

2013-11-07, Tallinn

Olukorrast riigis,
ehk
“NSA ja PRISMi
mõju
turvalisusele
maailmas”

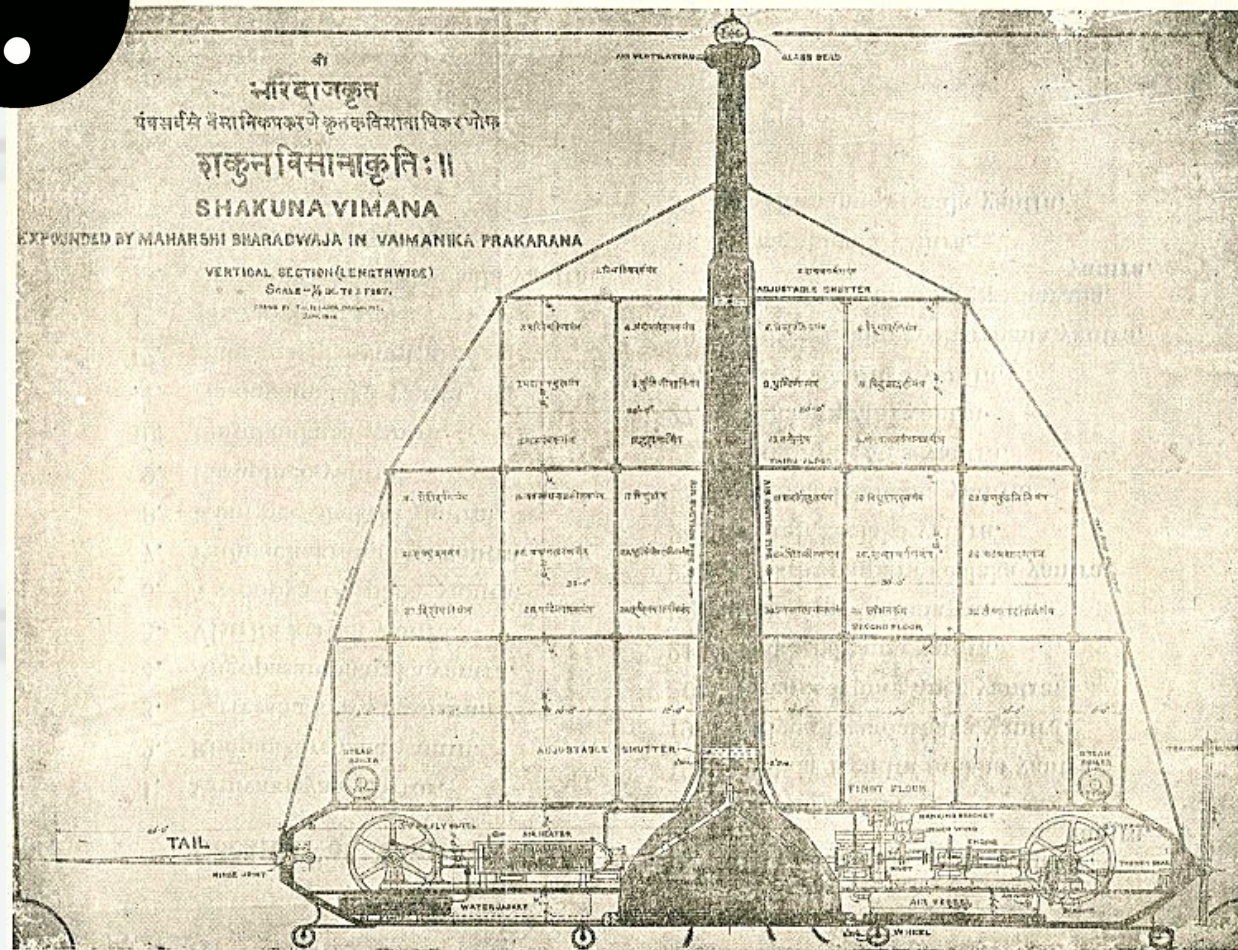
Anto Veldre, CERT-EE



Tisklaimer



NB! All copyrights belong to their respective owners!



Teesid

(*well*, vähemasti mingi lähtekoht)



Netikodanikud arvavad...

- Ei ole ilus turvastandardeid (NIST) timmida
 - (sama hea kui diktaatori tapmiseks tohterdada arstiteaduse õpikuid)
- Riistvara ja tarkvara tagauksestamine...
- Schrödinger'i paradoks nuhkimisriigis: kuniks Sinu faile kontrollitakse, oled sa ühtaegu nii süütu kui terrorist.
- Mida kroonu teeb, on salajane. Mida kodanik teeb, on avalik. Kuulge – kas äkki ei peaks olema vastupidi?
- „Benjamin Button“: Lihtne, aus, vaimselt terve inimene, kes hommikul läheb tööle ja õhtul tuleb töölt. Mis temal karta on?
- Kui sa pole midagi paha teinud, siis võib-olla pole sa üldse midagi teinud?

Ahto Lobjakas arvab...

<http://arvamus.postimees.ee/2582824/ahto-lobjakas-nuhkimise-sullogismid>

- Vaikne konstitutsiooniline pööre demokraatliku võimu kolmikjaotuses
- Küsimus: kas senine kolmetine võimude jaotus – seadusandlik, kohtu- ja täitevvõim - mis pärit Locke'ilt, Montesquieult ja Madisonilt - ikka kehtib?
- Kongress tunnistab võimetust nuhkimis-anarhia vastu. Kohtuvõim näeb NSA tööd vaid läbi salajaste erikohtute.
- USA nuhkimispuu on liiga suur, et kukkuda?

Mikko Hypponen arvab...

<http://lwn.net/SubscriberLink/571875/8edc2f30a8864e5b/>

- Think about the number of hard disks you can put into one of the "largest IKEA you have ever seen".
- “secret documents”, “all countries spy”,
“war on terrorism”, “nothing to hide”,
“Internet is a colony for the US” ?
- Are we willing to throw away the US Constitution and Bill of Rights, the Universal Declaration of Human Rights, and freedom of the press **to fight terrorism**?

#friendofafriendofafriend

Iva

- Mikko Hyppönen:
 - Mõned inimesed ütlevad, et selles nuhkimises pole midagi uut. Et me juba teadsime sellest.
 - Ärge kuulake neid! Me ehk kahtlustasime, mis toimub, kuid nüüd on meil faktid.
- Anto:
 - Kas teadsin? Olin kindel, arvasin, oletasin?

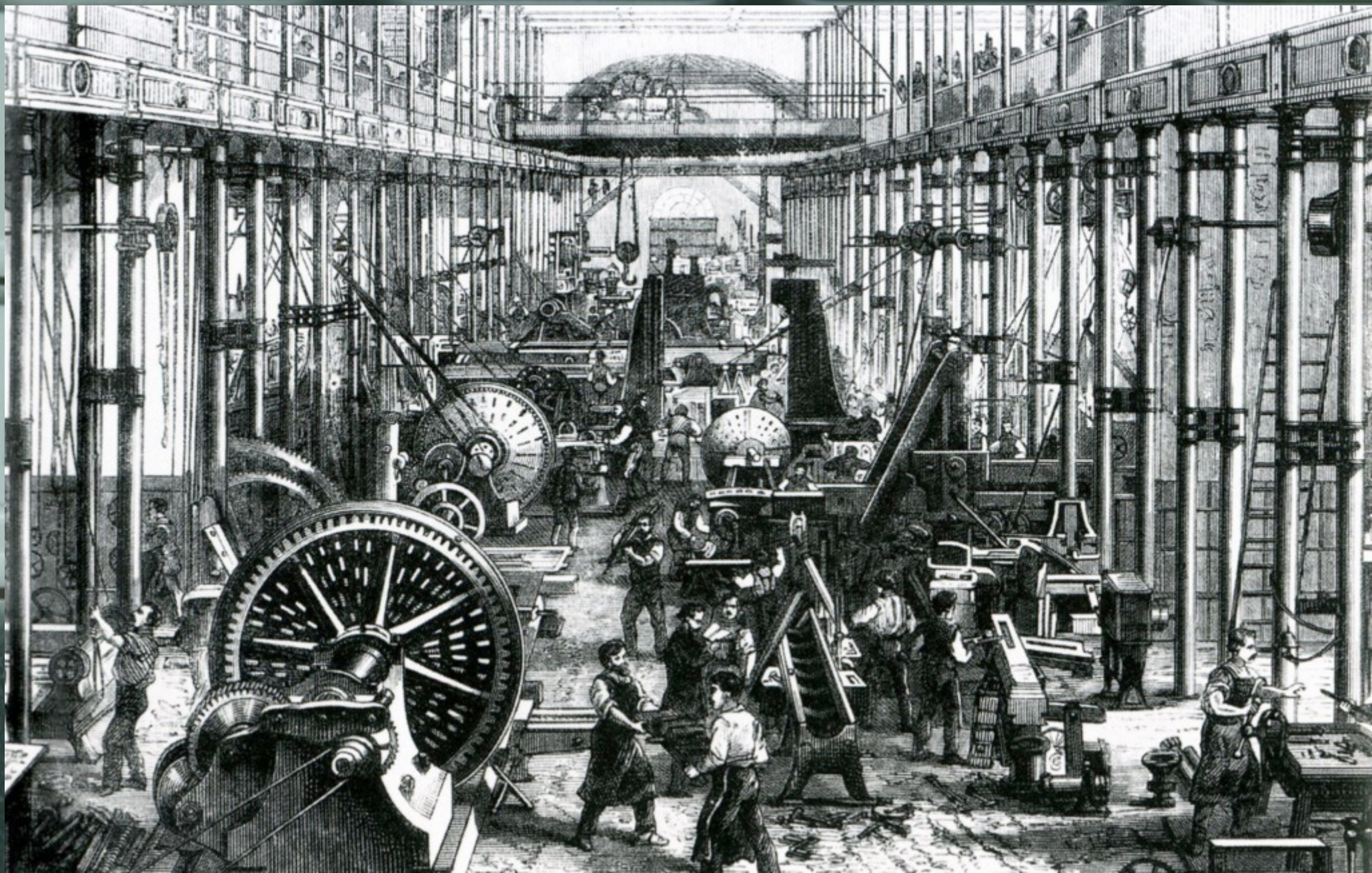


1 – Intro

(Tehnoloogia mõjust)



http://www.bellona.org/articles/articles_2012/fukushima-westcoast-radiation





(c) marko kivimäe

Tehnoloogia!

57



Poliitilise kontrolli tehnoloogiad



Kelner: millist maailma te soovisite?

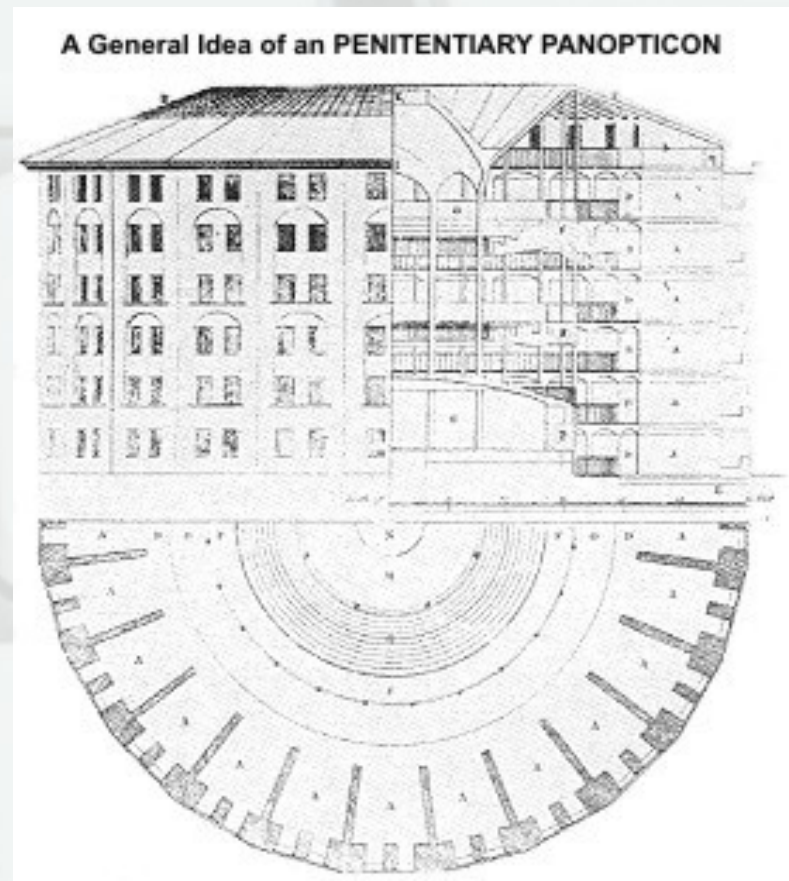


2 – Elitaarsed mängud



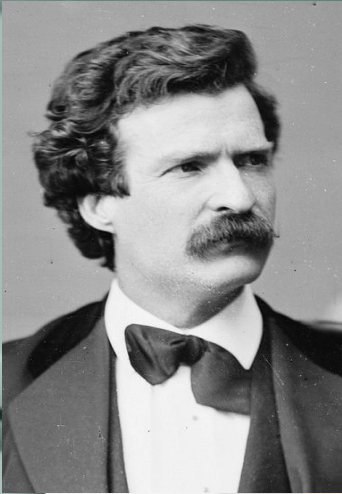


Mis kõik on maailmas võimalik...



Miks?

- Sest see on võimalik.
 - Tehnoloogia võimaldab seda;
 - Inimolemus võimaldab seda.

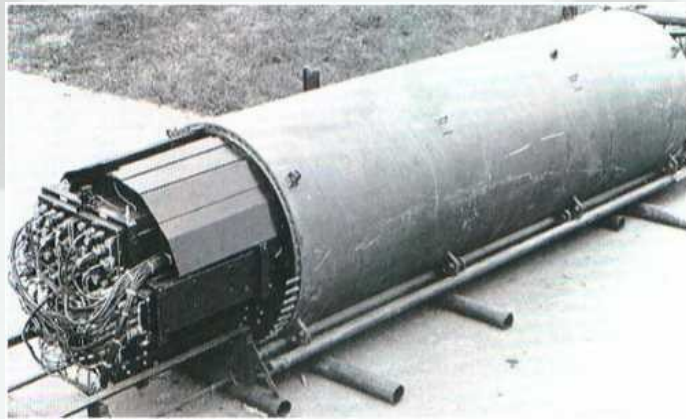


1906-09-07, Mark Twain

"We are of the Anglo-Saxon race, and when the Anglo-Saxon wants a thing he just takes it."

"The English and the Americans are thieves, highway-men, ~~and~~ pirates, and we are proud to be of the combination."

Ajalugu on olnud katkematu



Op! Ivy Bells 1971 @OxOTCK :
<http://rijmenants.blogspot.com/2009/12/operation-ivy-bells.html>

Op! GunMan
(CBS 1985-03-25):



Op! Gold (1956):

http://www.nsa.gov/public_info/_files/cryptologic_histories/learning_from_the_enemy.pdf

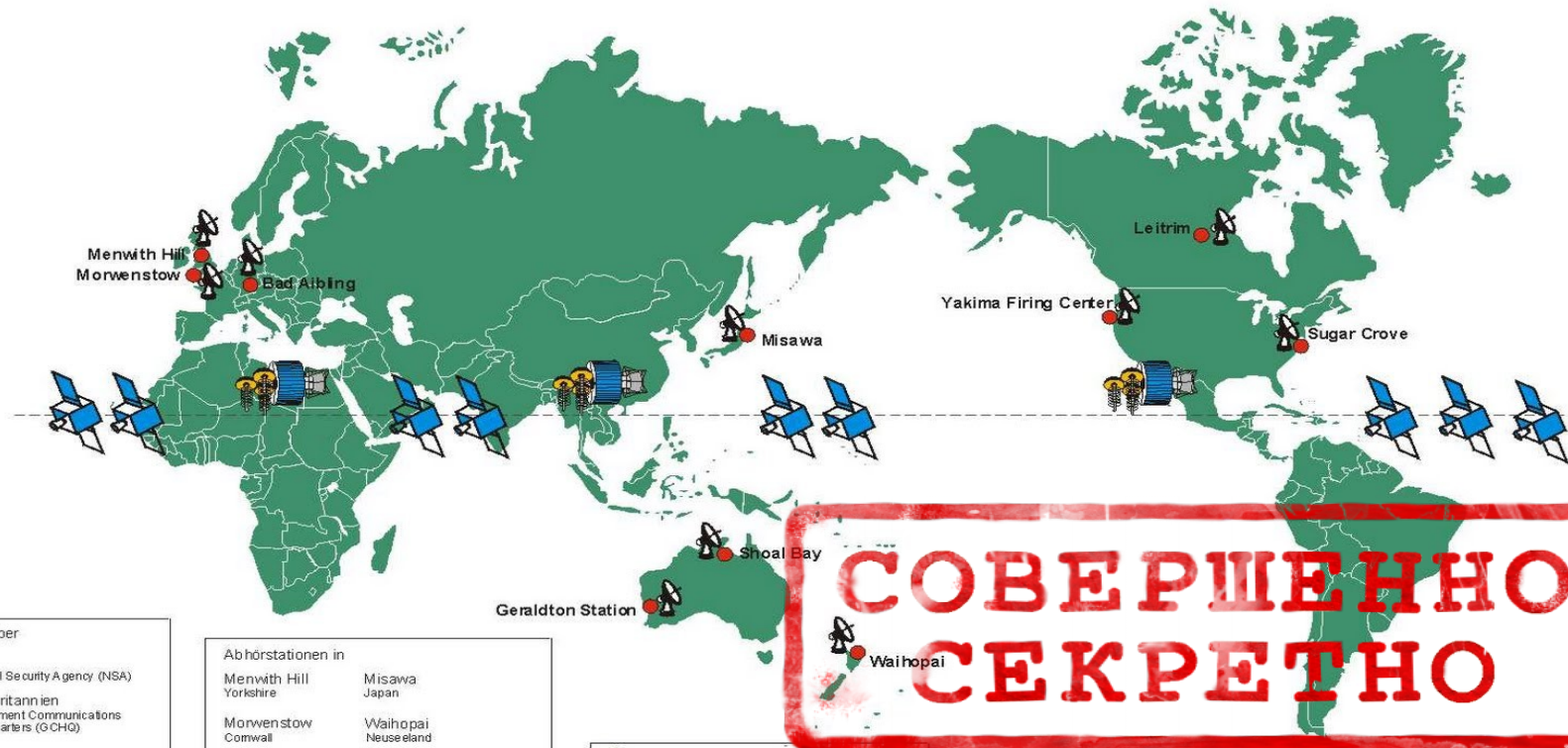
http://en.wikipedia.org/wiki/Operation_Gold

FVEY

фор нейшионлс оунли

Globales elektronisches Aufklärungssystem Echelon

Echelon hört ungefiltert den gesamten eMail-, Telefon-, Fax- und Telexverkehr ab, der weltweit über Satelliten weitergeleitet wird.



Betreiber

USA
National Security Agency (NSA)
Großbritannien
Government Communications
Headquarters (GCHQ)
Kanada
Communications Security
Establishment (CSE)
Australien
Defence Signals Directorate (DSD)
Neuseeland
Government Communications
Security Bureau

Abhörstationen in

Menwith Hill Yorkshire	Misawa Japan
Morwenstow Cornwall	Waihopai Neuseeland
Bad Aibling Bayern	Yakima Firing Center 200 km sw von Seattle
Geraldton Station Westaustralien	Leitrim Kanada
Shoal Bay Nordaustralien	Sugar Grove 250 km sw von Washington D.C.

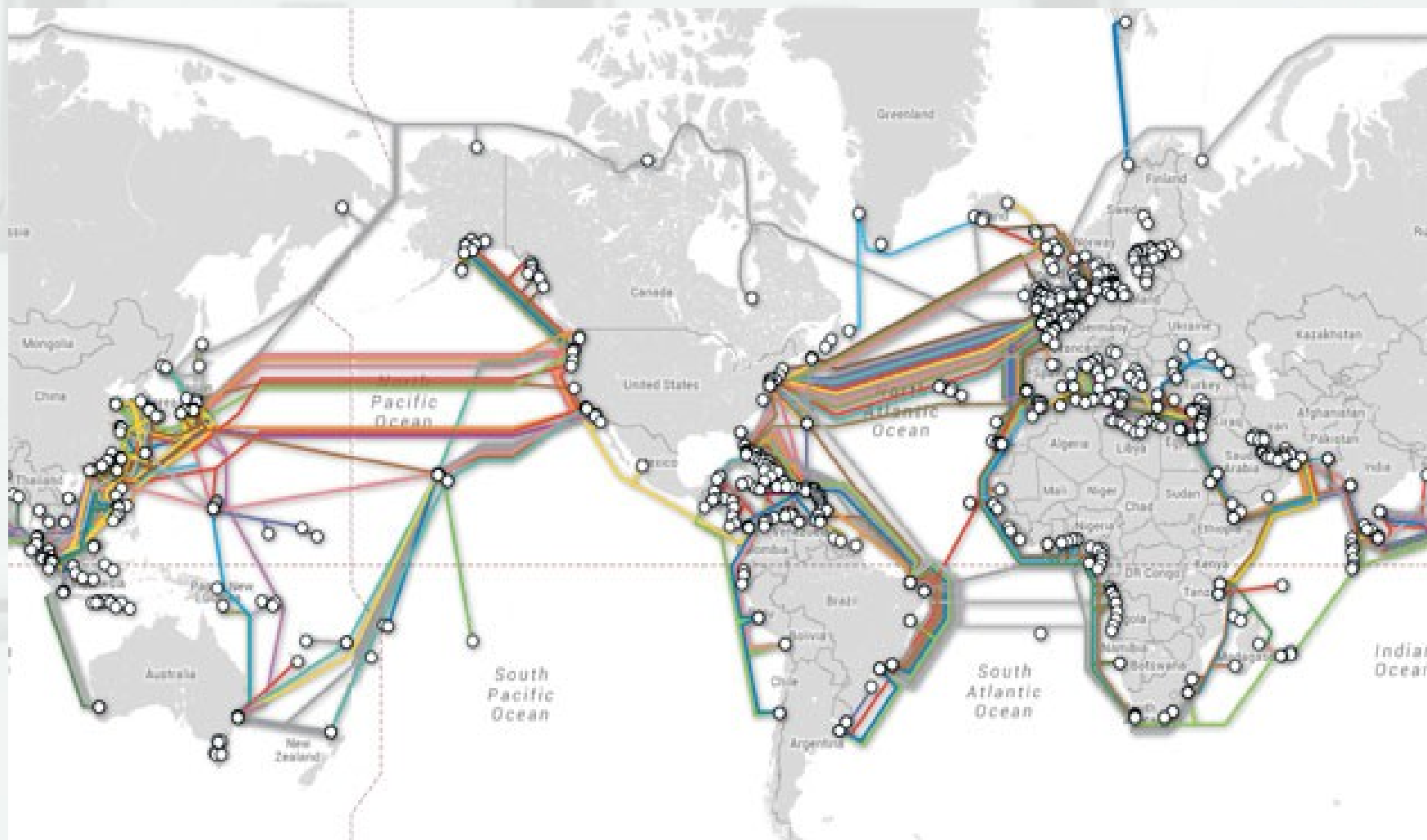


Kommunikationssatelliten

Kommunikationssatelliten

Abhörstation

Grafik: Landesamt für Verfassungsschutz Baden-Württemberg



<http://nsa.gov1.info/surveillance/>



Echelon



Duncan Campbell wins civil liberty award

THIS YEAR'S Cobden Award — for the piece of writing judged to have done most for civil liberty — has been given to Duncan Campbell of the *New Statesman*. Announcing the award, Malcolm Hurwitt, secretary of the Trust, cited Mr Campbell's 'major piece of investigative journalism' which exposed the government's telephone-tapping operations. He said: 'Duncan Campbell's revelations highlight the lack of accountability of the security services and the consequences of allowing these secret figures to define their

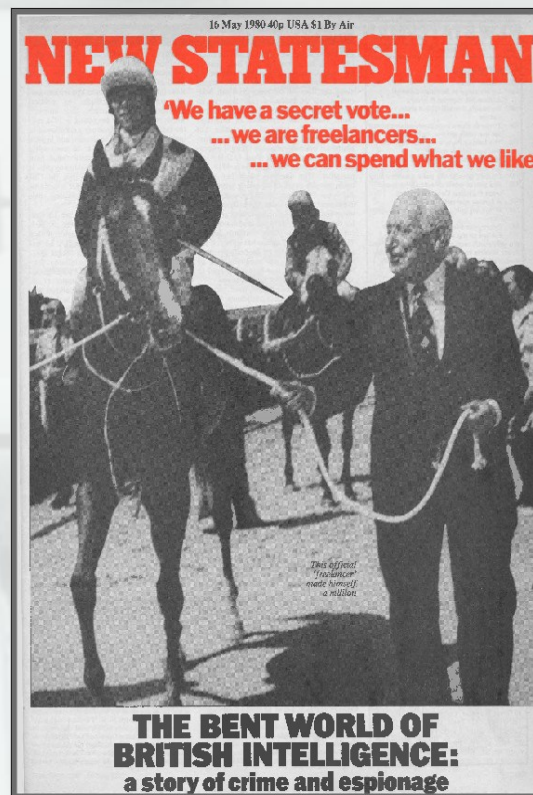
write laudatory mini-profiles of one of our own, so perhaps we can cite the *Observer's* useful compact account on 12 October:

Together (Campbell's articles this year) . . . constitute the most important body of knowledge about the secret activities and plans of a government to have been published since the post-Watergate disclosures in America . . .

Campbell, 27, combines the good investigative reporter's fanatical appetite for detail with the scientific training that enables him to recognise the significance of what he discovers.

After attending Dundee High School and Brasenose College, Oxford, where he got a first in physics, he began contributing stories about electronics to specialist journals.

In February 1977 he was arrested with another journalist, Crispin Aubrey, after interviewing a former Signals Corps intelligence analyst, and charged under Section 1 of the Official Secrets Act. The charges under this section were later dropped, and he was found guilty of lesser offences under Section 2. (He was given a dis-



CONTENTS



ACKNOWLEDGEMENTS

FOREWORD BY DAVID LANGE

FOREWORD BY JEFFREY RICHELSON

INTRODUCTION 12

CHAPTER 1 1984 19

CHAPTER 2 Hooked Up to the Spy Network: The UKUSA System 26

CHAPTER 3 The Power of the Dictionary: Inside ECHELON 42

CHAPTER 4 Fighting the Cold War: The Role of UKUSA 57

CHAPTER 5 The GCSB, ANZUS and a Nuclear-Free New Zealand 76

CHAPTER 6 Behind Closed Doors: What Happens Inside the GCSB 92

CHAPTER 7 The Organisation: Secret Structures of the GCSB 119

CHAPTER 8 Secret Squirrels: Who Runs the GCSB? 138

CHAPTER 9 Station NZC-332: Electronic Eavesdropping
from Tangimoana 147

http://en.wikipedia.org/wiki/Nicky_Hager

EUROPEAN PARLIAMENT

SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT

STOA

AN APPRAISAL OF TECHNOLOGIES OF POLITICAL CONTROL

Working document
(Consultation version)

Luxembourg, 6 January 1998

PE 166 499

Directorate General for Research

<http://cryptome.org/stoa-atpc.htm>

Autor	Berlin, Armin
Pealkiri	Ešelon hakkab liikuma / Armin Berlin
Väljaanne	Luup (1999) nr. 3, 8. veebr., lk. 36-38
Ilmunud	1999

Annotatsioon	Pealtkuulamissüsteemist ECHELON
Märksõnad	Ameerika Ühendriigid info kommunikatsioon luure luureteenistused
Ilumisaeg	1999-02

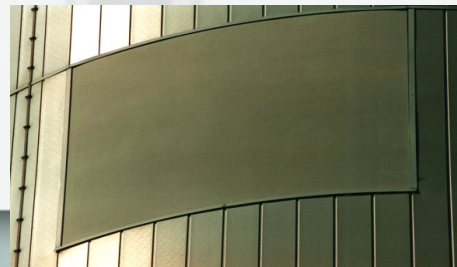
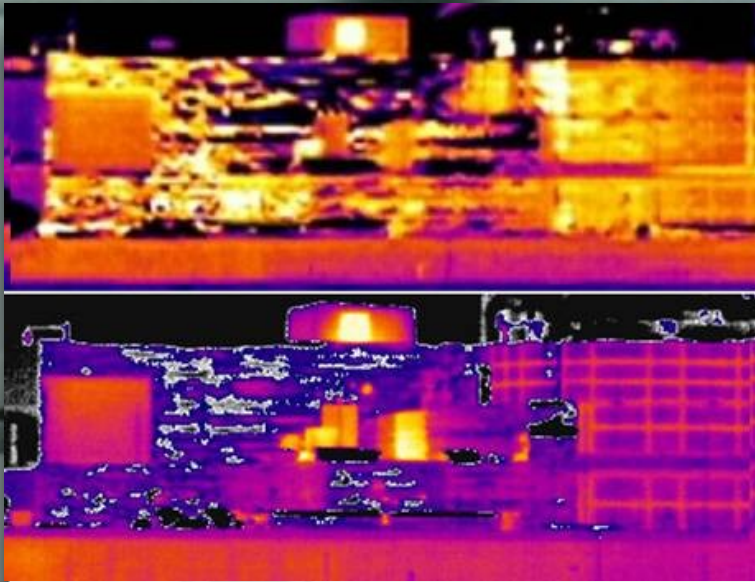
Postimees

404: Page not found

<http://www.postimees.ee/luup/99/03/sisukord.htm>



Linnupesa sarnane



1967-06-08 - USS Liberty

34 surnut

173 haavatut



http://en.wikipedia.org/wiki/USS_Liberty_incident

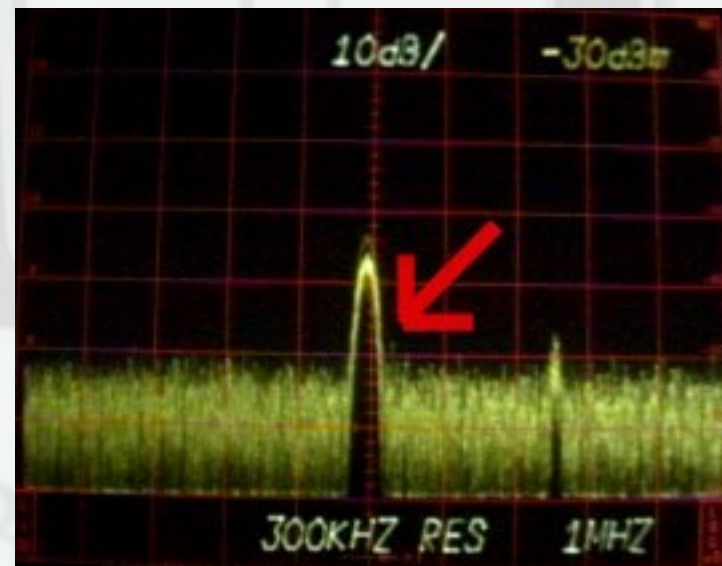
EW, Tallinn, 1993-09-28

«Täna kell 3.42 oli Ameerika Ühendriikide saatkonna õuel Kentmanni 20 pommilahvatus.»

«Pomm oli pandud garaažil oleva satelliidiantenni alla. Plahvatus oli tugev, raudkonstruktsioonil olev antenn kukkus katusele. Purunesid USA saatkonna, samas hoones oleva Suurbritannia saatkonna ja kõrvalmaja aknaklaasid.» Inimesed plahvatuses vigastada ei saanud. Oletatavasti moodustas lõhkekeha viis kilo kordiiti.

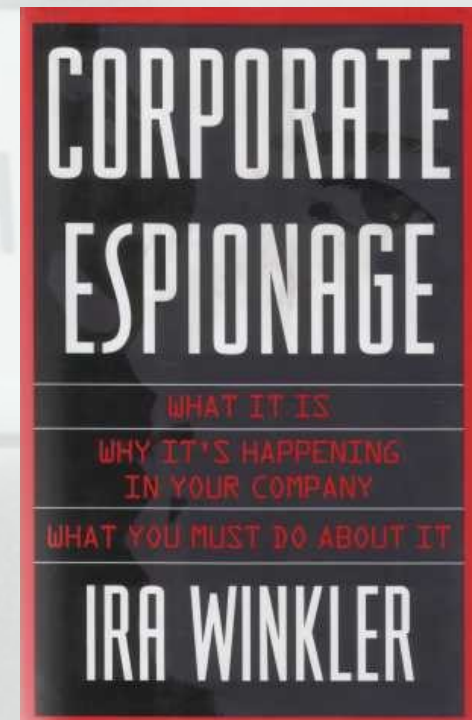
«Plahvatusi oli paar päeva ette valmistatud,» arvas saatkonna kõneisik. Paraboolantenn ja selle juurde kuulunud (samuti purunenud) kaablikapp olid osa süsteemist, mille kaudu nii ameeriklased kui ka inglased vahetasid oma peakorteriga kodeeritud telegramme.

3 - KII





Lutikad...



<http://cryptome.org/un-bug.htm>

Justkuidla@Võibollallaa

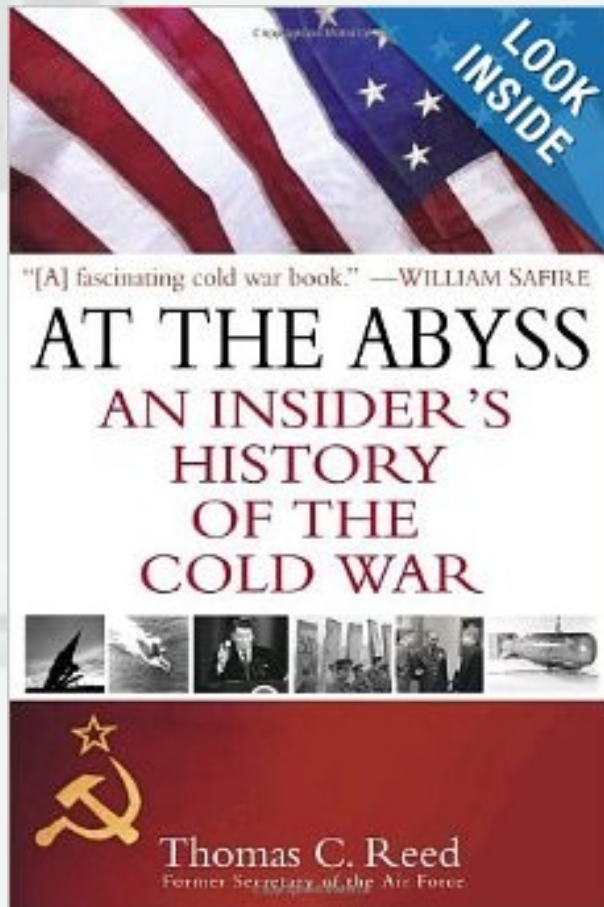
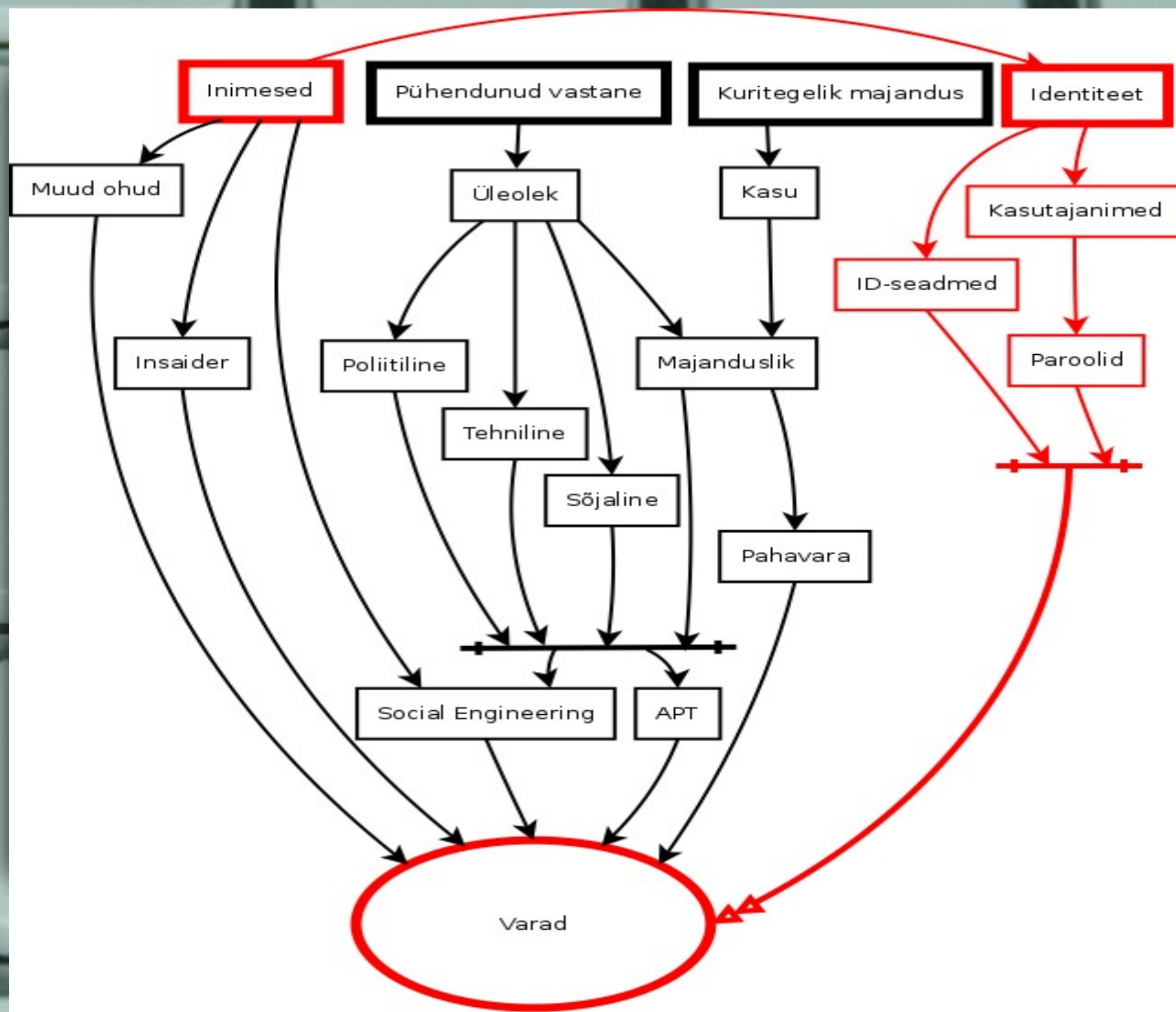


Таблица 2.6

Наименование объекта манипуля- ций	Место объекта или фокусной груп- пы по эффективности манипуля- ции общественным мнением для достижения цели				Сумма мест	«Среднее» место
	по сред- нему баллу	по Паре- то	по тур- нирной таблице	оценка пред- почте- ний		
Руководство фирмы	2	3	4	2	11	3
Группа высокопо- ставленных чинов- ников	3	1	2	1	7	1-2
Финансовое состоя- ние фирмы	1	2	1	3	7	1-2
Клиенты	4	4	3	4	15	4
Журналисты, освещ- ающие проблемы	5	5	5	5	20	5

Justkuidla@Võibollallaa





4 – arenenud keberühiskond



<http://flightlessbag.blogspot.com/>

Bugi - "Anttix1". Bugi?

Hr. Sertifitseerimiskeskus, mis teil lekib sealt?

Sellel lehel on võimalik jälgida, kuidas Sertifitseerimiskeskus AS-i poolt levitatav ID-kaardi tarkvara lekitab isikuandmeid: suvaline sait saab lugeda kaardilt nime ja isikukoodi ilma et kasutajat sellest kuidagi teavitataks.

Probleem on nii Maci kui Linuxi jaoks 29.10.2010 avaldatud "beetades", (<http://id.eesti.ee>) kui ka "ametlikes" Windowsi versioonides.

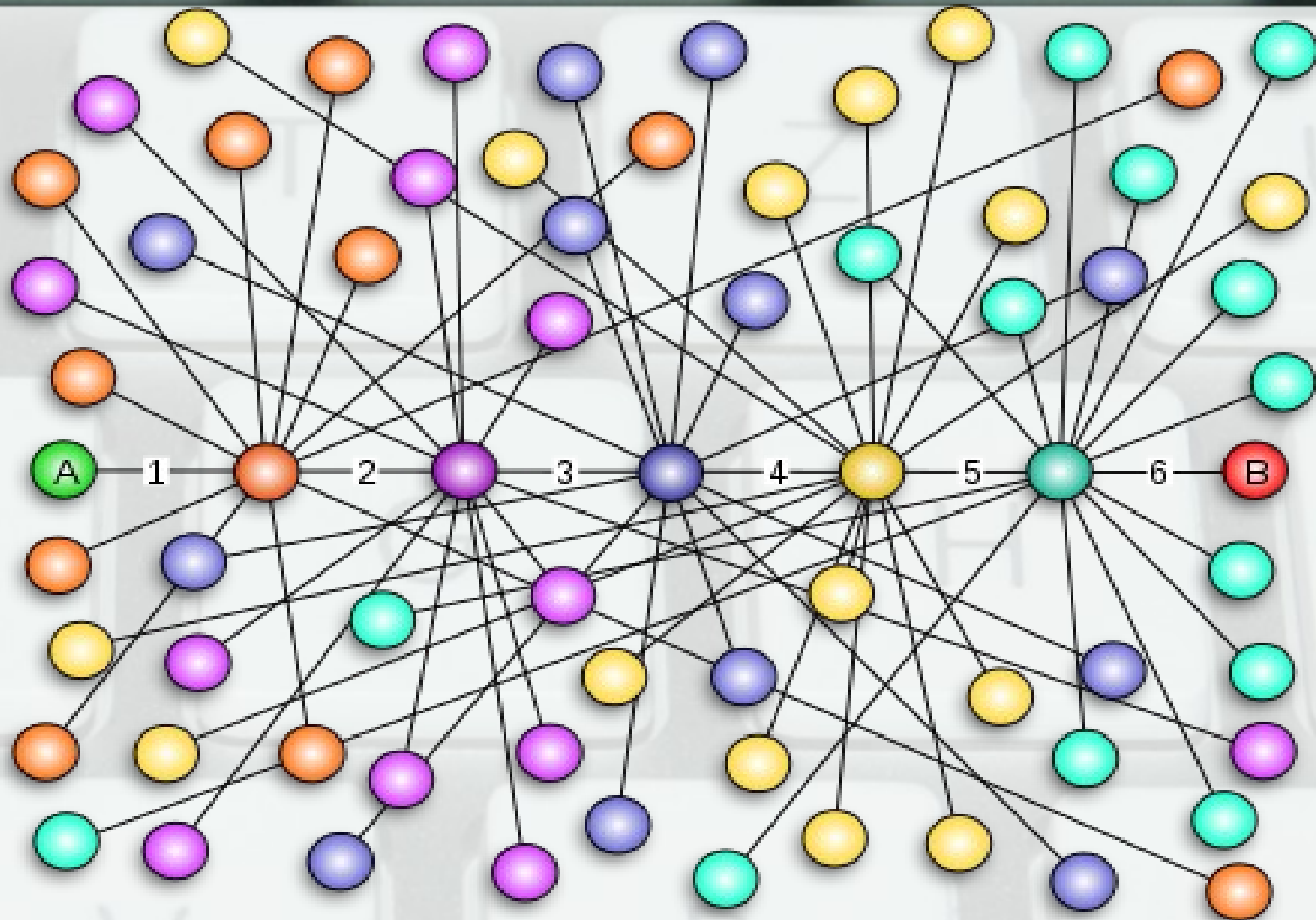
ID-kaardiga lähemalt tuttavad inimesed on sellele korduvalt tähelepanu juhtinud ja vabatahtlike poolt edasi arendatud tarkvaras (<http://esteid.googlecode.com>) on kasutajal võimalik end kaitsta: plugin keeldub tundmatule leheküljele isikuandmeid paljastamast ja näitab üleval servas kollast riba. SK versioonis on see "ebameeldiv" funktsionaalsus uuesti eemaldatud.

Tere ANTO VELDRE 36108142739

Viimati testitud 20.10.2010

Windows XP ID-Kaart 1.4.92 ID-kaardi draiver Firefoxile 0.8.8 Internet Explorer 8 Firefox 3.6.6

Linux esteidfirefoxplugin-3.0.BETA.739.171-1 Firefox 3.6.10



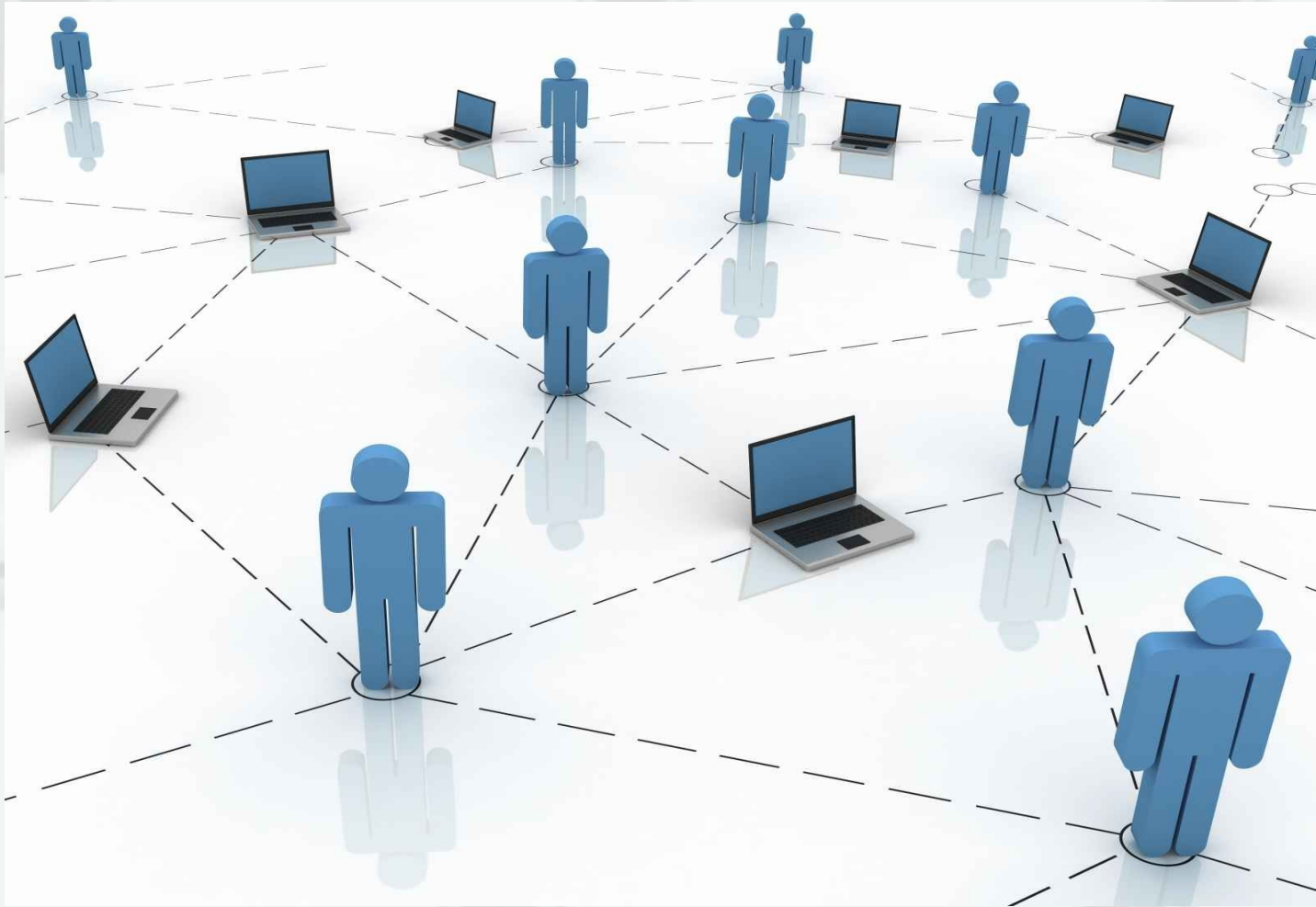
#friendofafriendofafriend

- http://en.wikipedia.org/wiki/Six_degrees_of_separation

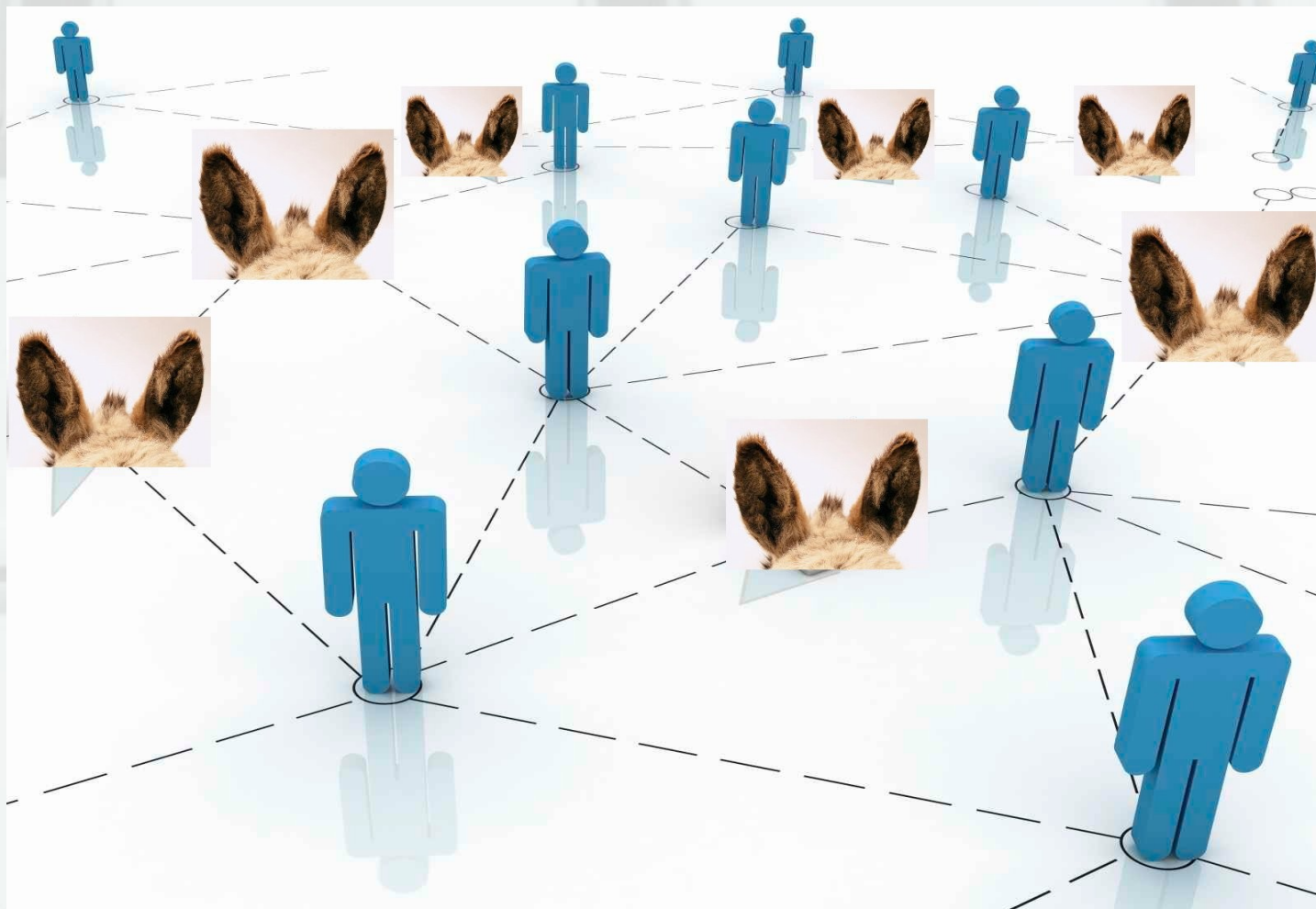
Suhtlus ürgajal

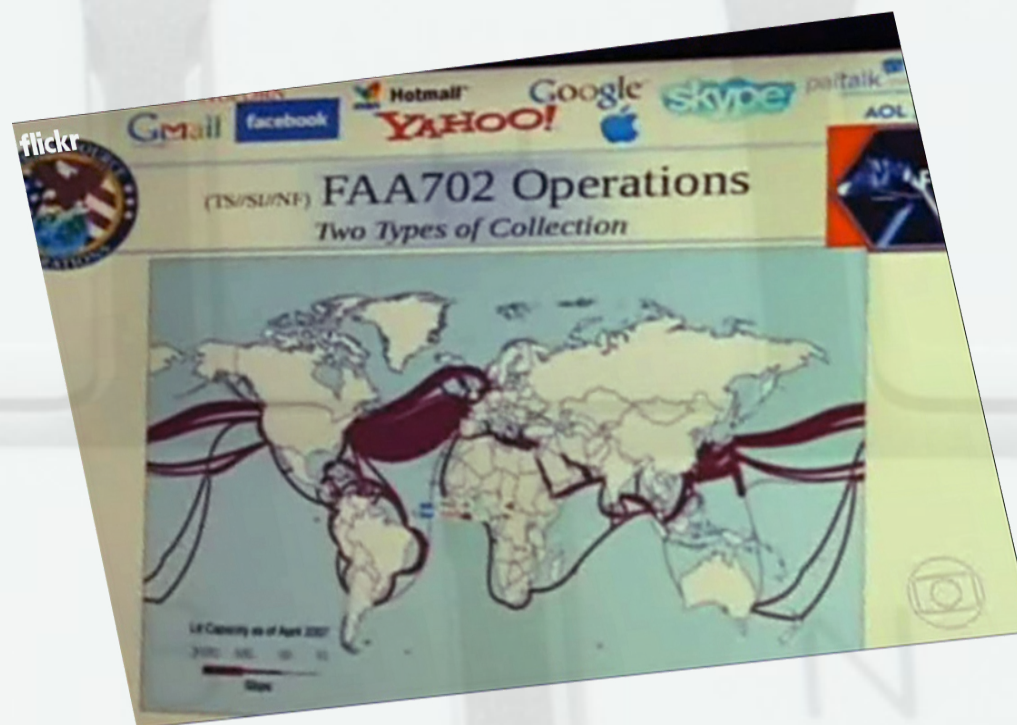


Suhtlus keberajastul



Kus on võimaluste lagi?





[194 pges.]

EUROPEAN PARLIAMENT



Session document

FINAL

A5-0264/2001

Part 1

11 July 2001

REPORT

on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))

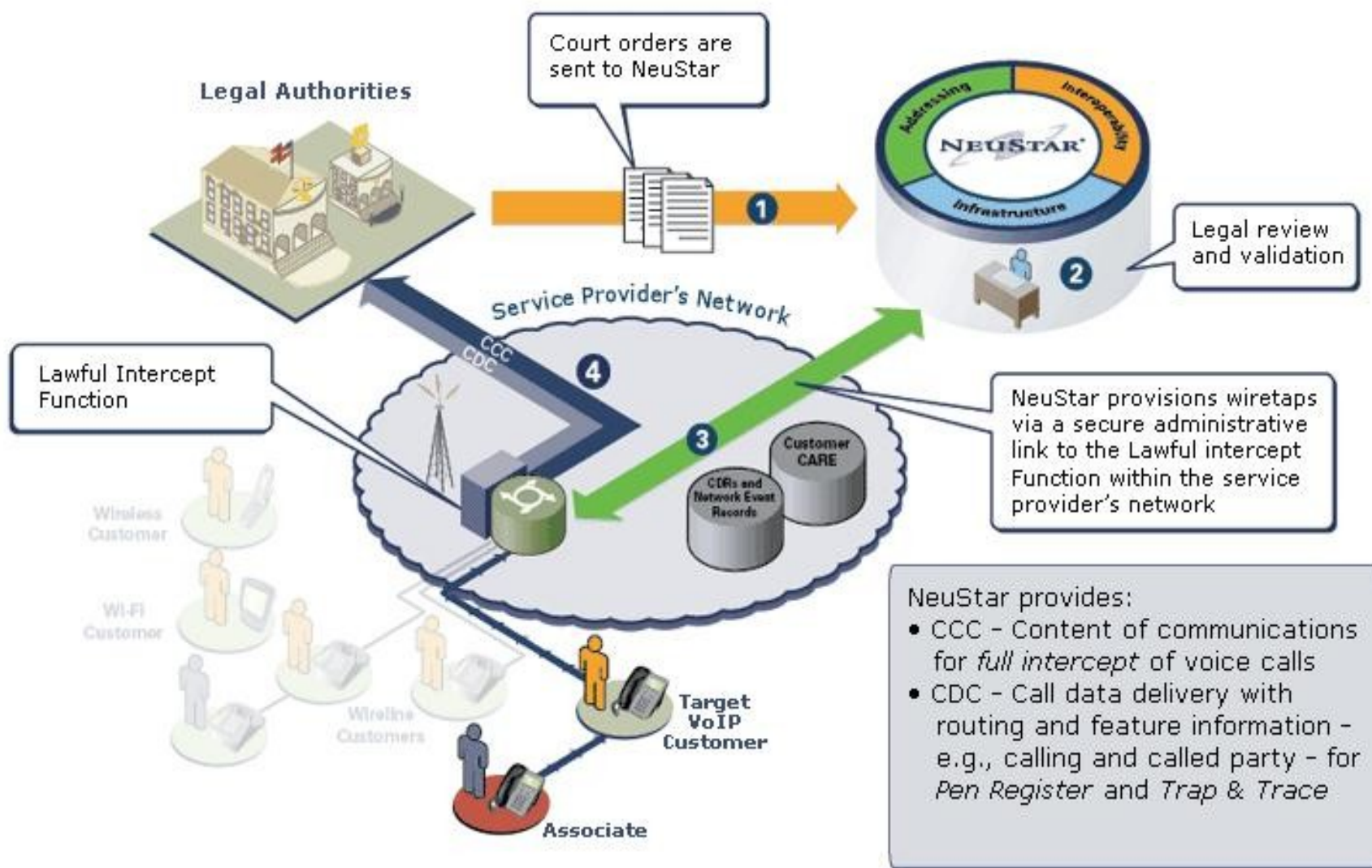
Part 1: Motion for a resolution

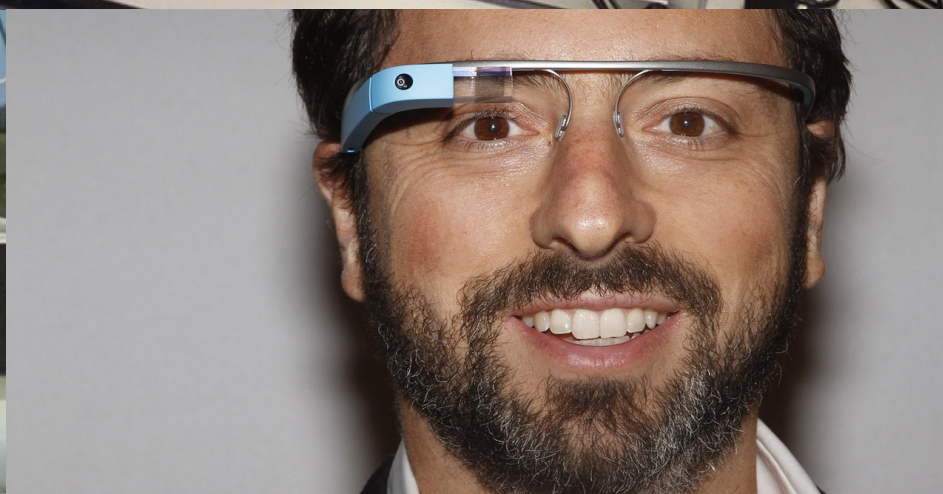
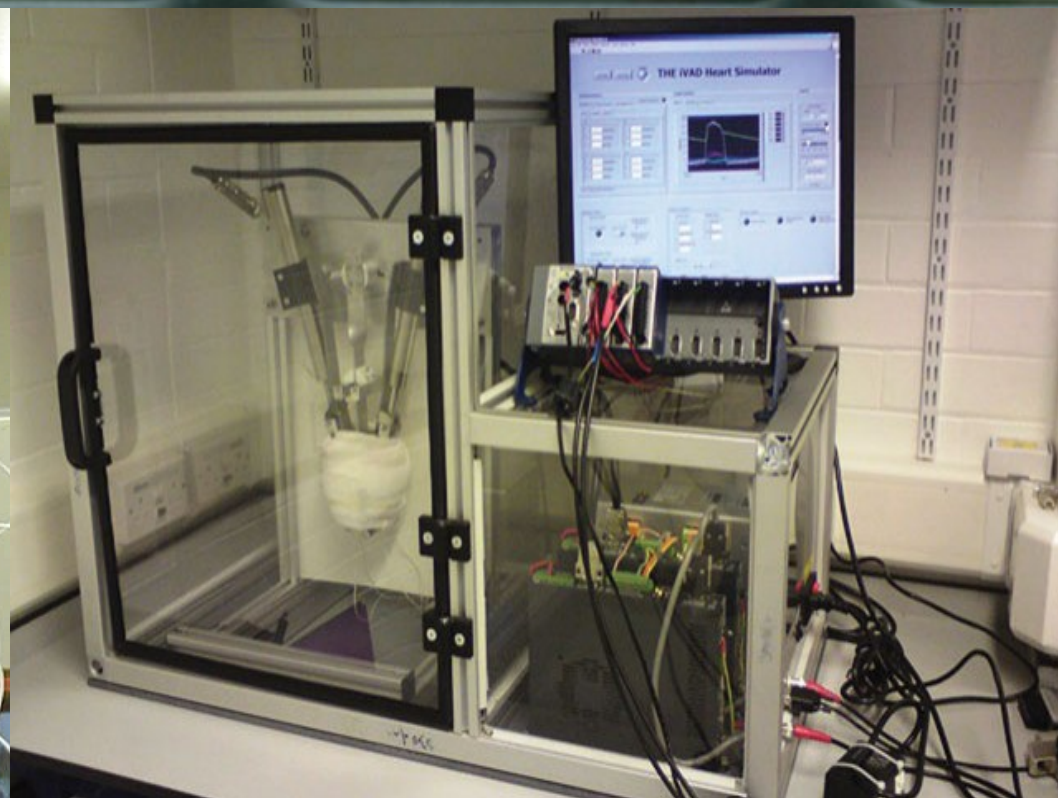
Explanatory statement

Temporary Committee on the ECHELON Interception System

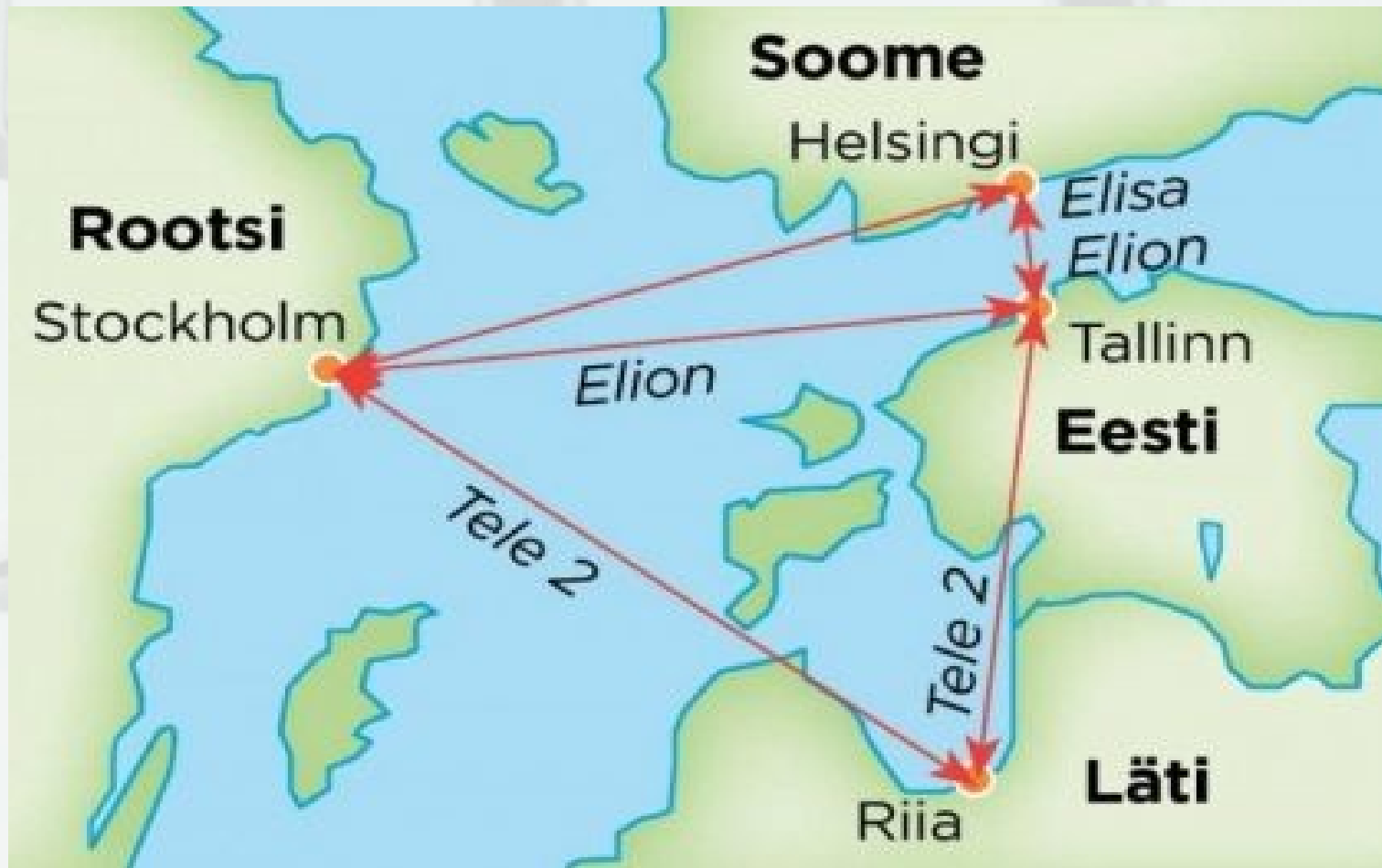
Rapporteur: Gerhard Schmid

Lawful Intercept of Communications





FRA?



<http://ekspress.delfi.ee/news/paevauudised/eestiudised/rootsi-luure-kuulab-eestlasi-pealt.d?id=27693951>



© 2013 Geek Culture



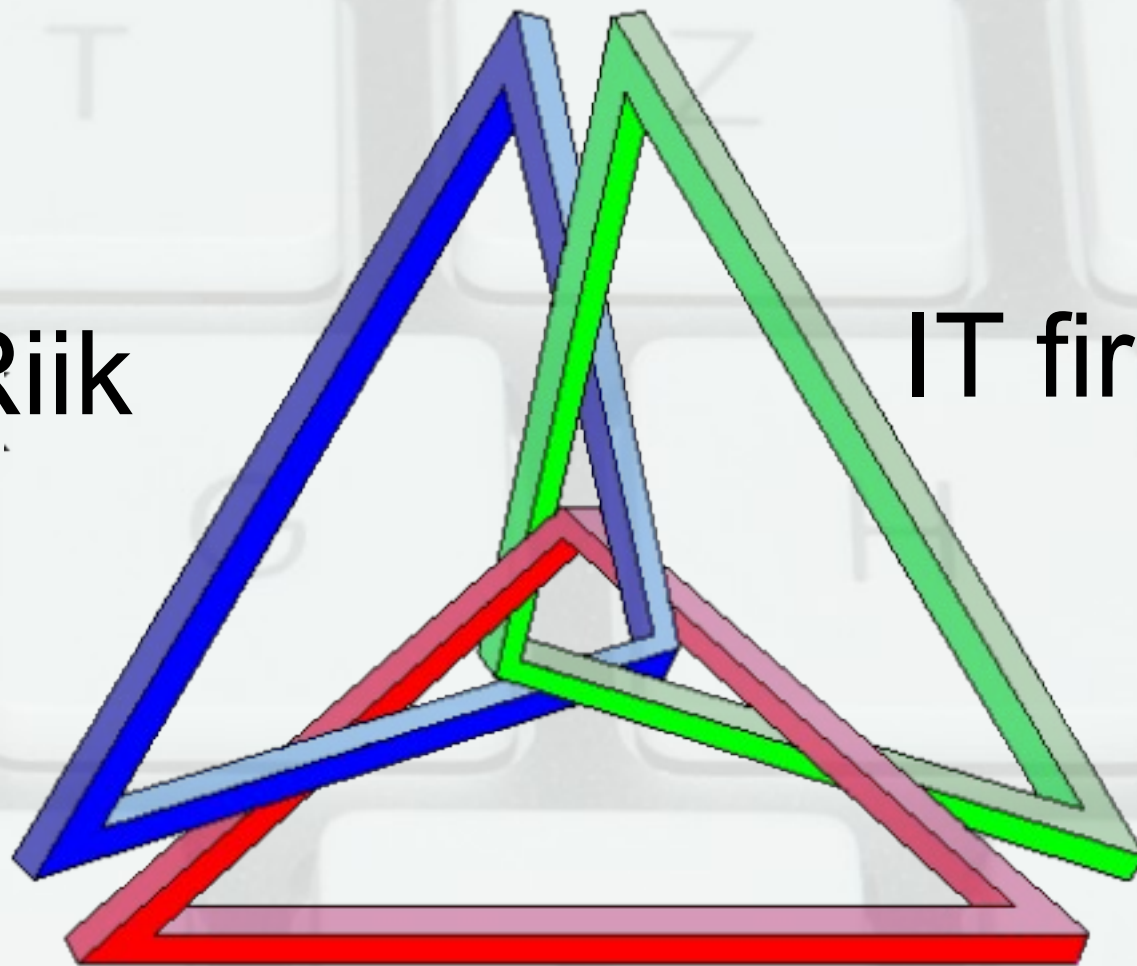
joyoftech.com

GrokLaw

- Viljandi poiss säutsus:
 - Kardinad on pesus. Tahaks o*. Satelliidid...
- GrokLaw: "On oht, et kui ma julgustan inimesi osalema, siis nad inkrimineerivad iseendid."
 - <http://www.groklaw.net/article.php?story=20130818120421175>
- UK pornofilter nõuab iseenda inkrimineerimist.
 - Porr?  **Yes**
 - Terroristlik materjal?  **Yes**

Riik

IT firmad



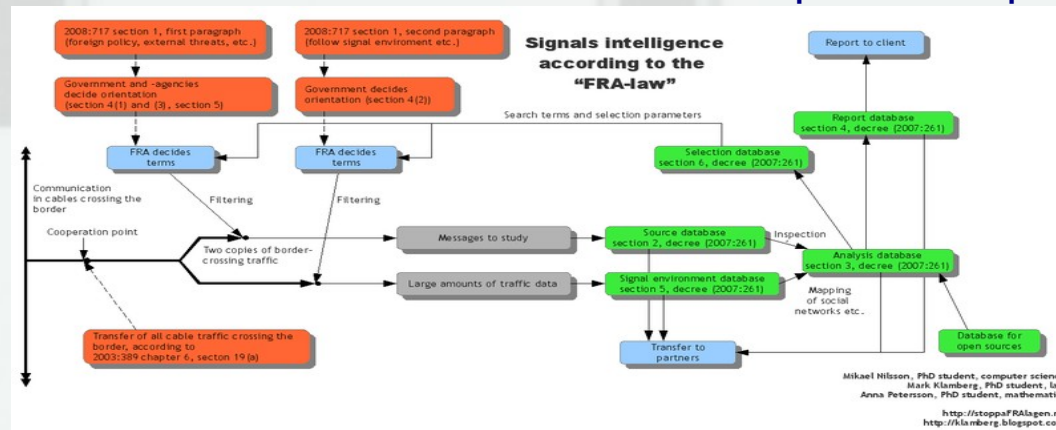
Inimesed



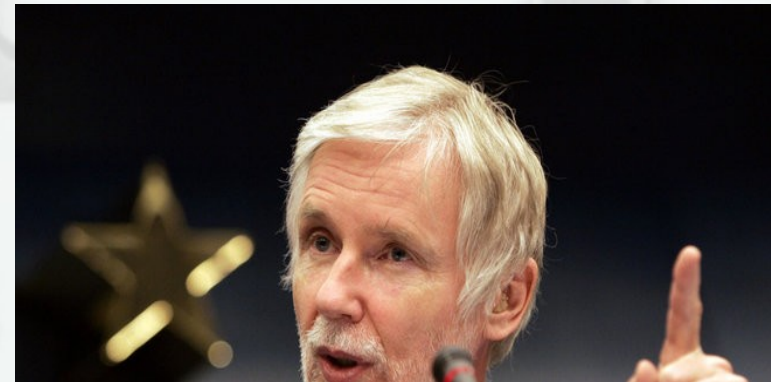
5 – Kuhu ja kuidas edasi?

Mis naabrid teevad?

http://en.wikipedia.org/wiki/FRA_law



- Finnish Information Security Cluster - Suomen tietoturvayhtiöiden case raportti #NSA #PRISM ohjelmasta



<http://fisc.fi/files/2013/09/CASE-Raportti-NSA-PRISM-ohjelmasta.pdf>

Moraali asemel

- PRISM näib infoturbeskandaalina, mida ta aga kindlasti ei ole.
- PRISM on üldinimlike demokraatlike väärtuste akuutne kriis, mille lahendamiseks sobiv aeg on pigem mööda lastud.
- Seekord on USA vaenlaseks mitte türann, paariariik või kurjategijad, vaid rahvas (sh omaenda rahvas) ning ajakirjanikud.
- USA kui riigi põhiväärtused on mõnusalt kahvlis.

Maarjamaa vaatepunkt

- Eesti dilemma seoses PRISM skandaaliga:
 - Meie suurim liitlane ja vabaduse tegelik garant on end mässinud põhiväärtusi hävitavasse globaalskandaali.
- Eesti on põhiväärtuste osas kahvlis veelgi mõnusamalt kui USA
- Kogukond & Piraadid vs ACLU & EFF?
 - Ärge lootkegi, et Eestis õnnestub põhiväärtuste alast diskussiooni vältida!!!

Kas maailm läks nüüd päris katki?

- Ei. Elu planeedil Maa jätkub. Aga.
- Ühiskonnas elamise reeglid ja mudelid tuleb viia vastavusse tehnoarengu ja küberajastuga.
- Vanamoodi enam riike pidada ei saa. Internet ei võimalda.
- Inimolend vajab pisukest puhvertsooni – privaatsust. Muidu võib tulla kodusõdu valitsuste ja kodanike vahel. OWS
- Globaalses maailmas võiksid 10 käsku kuidagi laieneda ka valitsustele, eriteenistustele ja tehnokorporatsioonidele. J.o.k.k.'i on *na pall'u saan'd*.

Moodsaim valitsemismudel

- Suurandmed
- Riigisaladus
- Tapadroonid

See on tehniliselt võimalik, kuid
sinnapoole ehk ei peaks püüdlema?
;-)

Muus osas aga ...

Eesti on jätkuvalt ID-lahenduste esirinnas,
igapäevane elu läheb edasi üha elliptilisemalt,
poes leiba ja piima jagub,
Sertifitseerimiskeskus vunkab ka kenasti,
eID süsteemi ekspordiga on alustatud.
Lähtekoodi muudkui avalikustatakse.

a.D. 2013

Muide, vaenlane ei maga

[+] E hääle jaotusalgorithm 30 minutit tagasi

e hääletussüsteem toimib lahutustehte põhimõttel. Kõik hääleõiguslikud kodanikud loetakse algselt e- hääletanuteks. Nendest lahutatakse valimispäeva jooksul paberhääletajad. Seejärel korrutatakse saadud tulemus soovitava hääletusprotsendi saamiseks sobiva koefitsendiga (näit 0,6) ja kustutatakse vajalik hulk e-hääli. Seejärel jagatakse e hääle jääk parteide vahel vastavalt sobiva valimistulemuse saamiseks vajalikule. Seejärel hävitatakse andmetöötlaste infokandjad.

-2 [thumbs down] [thumbs up] +3

▼ Vasta

[+] kvaliteedikontroll 0 sekundit tagasi

Ära aja lollust suust välja!

-0 [thumbs down] [thumbs up] +0

▼ Vasta



Tähh!

Küsida võib kõike!

materjal: xyz.ee / 2013-11-07-sk /