
Finnish Communications
Regulatory Authority
CERT-FI
CERT role in
Finnish Response Plan
ENISA @Athens
2008-05-29
Erka Koivunen
Head of CERT-FI
Finnish Communications
Regulatory Authority

CERT-FI

in a nutshell

CERT-FI – Finnish national CSIRT authority

- CERT == ~~Computer~~ Coordinated Emergency Response Team
  - **coordinated** response to information security incidents
  - **response** often reactive on the basis of a stimulus
  - Proactive **information gathering**
  - Processing and dissemination of **confidential** early warning information
  - function also known as CSIRT, PSIRT, IRT..
- CERT is **not**
  - an anti-virus company
  - a vulnerability researcher
  - a criminal forensics investigator
  - responsible for Your information security

CERT-FI – Finnish national CSIRT authority

The duties of the Finnish Communications Regulatory Authority are:

*1) to **supervise compliance** with this Act and any provisions issued under it, unless otherwise provided in section 32;*

*2) to **collect information on violations of and threats to information security** in respect of network services, communications services and value added services, and on significant faults and disruptions in such services;*

*3) to **investigate violations of and threats to information security** in respect of network services, communications services and value added services, and significant faults and disruptions in such services; and*

*4) **publicize information security matters**.*

Act on the Protection of Privacy in Electronic Communications (516/2004) section 31

CERT-FI – Finnish national CSIRT authority

Essential services

- National Point of Contact for incident reports
- Incident Handling
- National Information Security Situation Awareness Service
- Vulnerability Coordination

On duty 24/7/365

VAROITUS!

13.10.2007 07/2007 **Suomalaisia verkkopalveluiden käyttäjätunnuksia sisältäv tiedosto verkossa**

Tiedostossa vaikuttaa olevan noin 80000 suomalaisen internet-verkkopalvelun käyttäjien käyttäjätunnustiedot. Erityisesti yhteisöpalvelujen käyttäjien syytä o...

Näytä kaikki varoituk

Tietoturva nyt!

19.10.2007 12.41 **Salasanatiedostotapaus - tilannepäivitys 19.10.**

On käynyt ilmi, että osa salasanatiedostotapauksen alkuvaiheessa julkisuuteen toimittamistamme hyödynnettyjä haavoittuvuuksia koskevista tiedoista oli puutte...

18.10.2007 17.50 **Ruotsissa murrettu ja muutettu www-sivustoja**

Uutislähteiden mukaan Ruotsissa on viime päivinä nähty tavallista enemmän tapauksia, joissa www-sivustojen sisältöä on muutettu luvattomasti. Www-sivustojen ...

18.10.2007 17.03 **Salasanatiedostotapauksen poliisitutkinta eteni**

Keskusrikospoliisi on julkaissut ...

Näytä kaikki kirjoituk

Haavoittuvuudet

19.10.2007 142/2007 **Haavoittuvuuksia Mozilla Thunderbird -ohjelmistossa**

Mozilla Thunderbird -ohjelmistosta on löydetty haavoittuvuuksia, joit hyväksikäyttämällä hyökkääjän voi olla mahdollista suorittaa kohdejärjestelmässä omia ...

19.10.2007 141/2007 **Haavoittuvuus Mozilla SeaMonkey -ohjelmistossa**

Mozilla SeaMonkey -ohjelmistosta on löydetty haavoittuvuuksia, joita hyväksikäyttämällä hyökkääjän voi olla mahdollista mm. saada halt kohdejärjestelmän...

19.10.2007 140/2007 **RealPlayerin ActiveX-haavoittuvuus**

RealPlayer-ohjelmistoon liittyvästä ActiveX-komponentista on löydett puskurin ylivuotoon perustuva haavoittuvuus, joka mahdollistaa hyökkääjän ohjelmakoodin...

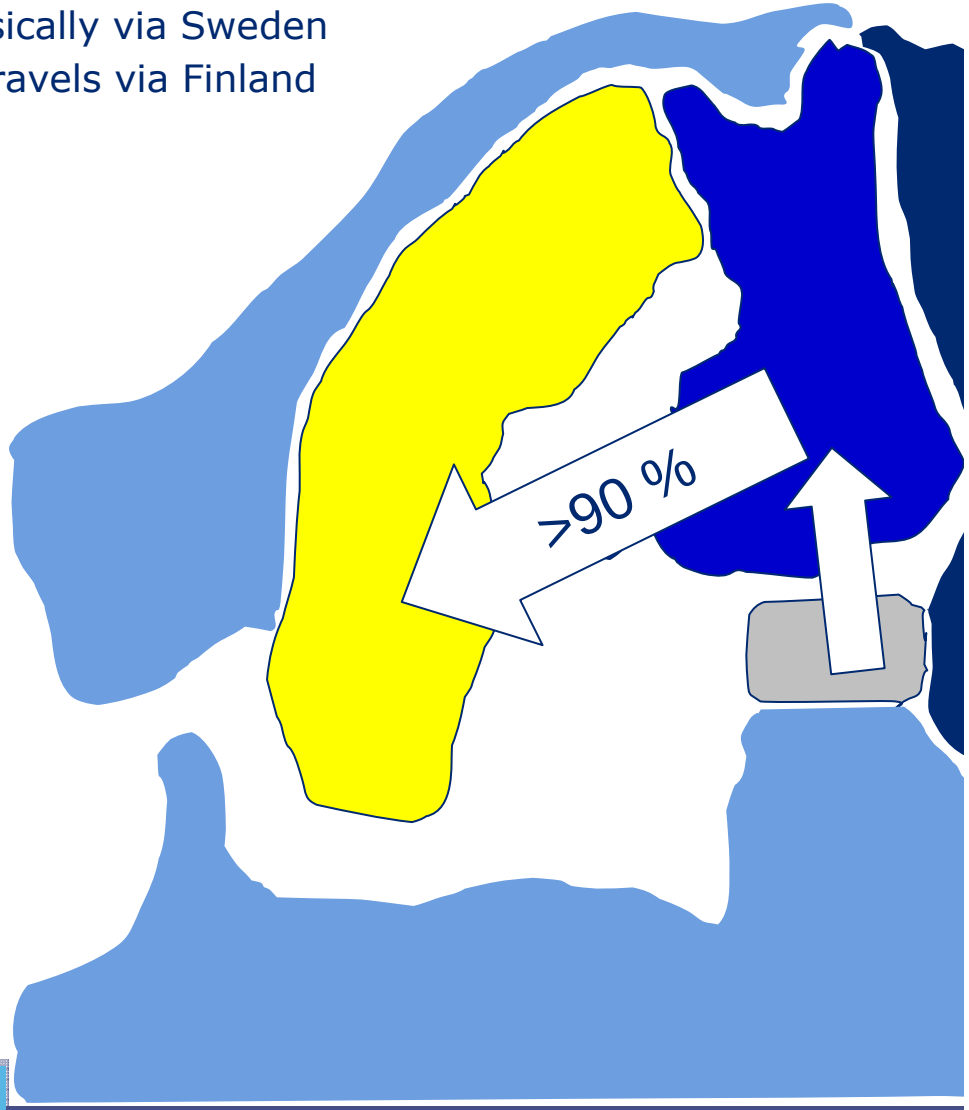
Näytä kaikki haavoittuvuu

CERT-FI

as a part of the national response plan

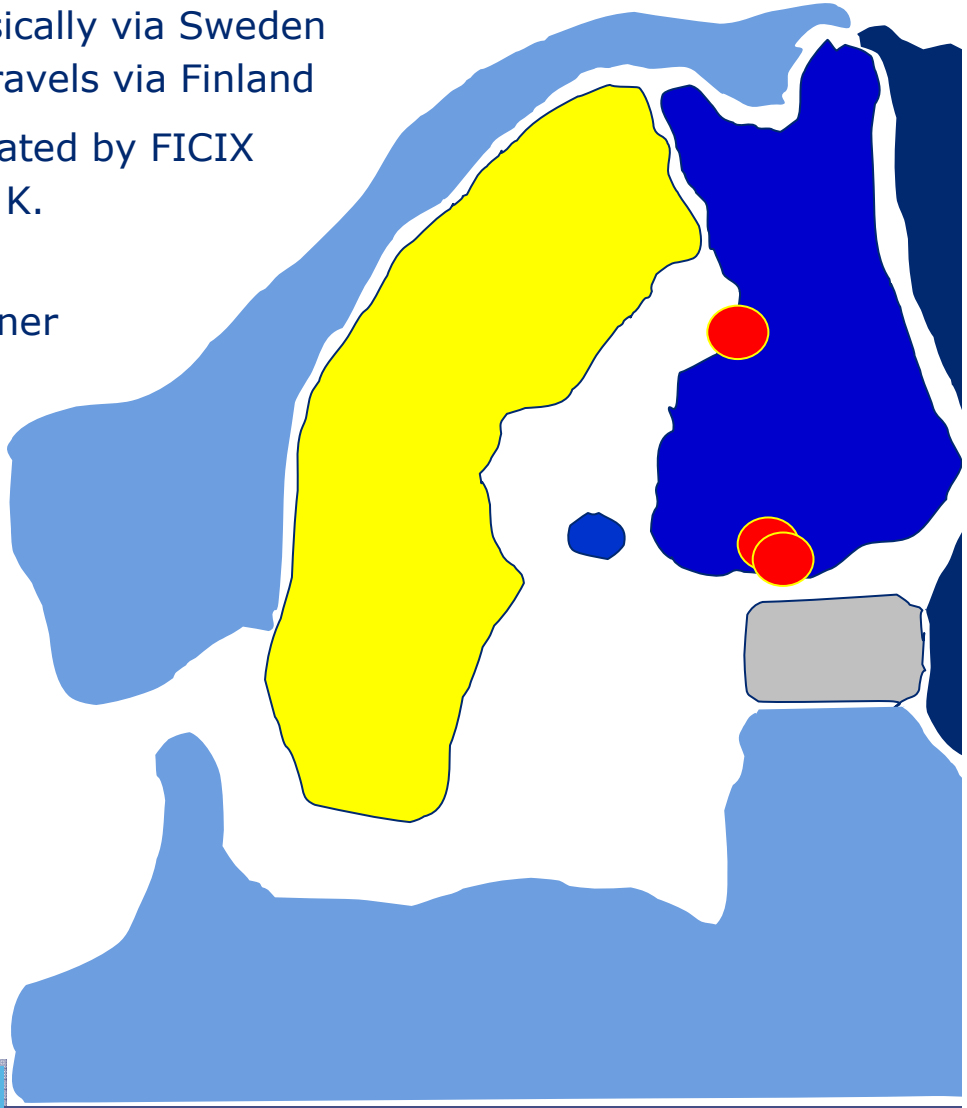
About Finnish public communication networks

- A main route to the ”The Internet” goes physically via Sweden
  - NB: Portion of traffic to/from Estonia travels via Finland



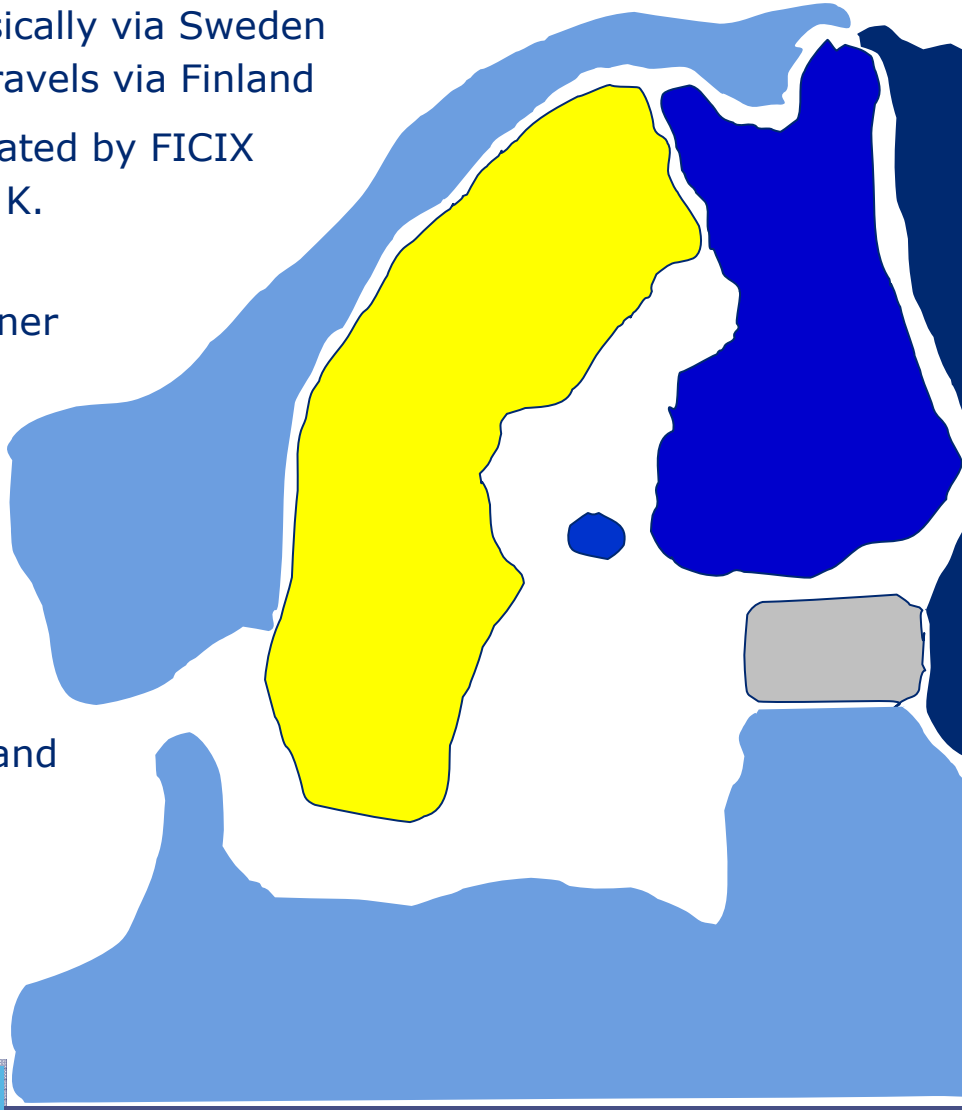
About Finnish public communication networks

- A main route to the ”The Internet” goes physically via Sweden
  - NB: Portion of traffic to/from Estonia travels via Finland
- Three internal Internet Exchange nodes operated by FICIX
  - also holds copies of DNS roots I, J and K.
- .FI TLD managed and operated by FICORA
  - implemented in highly distributed manner



About Finnish public communication networks

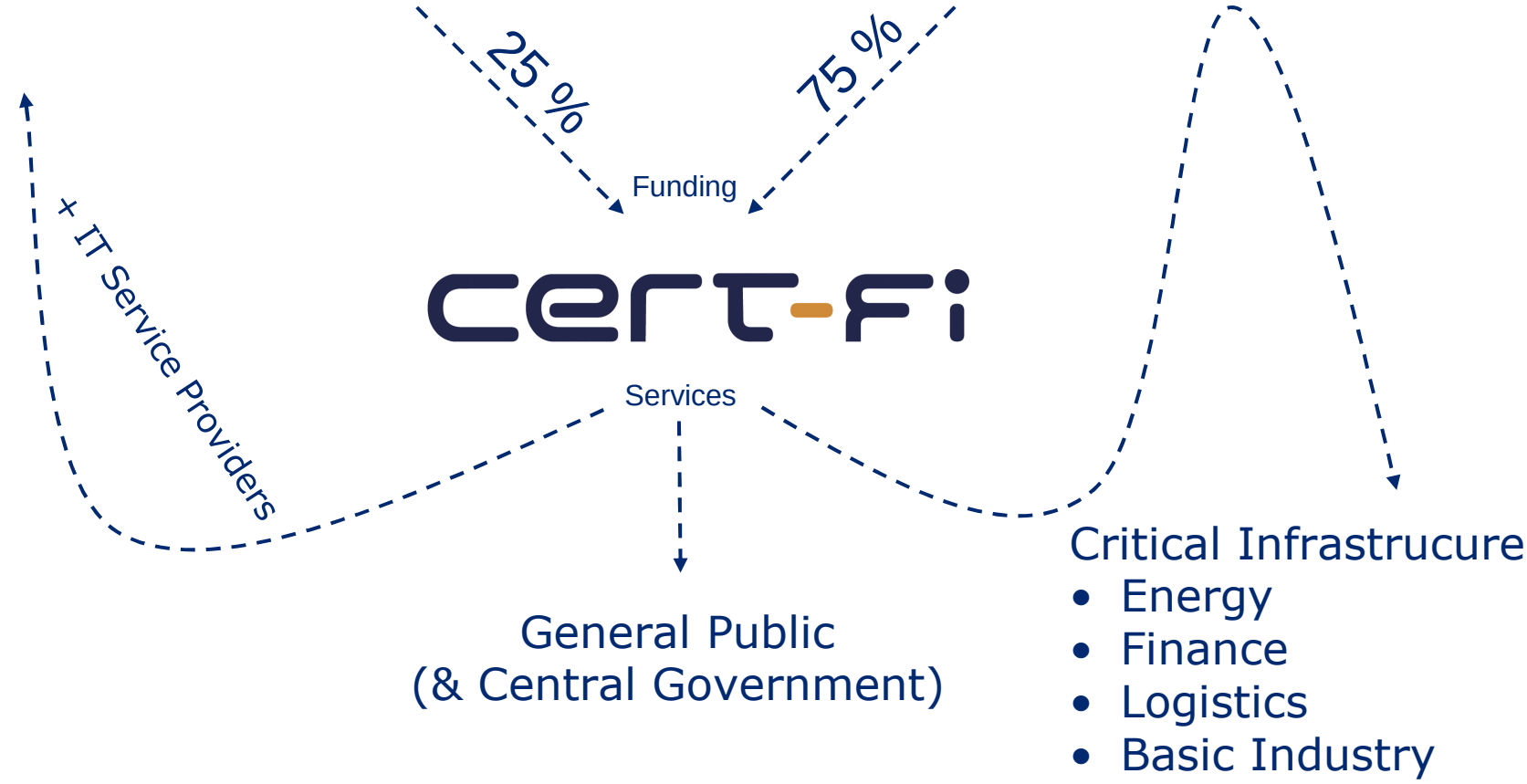
- A main route to the ”The Internet” goes physically via Sweden
  - NB: Portion of traffic to/from Estonia travels via Finland
- Three internal Internet Exchange nodes operated by FICIX
  - also holds copies of DNS roots I, J and K.
- .FI TLD managed and operated by FICORA
  - implemented in highly distributed manner
- Genuine competition in carrier networks
  - ..at least in and between major cities
  - access networks a problem in rural areas
- Major network operators are in international ownership
  - ongoing debate: which parts of the network and services should reside in and be operated from within Finland
  - ongoing debate: prioritised customers vs. costs compensation schemes
- Government functions largely relying on commercial network providers



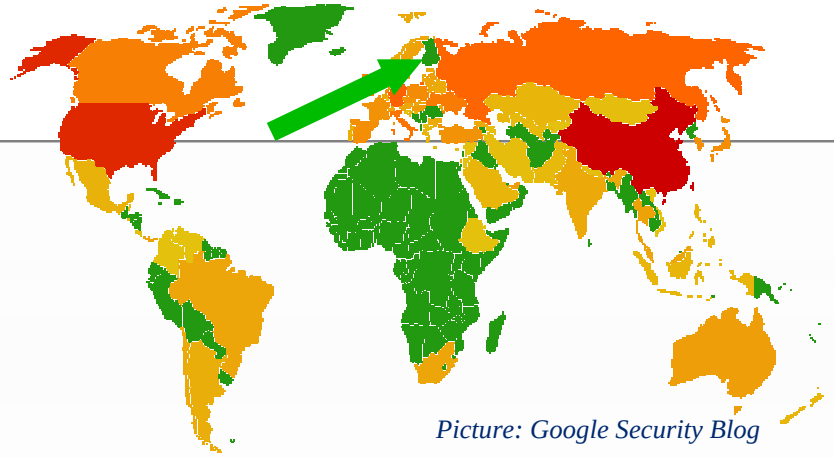
CERT-FI Funding and Constituency

Telecommunications operators

National EMERGENCY SUPPLY Agency
Co-operation for the protection of critical systems



"Finnish networks the cleaniest?"



Picture: Google Security Blog

cert-fi autoreporter

National response plan in action w/ CERT-FI

- Case Estonia DDoS of May 2007
- Major Vulnerability Cases
  - 2002: SNMP
  - 2005: ISAKMP
  - 200x: Juniper and Cisco vulnerabilities
  - 2008: Archive Formats
- TIETO 2007 Exercise
- Case EU2007.fi & ASEM

National EMERGENCY SUPPLY Agency

Co-operation for the protection of critical systems

Telephone: +358 9 6966 510

E-mail: cert@ficora.fi

WWW: www.cert.fi

CERT-FI alerts and advisories are available in Finnish via:

- E-mail
- SMS (subscription fees apply)
- web pages
- RSS feed
- TELETEXT page 848 (YLE)