- Menneske: ~1km, vibrationer i luft
- Elefant: ~10km, vibrationer i jord
- Hvaler: ~1.600km, vibrationer i vand

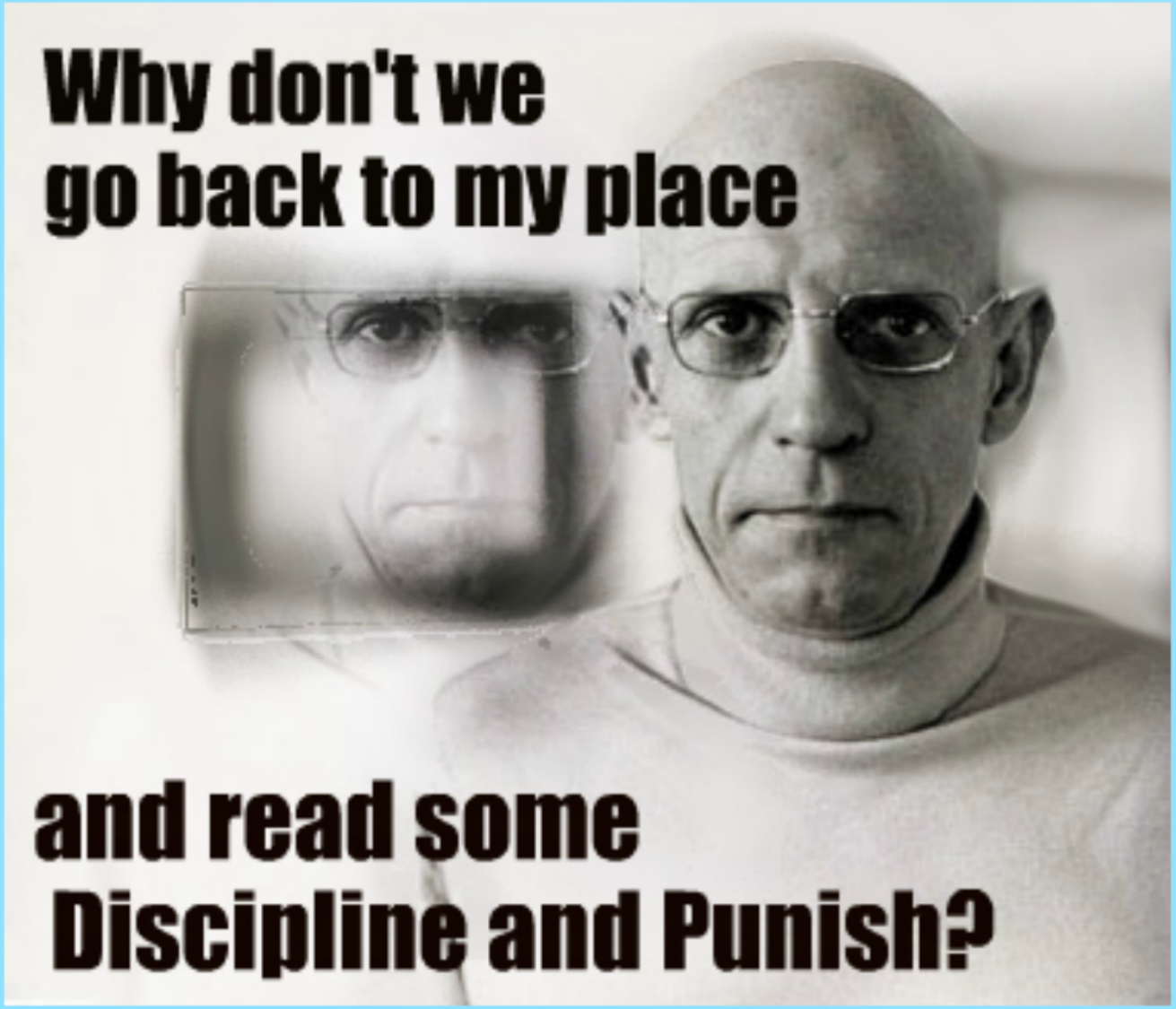
Ny rekord! Mennesker: ~20.000.000.000 km

lysets hastighed, stadig 18 timer

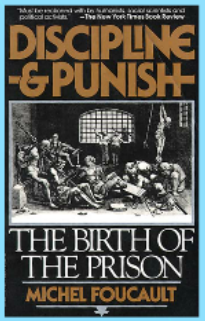
# Historisk overvågning

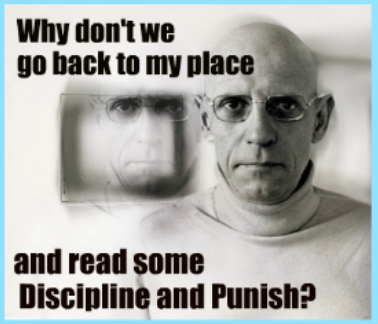

Jeremy Bentham, 1791


"Must be reckoned with by humanists, social scientists and political activists." —The New York Times Book Review
DISCIPLINE & PUNISH
THE BIRTH OF THE PRISON
MICHEL FOUCAULT


Why don't we go back to my place
and read some Discipline and Punish?

# Historisk overvågning



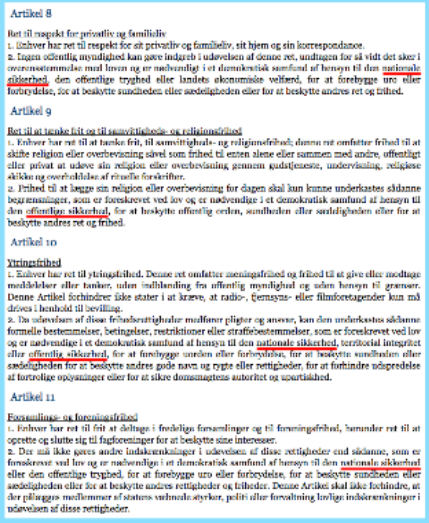
# Hvad siger loven?

# Den Europæiske Menneskerettighedskonvention

## Artikel 8 om ret til respekt for privatliv og familieliv:

*Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance*

*"... undtagen i overensstemmelse med loven og nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed ... at forebygge uro ....."*



Artikel 8

Ret til respekt for privatliv og familieliv
1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.
2. Ingen offentlig myndighed kan gøre indgreb i udøvelsen af denne ret, undtagen for så vidt det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres ret og frihed.

Artikel 9

Ret til at tænke frit og til samvittigheds- og religionsfrihed
1. Enhver har ret til at tænke frit, til samvittigheds- og religionsfrihed; denne ret omfatter frihed til at skifte religion eller overbevisning såvel som frihed til enten alene eller sammen med andre, offentligt eller privat at udøve sin religion eller overbevisning gennem gudstjeneste, undervisning, religiøse skikke og overholdelse af rituelle forskrifter.
2. Frihed til at lægge sin religion eller overbevisning for dagen skal kun kunne underkastes sådanne begrænsninger, som er foreskrevet ved lov og er nødvendige i et demokratisk samfund af hensyn til den offentlige sikkerhed, for at beskytte offentlig orden, sundheden eller sædeligheden eller for at beskytte andres ret og frihed.

Artikel 10

Ytringsfrihed
1. Enhver har ret til ytringsfrihed. Denne ret omfatter meningsfrihed og frihed til at give eller modtage meddelelser eller tanker, uden indblanding fra offentlig myndighed og uden hensyn til grænser. Denne Artikel forhindrer ikke stater i at kræve, at radio-, fjernsyns- eller filmforetagender kun må drives i henhold til bevilling.
2. Da udøvelsen af disse friheder medfører pligter og ansvar, kan den underkastes sådanne formelle bestemmelser, betingelser, restriktioner eller straffebestemmelser, som er foreskrevet ved lov og er nødvendige i et demokratisk samfund af hensyn til den nationale sikkerhed, territorial integritet eller offentlig sikkerhed, for at forebygge uorden eller forbrydelser, for at beskytte sundheden eller sædeligheden for at beskytte andres gode navn og rygte eller rettigheder, for at forhindre udspredelse af fortrolige oplysninger eller for at sikre domsmagtens autoritet og upartiskhed.

Artikel 11

Forsamlings- og foreningsfrihed
1. Enhver har ret til fri at deltage i fredelige forsamlinger og til foreningsfrihed, herunder ret til at oprette og slutte sig til fagforeninger for at beskytte sine interesser.
2. Der må ikke gøres andre indskrænkninger i udøvelsen af disse rettigheder end sådanne, som er foreskrevet ved lov og er nødvendige i et demokratisk samfund af hensyn til den nationale sikkerhed eller den offentlige tryghed, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder. Denne Artikel skal ikke forhindre, at der pålægges medlemmer af statens væbnede styrker, politi eller forvaltning lovlige indskrænkninger i udøvelsen af disse rettigheder.

## Artikel 8

Ret til respekt for privatliv og familieliv

1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.
2. Ingen offentlig myndighed kan gøre indgreb i udøvelsen af denne ret, undtagen for så vidt det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres ret og frihed.

## Artikel 9

Ret til at tænke frit og til samvittigheds- og religionsfrihed

1. Enhver har ret til at tænke frit, til samvittigheds- og religionsfrihed; denne ret omfatter frihed til at skifte religion eller overbevisning såvel som frihed til enten alene eller sammen med andre, offentligt eller privat at udøve sin religion eller overbevisning gennem gudstjeneste, undervisning, religiøse skikke og overholdelse af rituelle forskrifter.
2. Frihed til at lægge sin religion eller overbevisning for dagen skal kun kunne underkastes sådanne begrænsninger, som er foreskrevet ved lov og er nødvendige i et demokratisk samfund af hensyn til den offentlige sikkerhed, for at beskytte offentlig orden, sundheden eller sædeligheden eller for at beskytte andres ret og frihed.

## Artikel 10

Ytringsfrihed

1. Enhver har ret til ytringsfrihed. Denne ret omfatter meningsfrihed og frihed til at give eller modtage meddelelser eller tanker, uden indblanding fra offentlig myndighed og uden hensyn til grænser. Denne Artikel forhindrer ikke stater i at kræve, at radio-, fjernsyns- eller filmforetagender kun må drives i henhold til bevilling.
2. Da udøvelsen af disse frihedsrettigheder medfører pligter og ansvar, kan den underkastes sådanne formelle bestemmelser, betingelser, restriktioner eller straffebestemmelser, som er foreskrevet ved lov og er nødvendige i et demokratisk samfund af hensyn til den nationale sikkerhed, territorial integritet eller offentlig sikkerhed, for at forebygge uorden eller forbrydelse, for at beskytte sundheden eller sædeligheden for at beskytte andres gode navn og rygte eller rettigheder, for at forhindre udspredelse af fortrolige oplysninger eller for at sikre domsmagtens autoritet og upartiskhed.

## Artikel 11

Forsamlings- og foreningsfrihed

1. Enhver har ret til frit at deltage i fredelige forsamlinger og til foreningsfrihed, herunder ret til at oprette og slutte sig til fagforeninger for at beskytte sine interesser.
2. Der må ikke gøres andre indskrænkninger i udøvelsen af disse rettigheder end sådanne, som er foreskrevet ved lov og er nødvendige i et demokratisk samfund af hensyn til den nationale sikkerhed eller den offentlige tryghed, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder. Denne Artikel skal ikke forhindre, at der pålægges medlemmer af statens væbnede styrker, politi eller forvaltning lovlige indskrænkninger i udøvelsen af disse rettigheder.

# Hvad siger loven?

# Hvordan bliver loven brugt?

# Collect it all!

n og SMS

ng from terrorists?

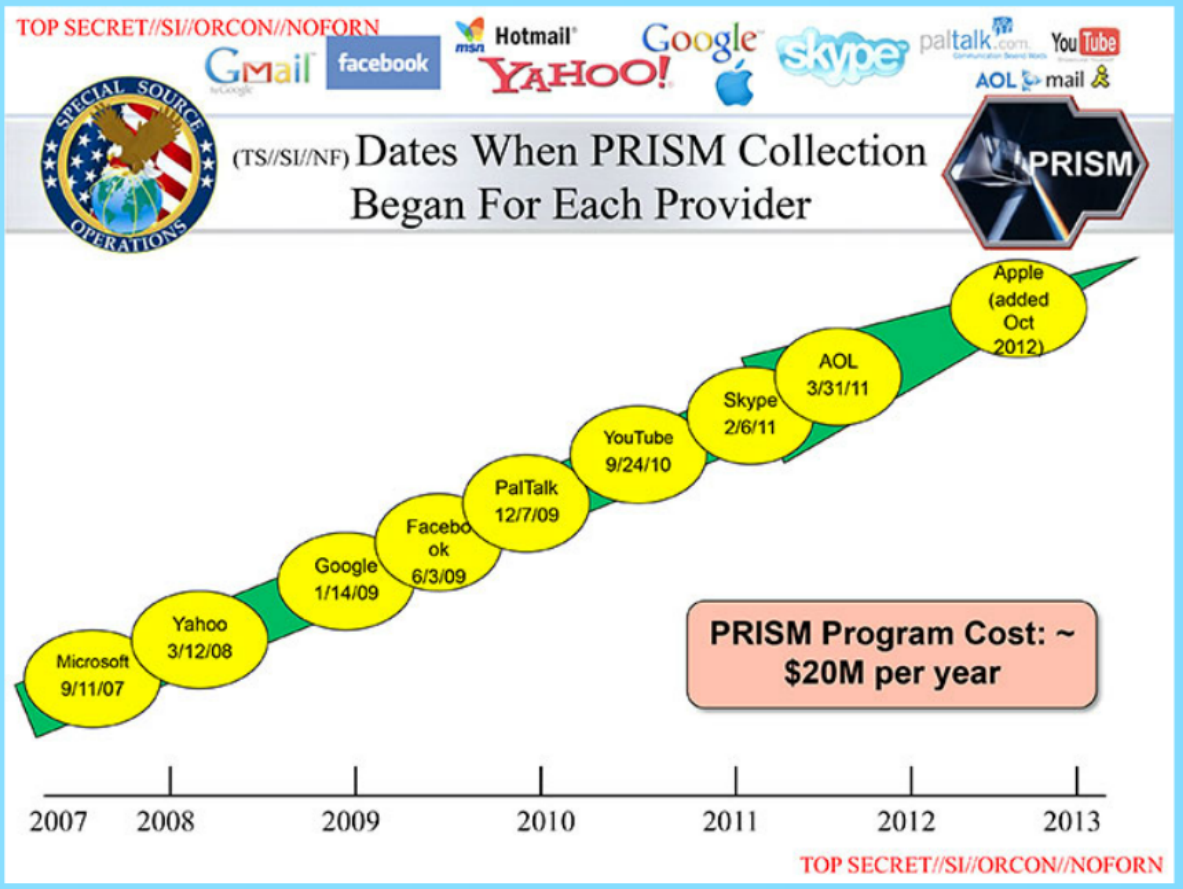
Vi

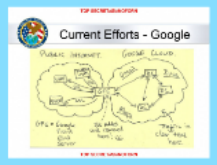
# Telefon og SMS

Only collecting from terrorists?

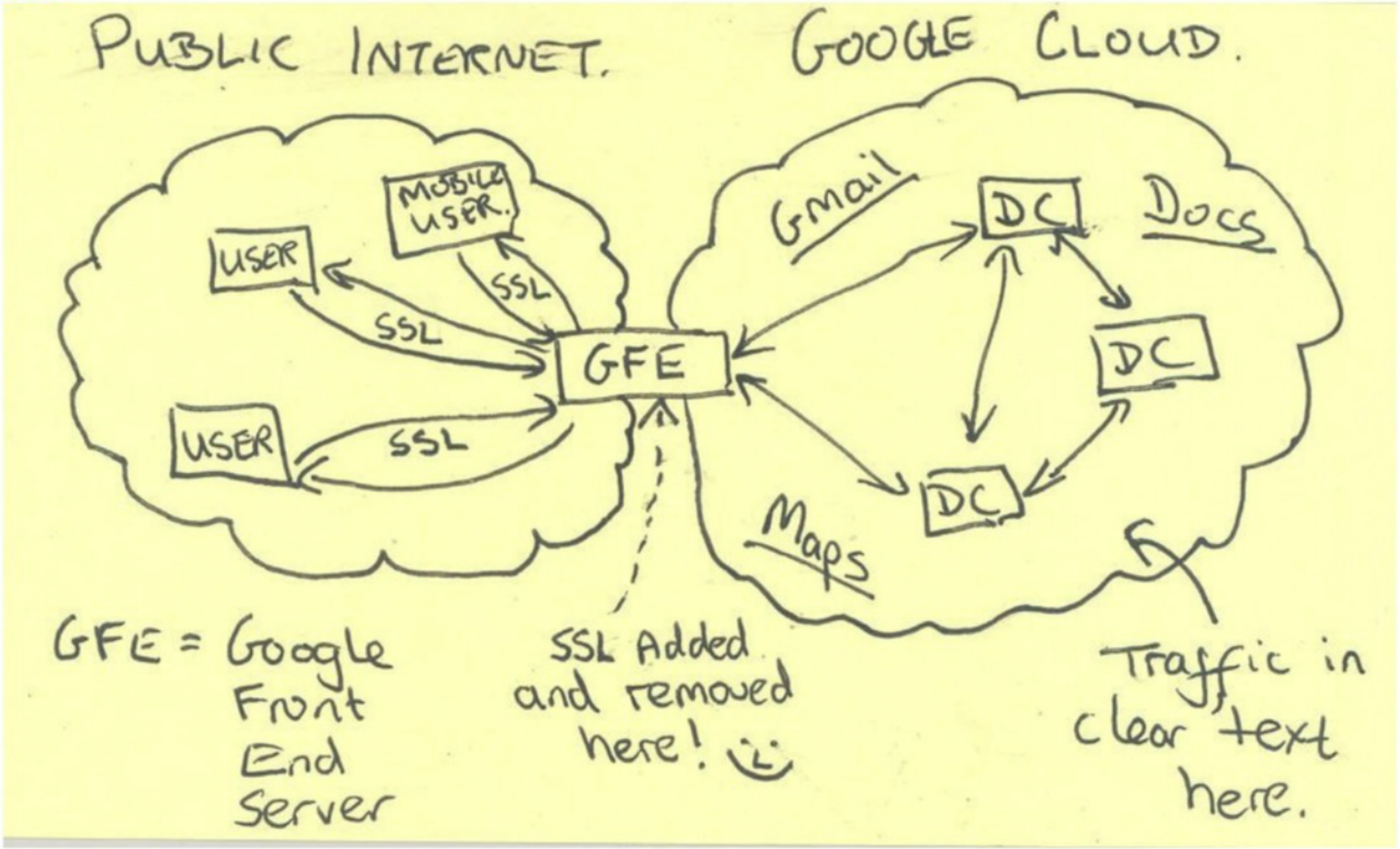
- Nationalt: AT&T, Verizon, ...
  250 mio. kunder
  2 mio. km fiber
  320 mio. i USA
  40,000km om jorden
- Internationalt: Belgacom, Gemalto, .....
  Du er her!
  Alle opkald, fx Bahamas
  "Metadata" udover
  200 mio. SMS/dag
  20 mio. SMS Danmark/dag
- Politisk: Angela Merkel, .....
  35 ledere
  195 lande

# Virksomhedsdata

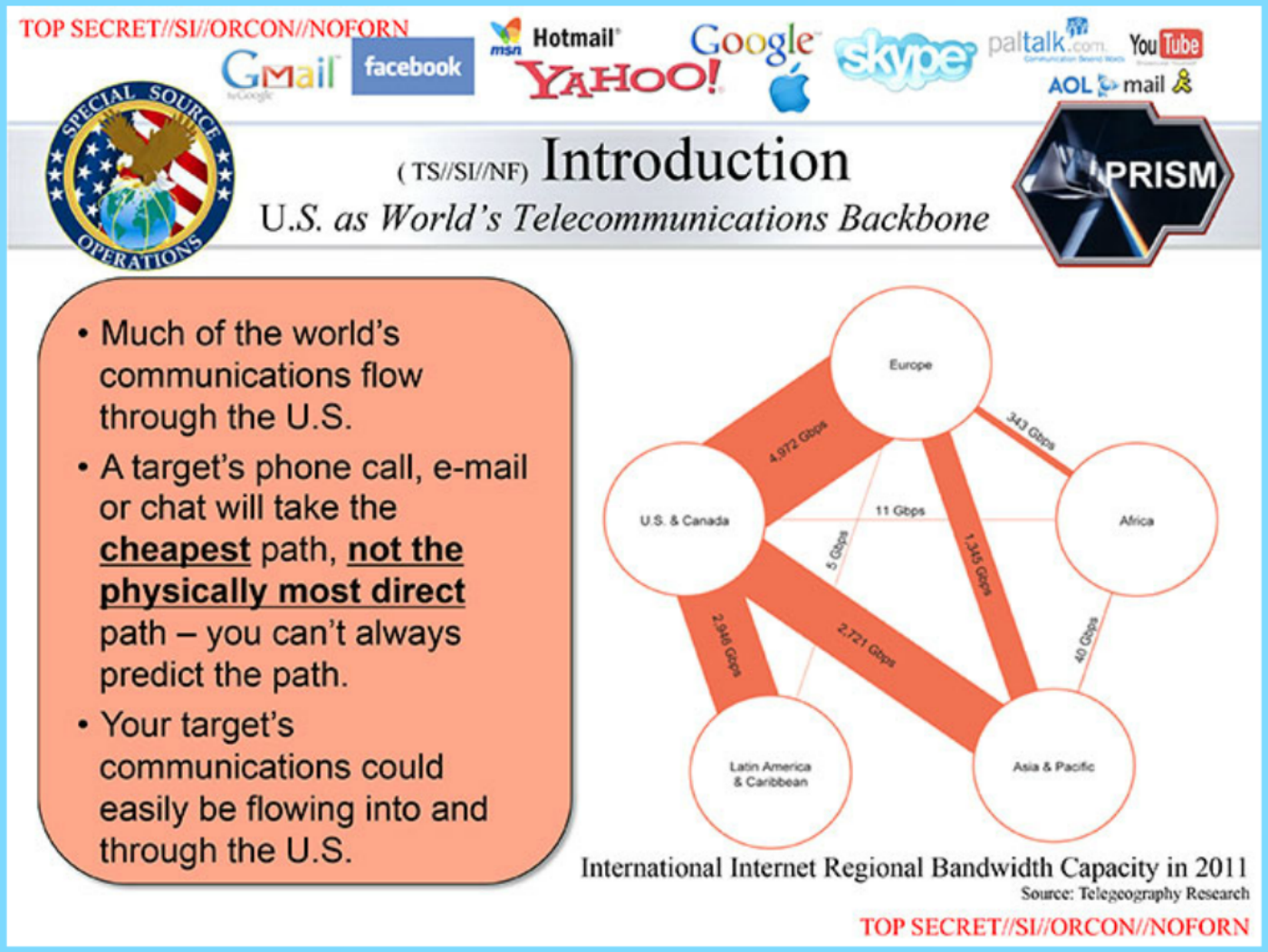


# Current Efforts - Google



# Internet




PRISM, Tempora, MUSCULAR, Project 6, Stateroom, Lustre, .....

# Og så videre..

Simkort skift

*Flyrejser*

GPS-koordinater

Adgangskoder

Pengeoverførsler

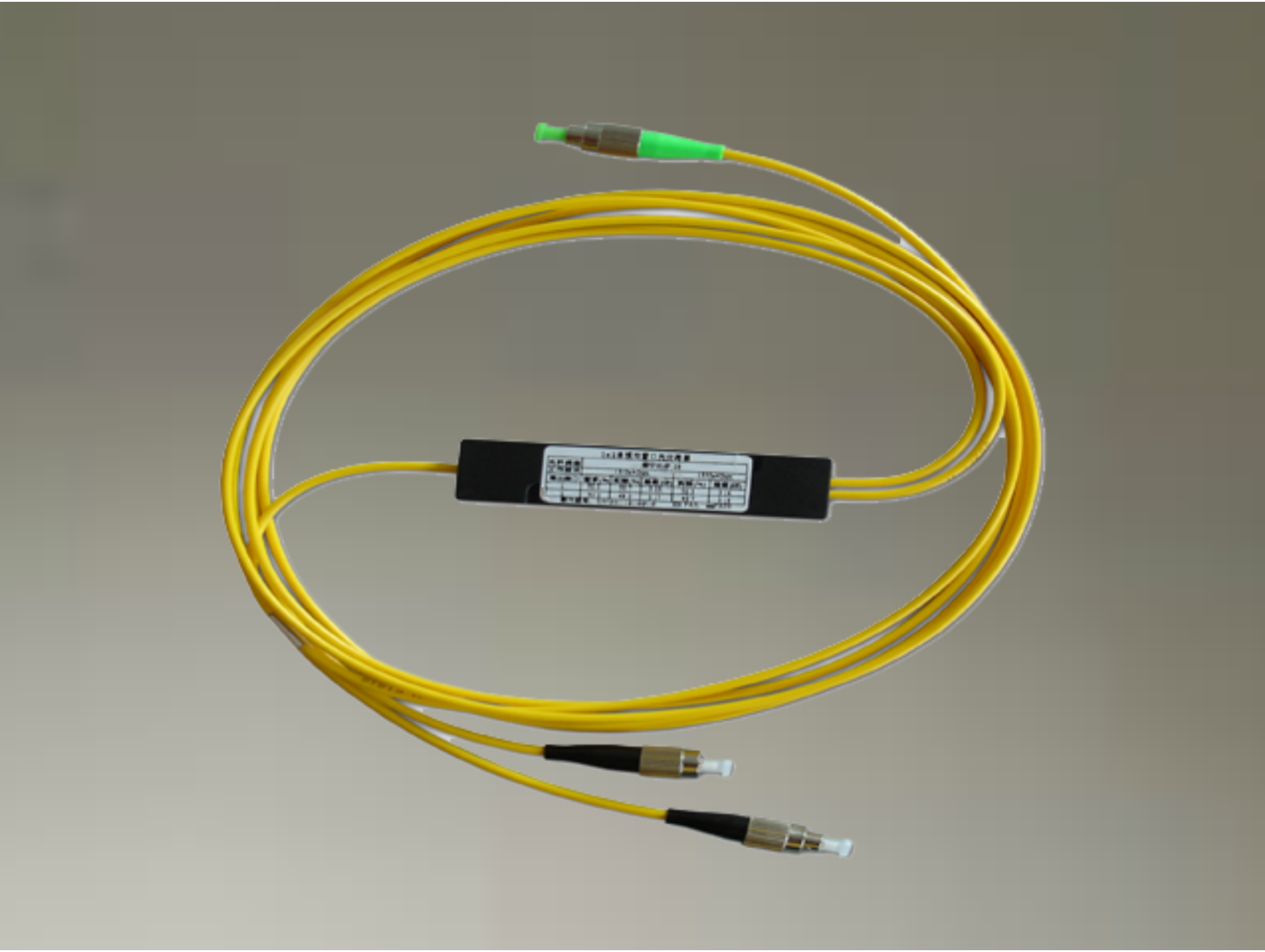
Grænse-overgang

EM bølger

Konferencer

# Metoder

# Telefonopkald

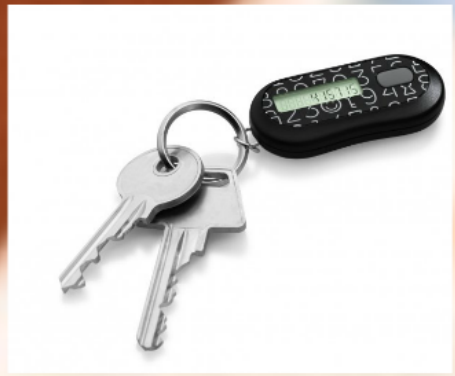


# Telefonopkald

# gemalto

security to be free

- Aflytning af højtstående medarbejdere
- 2.000.000.000 simkort om året
- 75% danske befolkning



telenor

3

Telia

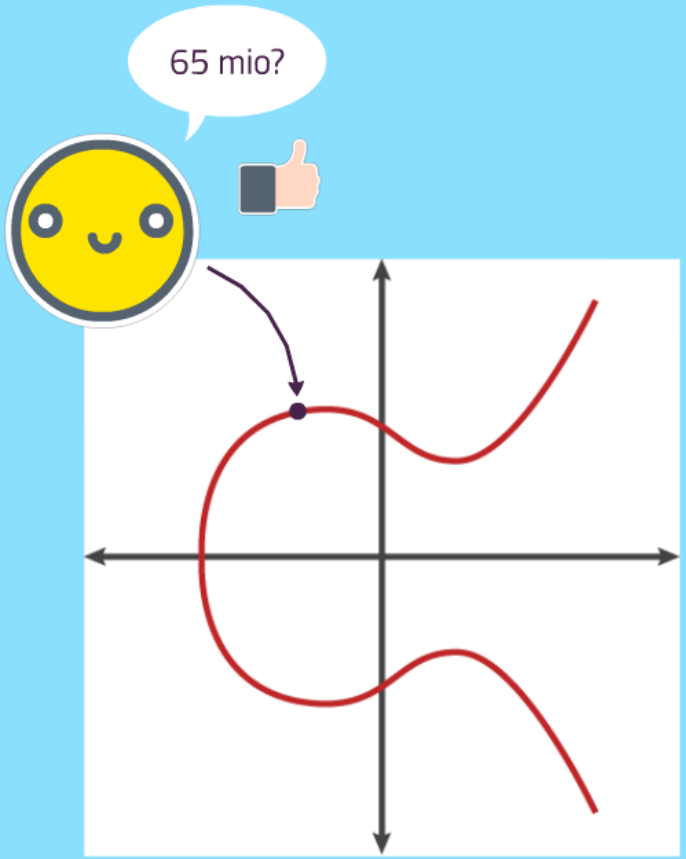
# Telefonopkald

# Bagdøre

- NSA budget, cryptanalyse og exloits, 230 mio.

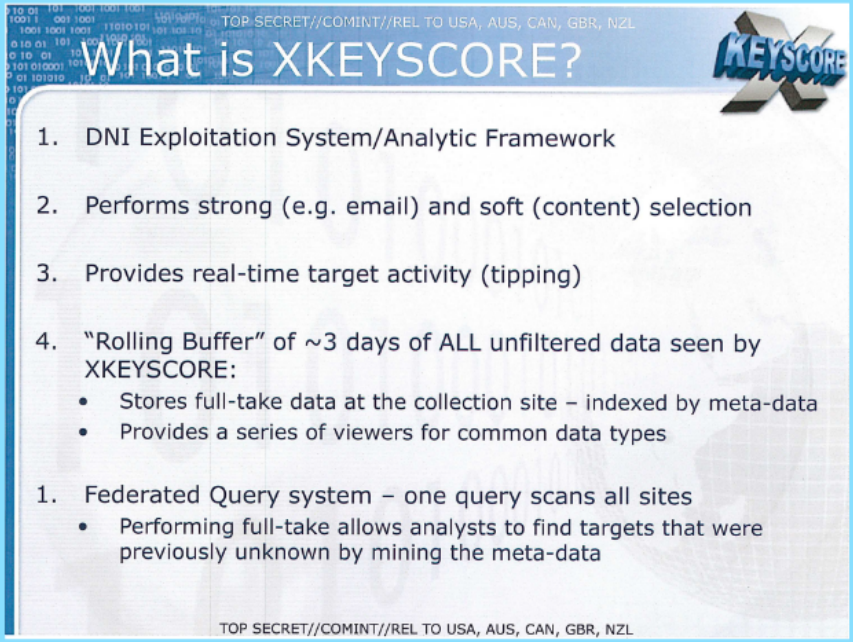
- Deanonymizing (TOR netværk)
- Bryde kryptering for HTTPS og VPN
- Store problemer med TrueCrypt

- Svække state-of-art kryptering



# Søgning

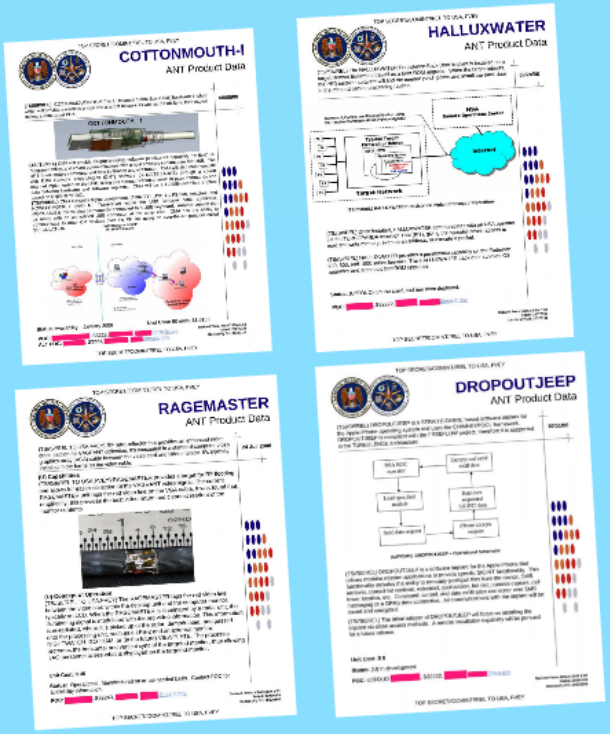

- Over 700 servere
- Over 150 steder i verden
- Plugins: mail, filer, http, chat, ..., fuld log

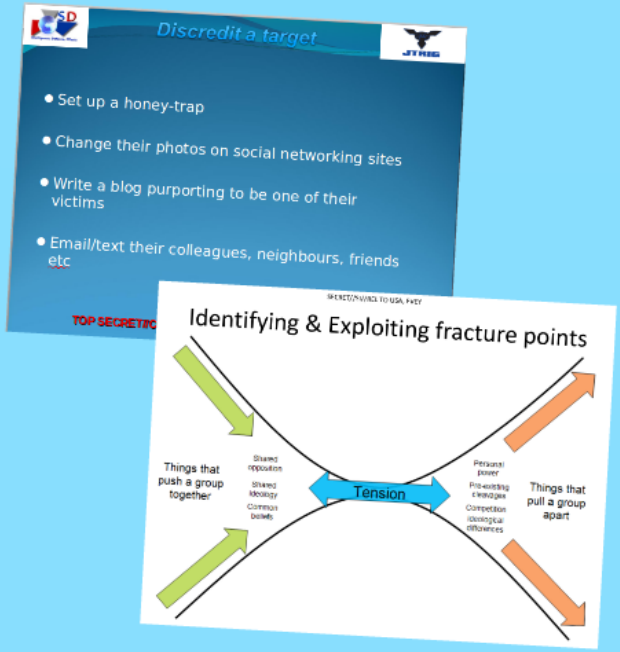



## Show me all ...

- encrypted word documents from Iran
- excel files containing MAC adresses
- exploitable machines in country X
- PGP usages in Iran
- VPN startups in country X [...] decrypt and discover users
- traffic from German speakers in Pakistan
- suspicious Google (Maps) searches

# Fysisk / psykisk



TOP SECRET//COMINT//REL TO USA, FVEY

# COTTONMOUTH-I

## ANT Product Data

08/05/08

**(TS//SI//REL)** COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.


**(TS//SI//REL)** CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

**(TS//SI//REL)** CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.


**Status:** Availability – January 2009 **Unit Cost:** 50 units: $1,015K

**POC:** [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
**ALT POC:** [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

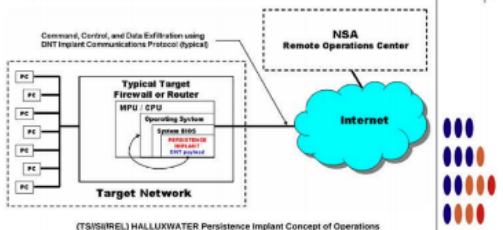
TOP SECRET//COMINT//REL TO USA, FVEY

# HALLUXWATER

## ANT Product Data

06/24/08

(TS//SI//REL) The HALLUXWATER Persistence Back Door implant is installed on a target Huawei Eudemon firewall as a boot ROM upgrade. When the target reboots, the PBD installer software will find the needed patch points and install the back door in the inbound packet processing routine.




(TS//SI//REL) HALLUXWATER Persistence Implant Concept of Operations

(TS//SI//REL) Once installed, HALLUXWATER communicates with an NSA operator via the TURBOPANDA Insertion Tool (PIT), giving the operator covert access to read and write memory, execute an address, or execute a packet.

(TS//SI//REL) HALLUXWATER provides a persistence capability on the Eudemon 200, 500, and 1000 series firewalls. The HALLUXWATER back door survives OS upgrades and automatic bootROM upgrades.

**Status:** (U//FOUO) On the shelf, and has been deployed.

**POC:** [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

# RAGEMASTER

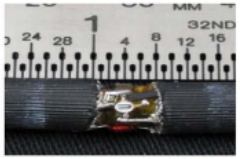
## ANT Product Data

24 Jul 2008

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

**(U) Capabilities**

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.




**(U) Concept of Operation**

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

**Unit Cost: $ 30**

**Status:** Operational. Manufactured on an as-needed basis. Contact POC for availability information.

**POC:** [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

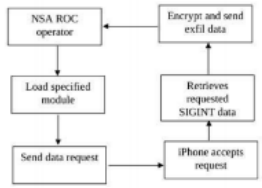
TOP SECRET//COMINT//REL TO USA, FVEY

# DROPOUTJEEP

## ANT Product Data

10/01/08

(TS//SI//REL) DROPOUTJEEP is a STRAITBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.




(U//FOUO) DROPOUTJEEP – Operational Schematic

(TS//SI//REL) DROPOUTJEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted.

(TS//SI//REL) The initial release of DROPOUTJEEP will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.

**Unit Cost: $ 0**

**Status:** (U) In development

**POC:** U//FOUO [redacted], S32222, [redacted]@nsa.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

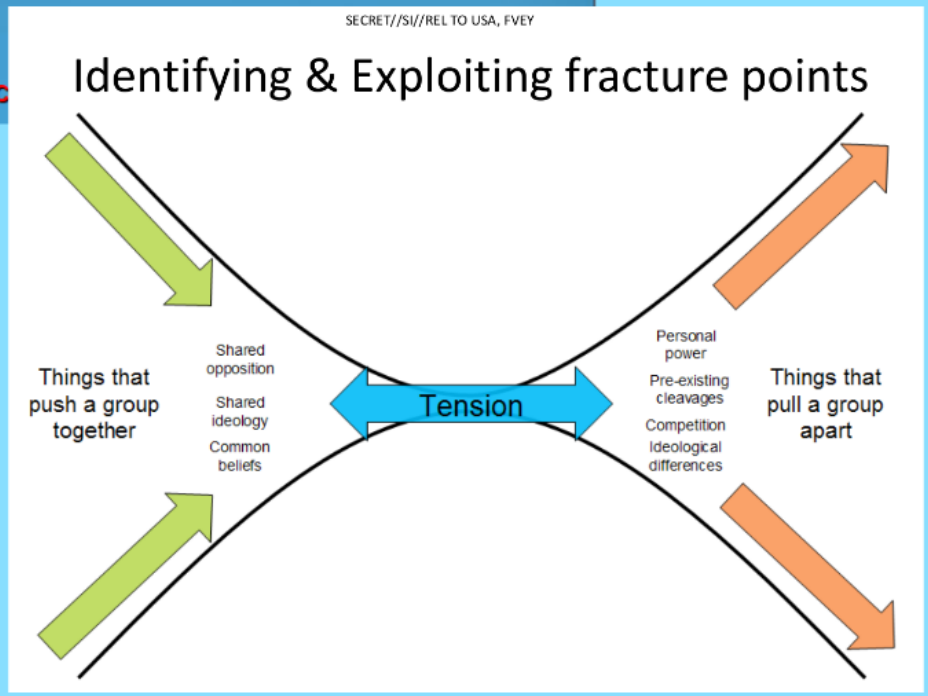
## Discredit a target

- Set up a honey-trap
- Change their photos on social networking sites
- Write a blog purporting to be one of their victims
- Email/text their colleagues, neighbours, friends etc

TOP SECRET//C

SECRET//SI//REL TO USA, FVEY

## Identifying & Exploiting fracture points



# Metoder

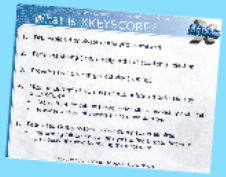
## Telefonopkald

## Bagdøre

- NSA budget, cryptanalyse og exloits, 230 mio.
- Deanonymizing (TOR netværk)
- Bryde kryptering for HTTPS og VPN
- Store problemer med TrueCrypt
- Svække state-of-art kryptering


## Søgning


- Over 700 servere
- Over 150 steder i verden
- Plugins: mail, filer, http, chat, ..., fuld log




Show me all ...

- encrypted word documents from Iran
- excel files containing MAC adresses
- exploitable machines in country X
- PGP usages in Iran
- VPN startups in country X [...] decrypt and discover users
- traffic from German speakers in Pakistan
- suspicious Google (Maps) searches

## Fysisk / psykisk

# Global overvågning

## Europa Parlamentet 2001

Existence of global system for interception of private and commercial communication

| | Udenlandsk | Regering | Civilt |
|---|---|---|---|
| Belgium | + | + | - |
| Denmark | + | + | + |
| Finland | + | + | + |
| France | + | + | + |
| Germany | + | + | + |
| Greece | + | + | - |
| Ireland | - | - | - |
| Italy | + | + | + |
| Luxembourg | - | - | - |
| Netherlands | + | + | + |
| Austria | + | + | - |
| Portugal | + | + | - |
| Sweden | + | + | + |
| Spain | + | + | + |
| UK | + | + | + |
| USA | + | + | + |
| Canada | + | + | + |
| Australia | + | + | + |
| New Zealand | + | + | + |

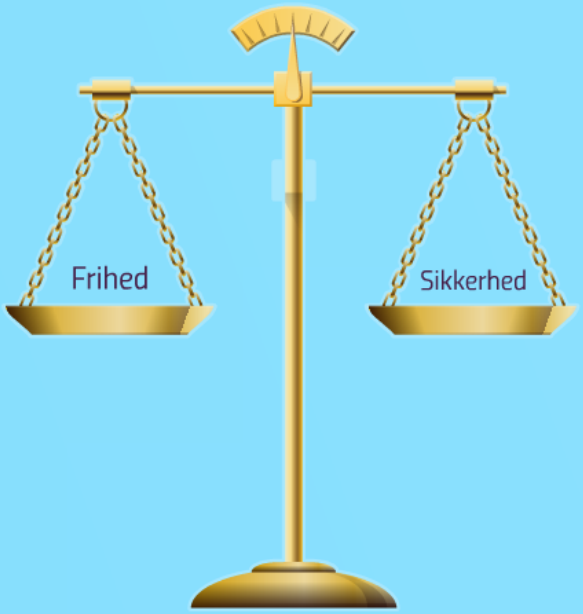
*"Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it."*– Edward Snowden

# Overvågningsparadokset

Vi mener privat kommunikation er en menneskerettighed.

Vi ved, meget kommunikation vi tror er privat, ikke er.

Vi er ligeglade?

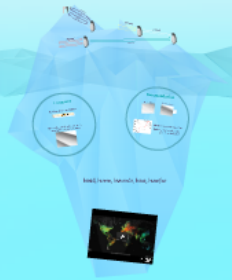



"*Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.*" - Benjamin Franklin

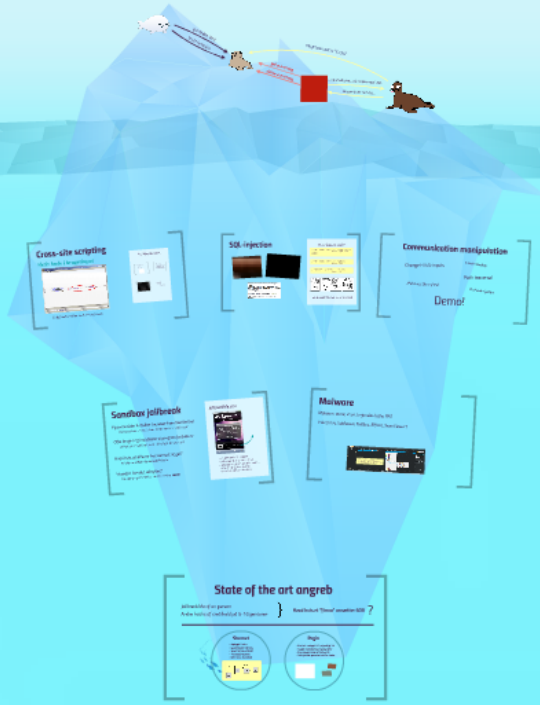
# Angreb / overvågning

Michael Nielsen

## Information



## Angreb




## Overvågning