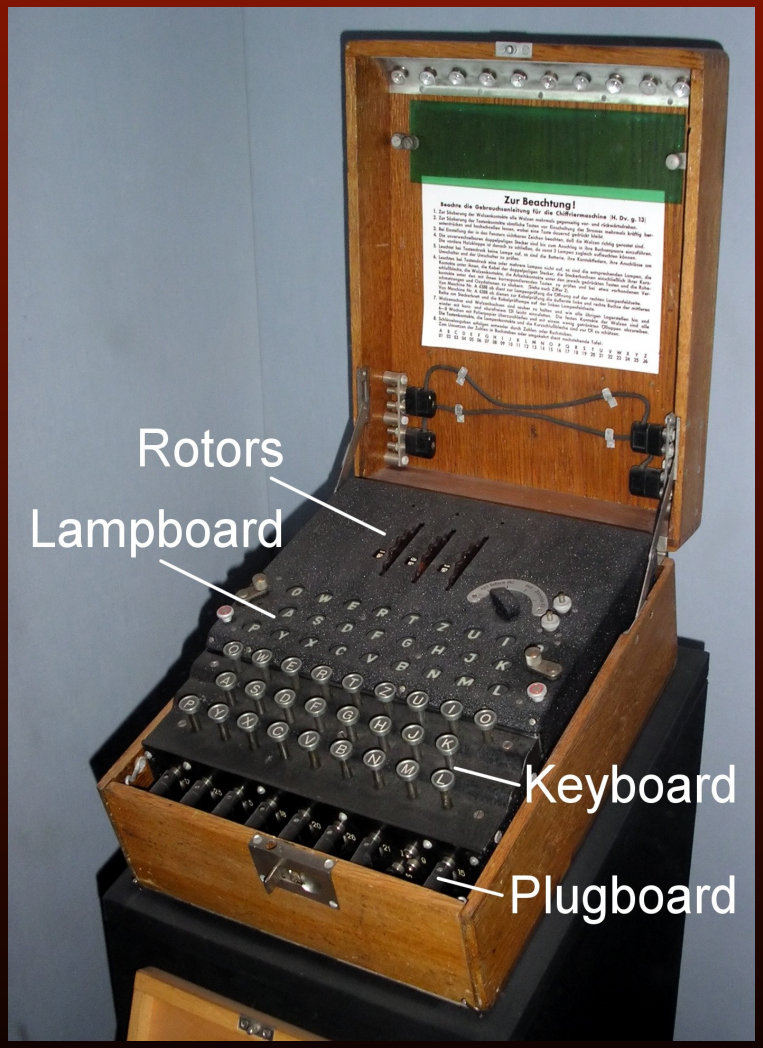
Suur Vend, infosõda ja võrguprivaatsus

TPK2012
Kaido Kikkas

Oli kord Enigma...

- Algselt tsiviilseade, a-st 1925 sõjalised edasiarendused
- Aitas Francol võita Hispaania kodusõja
- Saksa sõjajõudude peamine kodeerimis-vahend, eri versioonid armeel, laevastikul, õhujõududel ja luurel



http://upload.wikimedia.org/wikipedia/commons/3/3e/EnigmaMachineLabeled.jpg

Enigma lahtimuukimine

- Bletchley Park, Alan Turing ja Bombed
- Marian Rejewski ja kolleegid
- U559 koodiraamatud

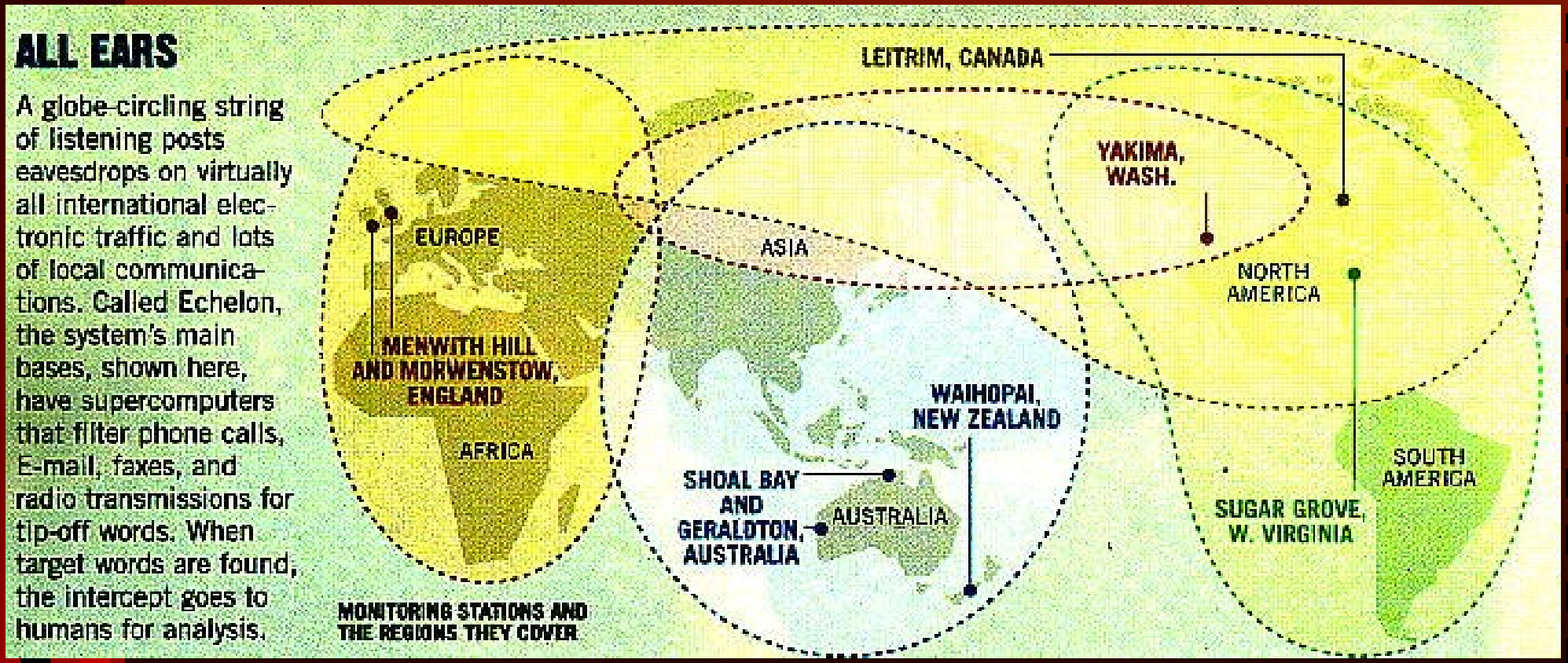
- Salastatud kuni 70-ndate lõpuni

http://upload.wikimedia.org/wikipedia/commons/6/6e/Bletchley_Park.jpg

UKUSA ja Neljapoolne Lepe

- 1947 – ingliskeelsed suurriigid (tegelikult viis – Austraalia läks kirja koos Uus-Meremaaga) sõlmivad Neljapoolse Leppe luureinfo vahetamise kohta (UKUSA e AUSCANZUKUS)
- Maailm jagatakse tsoonideks. Üks versioon:
  - Suurbritannia – Euroopa, NL Aasia-osa ja Aafrika
  - USA – Ameerika
  - Kanada – põhjapiirkonnad
  - Austraalia ja Uus-Meremaa - Okeaania

Teine versioon



http://cryptome.org/jya/echelon-bw.htm

ECHELON

- Algus eri allikate järgi 50.-60. aastatel
- Algselt mõeldud lühilaine-raadioside pealtkuulamiseks, hiljem vastavalt tehnika arengule ka muud kanalid (tava- ja mobiiltelefon, faks, erinevad internetiside liigid)
- Külma sõja aegadel eeskätt idabloki riikide vastu, hiljem aga on peamisteks märksõnadeks nn ”sõda terrorismiga” ning poliitiline ja tööstusspionaaž

Üks tuntumaid: Menwith Hill

http://upload.wikimedia.org/wikipedia/commons/e/e0/Menwith-hill-radomes.jpg

Luuretsükkel

- Kavandamine
- Info vaheltlõikamine ja kokkukogumine
- Info analüüs ja töötlemine
- Lõppjärelduste kokkupanek
- Tulemuste edastamine
- (tagasi algusse)

Mõned näited

- Project Shamrock – NSA kuulas a-st 1945 suuremat osa USA sidekaableid
- Lühilaineraadio pealtkuulamine erinevate jaamade abil (UK, Küpros, Itaalia, Türgi). A-st 1945, 80-ndatel hakkas taanduma
- Kaugraadioside pealtkuulamine satelliitide abil a-st 1968 (Canyon –satelliidiseeria 1968-77)
- Merealuste kaablite pealtkuulamine (Operation Ivy Bells; USS Halibut 1971)
- Interneti pealtkuulamine alates 80-ndatest

Mõned kasutusnäited

- 1993 – eurooplaste ühisfirma Panavia lennukitehingut Saudi Araabiaga jälgitakse USAst väga põhjalikult
- 1994 – prantslaste Thomson CSF kaotab Brasiilias radaritehingu USA Raytheonile
- 1995 – USA McDonnell-Douglas lööb eurooplaste Airbusilt üle Saudi Araabia lennukidiili (NSA kuulas telefone pealt)

Teine näide: Suur Hiina Tulemüür

- Tuntud ka nime ”Kuldne Kilp” all
- Hiina võimude poolt loodud riiklik võrgutsensuuri- ja jälgimissüsteem
- Kogu rahvusvaheline võrguliiklus käib läbi spetsiaalsete lüüside, kus lisaks blokeerimisele tegeldakse ka aktiivse nuhkimisega
- Tugineb suurel määral Lääne tehnoloogiale!
- Asi on karm: äärmuslikul juhul võib Internetis valede asjade tegemise eest kuuli saada
- Paradoks: Hiina on maailma spämmerite esireas...

Suured Vennad omavahel

- Sõdimine infoajastul:
  - riikidevaheline sõda => kuritegevus ja terrorism
  - mittesurmavad meetmed ja eriüksuste (vs massiarmee) kasutamine omandavad suurema tähtsuse
  - tahte, juhtimise ja teadmiste tähtsus ja osakaal kasvavad
  - rahvusvahelise massimeedia ja psühho-loogilise sõja tähtsus kasvab
  - sõjalis-tehniline revolutsioon, “kuuenda põlvkonna sõjapidamine”

Sõjapidamise kuus põlvkonda (kindralmajor V. Sliptšenko järgi)

- 1. orjanduslik ja feodaalühiskond, primitiivsed tehnoloogiad
- 2. püssirohi, sileraudsed musketid, suurtükid
- 3. vintraudsed püssid ja suurtükid, suurem tulejõud, -kiirus, -täpsus
- 4. automaatrelvad, soomukid, lennukid, sideseadmed, võimsad transpordivahendid
- 5. põlvkond - tuumarelv
- 6. suunatud energia, automatiseeritud täpsusrelvad, elektroonika, andmeside, kosmosesõda. Vastase territooriumi pole vaja hõivata. Õhujõud ja -kaitse, laevastik, elektrooniline sõda

Kübersõda

Infosõda kitsamas mõttes – desinformatsiooni levitamine (N: 2007 üritasid venelased teha “valgeid sukkpükse” ka Internetis)

- Spionaaž – vastase järel nuhkimine IKT vahenditega (Titan Rain, Moonlight Maze)
- Sabotaaž – üha enam kriitilist taristut on võrkepidi haavatav (vahel ei pea isegi võrku olema – vt Stuxneti juhtumit)

Veri on paksem kui vesi

- … ja vendi (ka suuri) peab aitama
- Partisanisõja uus tulemine
  - Hiina punahäkkerid (Titan Rain 2003, Operation Aurora 2009)
  - Vene rühmitused (Moonlight Maze 1998)
  - Iisrael/Palestiina, India/Pakistan, Korea...
  - Eesti (KKL)?
- Väga oluliseks muutub kriitilise massi piisavalt väljaõpetatud ja indoktrineeritud tavakodanike olemasolu

Kas Suur Vend on paratamatus?

- Nagu juba korduvalt öeldud, 100% turvalisust ei ole olemas
- 100% privaatsust ka ei ole (kui tehnoloogia peab, siis tuleb probleem klaveri ja tooli vahel)
- On aga olemas erinevaid abinõusid Suure Venna segamiseks

Interneti tagakülg

- Dark Internet (*dark addresses*)
- Deep Web
- Darknet
- Freenet
- Tor
- I2P

Dark Internet

- Aadressid, mis on tavavõrgust kättesaa-matud
- ”Interneti nurgatagused”, mis erinevatel põh-justel jäid võrgu arengust maha – üks suur põhjus on salastatus/militaarotstarve (MILNET USAs)
  - MILNET oli algse ARPAneti osa, mis 1983. aastal turvakaalutlustel eraldati, ent jäeti alles lüüsid, mis vahendasid näiteks e-posti
  - MILNET => Defense Data Network => NIPRNET – aga mõned osad ”jäid rongist maha”
- Tulemus – nurgatagused, kuhu saab ligi vaid 1337 seltskond

Deep Web

- Süvaveeb (*contra* pinnaveeb e. Surface Web) – see osa veebist, mida otsimootorid ei leia
- Kordades suurem kui pinnaveeb. Moodustavad näiteks
  - Dünaamiliselt loodav ja pidevalt muutuv materjal (paljud veebiportaalid)
  - Tagasiviideteta lehed, kuhu ei viita ükski leht
  - Lehed, mis otseselt keelavad indekseerimise
  - Erinevad privaatlehed
  - Materjal, mille vormingut ei osata indekseerida
- Piir hägustub, üha enam asju ”tuleb alt üles”

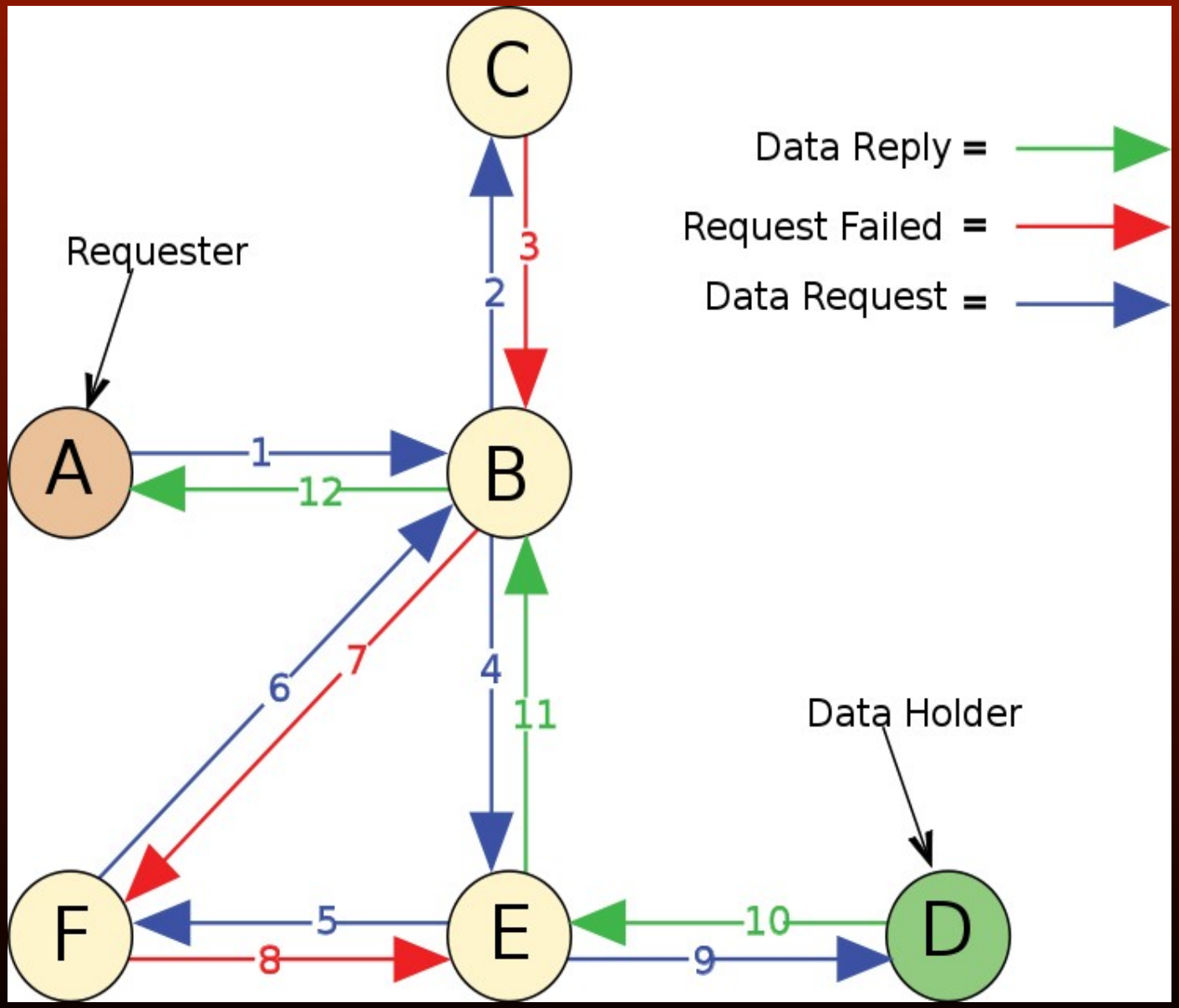
Darknet

- Tähendab üldisemas mõistes kinnist, ”ainult sõprade” võrku (vrdl usaldusvõrgustikud!)
- Kasutatakse tõsisemates anonüümsuhtluse kanalites
- Teine aspekt – P2P failijagamissüsteemid, mis toimivad samal põhimõttel

Freenet

- Sõnavabadust ja anonüümsuhtlust edendav tarkvaraprojekt, Ian Clarke 2000
- Eri turvalisusastmed, kaks peamist režiimi:
  - Opennet – ühendust võetakse ka võõrastega
  - Darknet – ühendus ainult usaldatavate inimestega

Freeneti päringuskeem

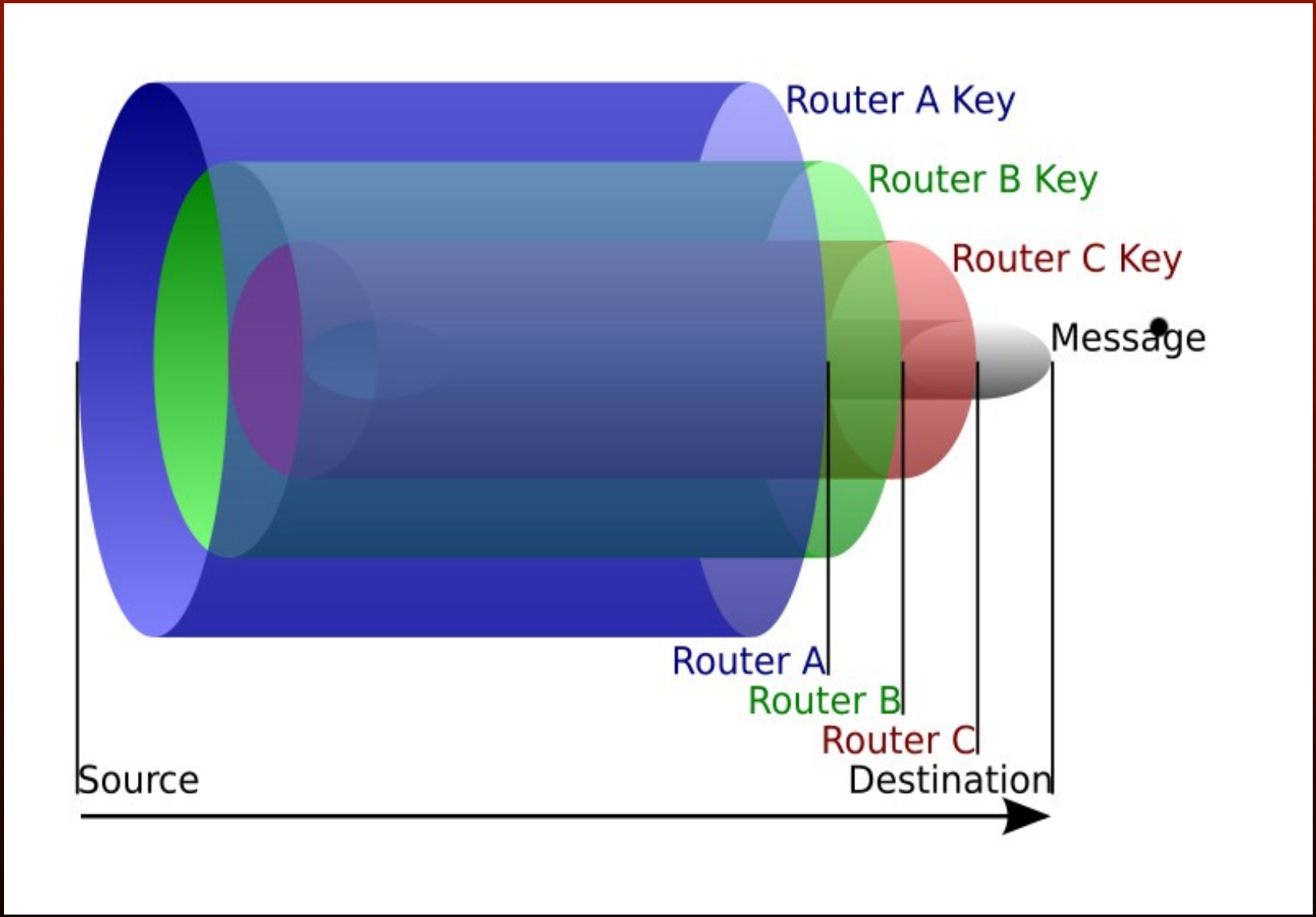


http://upload.wikimedia.org/wikipedia/commons/a/ae/Freenet_Request_Sequence_ZP.svg

”Sibulruutimine”

- *Onion routing*
- Mitmekordselt krüpteeritud sõnum läbib edastusserverite ahela, iga server eemaldab ühe krüptokihi (nagu sibula koorimine)
- Põhimõte pärineb aastast 1999
- Eraldi võttes ei ole ”sibul” privaatsuse tagamiseks piisav – põhiliselt muudab keeruliseks NII saatja KUI saaja tuvastamise
- Haavatav erinevate rünnakutega

”Sibulruutimise” skeem



- http://upload.wikimedia.org/wikipedia/commons/e/e1/Onion_diagram.svg

Tor

- Aastast 2004
- Anonüümsusvõrgustik, sisuliselt ”jälgede segamise masin”
- Sõnum on haavatav enne ja pärast Tor'i võrku jõudmist, lisaks on võimalik liiklusanalüüs kogu teekonna nägemise korral. Varem esines ka nimeserverilekkeid

I2P

- *Invisible Internet Project*
- ”Küüslaukruutimine” (!) - sõnumeid krüpteeritakse suurema komplektina, takistamaks liiklusanalüüsi
- Pseudonüümne krüpteeritud *end-to-end* sidega sõnumivõrgustik, on loodud ka rida muid rakendusi (failivahetus jne)

Tava-Interneti jaoks

- *Porn...* ups, *Privacy Mode* uuemates brauserites
- Anonüümne e-post
- Anonüümsusserverid veebi jaoks (*proxy*)
- Lisaks muidugi tavaline terve mõistus

Anonüümne remailer

- Johan "Julf" Helsingius ja anon.penet.fi (nn tüüp 0, sisuliselt pseudonüümne edastaja)
    - Pakkus ano- ja pseudonüümset meiliteenust
    - Kasutas seostetabelit
    - Krüpteerimist ei olnud
- Pandi kinni peale suurt kisa 1996. aastal (Londoni *Observer* süüdistas JH-t umbes 90% Interneti lasteporno edastamises), suur roll oli saientoloogidel

...

- Cypherpunk-tüüpi edastajad (tüüp 1)
  - Jäik anonüümsus, mitte mingit vihjet kasutajale – vaid ühesuunaline edastamine
  - Krüpteeritud sõnumi saatmine (PGP või GPG)
  - Aheledastus läbi mitme serveri - iga lüli "näeb" vaid eelmist

...

- Mixmaster-klass (tüüp 2)
  - Vajab allalaetavat tarkvara
  - Edastab sõnumid ühtse suurusega pakkidena, segab nende järjekorra ja krüpteerib
  - Võimaldab kahepoolset sidet
- Mixminion-klass (tüüp 3)
  - Eelmise laiemate võimalustega edasiarendus, krüpteerimine toimub iga edastussammu juures eraldi
- Vt ka http://www.andrebacard.com/remail.html

Anonüümne surfamine

- Veebis saab kasutada anonüümsus*proxy*'t, mis lõikab ära veebiserverisse mineva kasutajainfo (proxify.com, snoopblocker.com)
- Firmad nagu http://www.ultimate-anonymity.com - pakub nii anonüümset veebi, meili kui ka P2P-teenust
- Jällegi kahtpidi suhtumine

Steganograafia

- Kasutusel juba vanal ajal – salatintidena saab kasutada piima, sidrunimahla, kokakoolat, kehavedelikke jpm
- Digiajastul tähistab sõnumi peitmist mingit muud liiki faili sisse (foto, heliklipp, tehniline joonis vmm)
- Näide: muudame fotol iga 50-nda piksli värvust, pannes selle tähistama mingit kindlat sümbolit

Näide Wikipedia artiklist steganograafia kohta (lugege!)

=>

http://upload.wikimedia.org/wikipedia/commons/4/4e/StenographyOriginal.png,
http://upload.wikimedia.org/wikipedia/commons/1/1b/StenographyRecovered.png

Failidel on vahe

- Kes tahab mõnd eespoolmainitud teenust turvaliselt kasutada, peaks piirduma ainult puht-tekstifailidega!
- Võrdluseks: MS Office'i dokumendid sisaldavad vaikimisi päris suurt hulka infot. Vt http://office.microsoft.com/en-us/excel-help/remove-hidden-data-and-personal-information-from-office-documents-HA010037593.aspx

Kokkuvõtteks

- Sama seis kui turvalisuse, autorikaitse ja paljude muude valdkondadega – pidev vägikaikavedu
- Kodanike jälgimine on väga vana ja laiaulatuslik tegevus
- Kui see ei meeldi, saab seda raskemaks teha
- Hinnaks on mugavus
- 100% garantiid ei ole!

Kogu lugu!