



# Coordination of a major disturbance in cyberspace

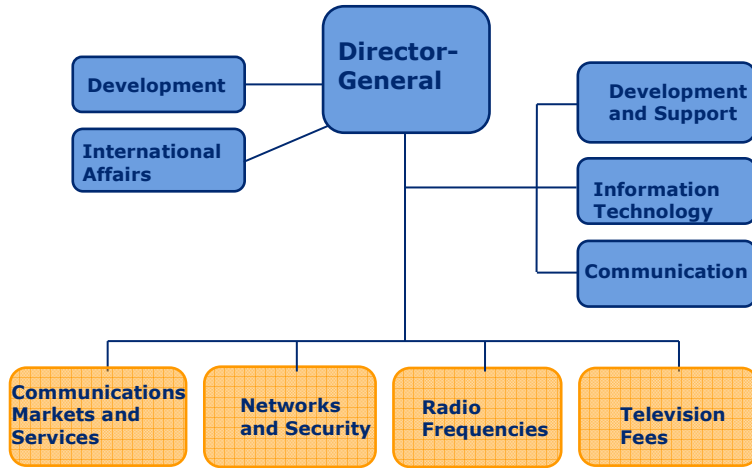
Kauto Huopio

FICORA / **CERT-FI**

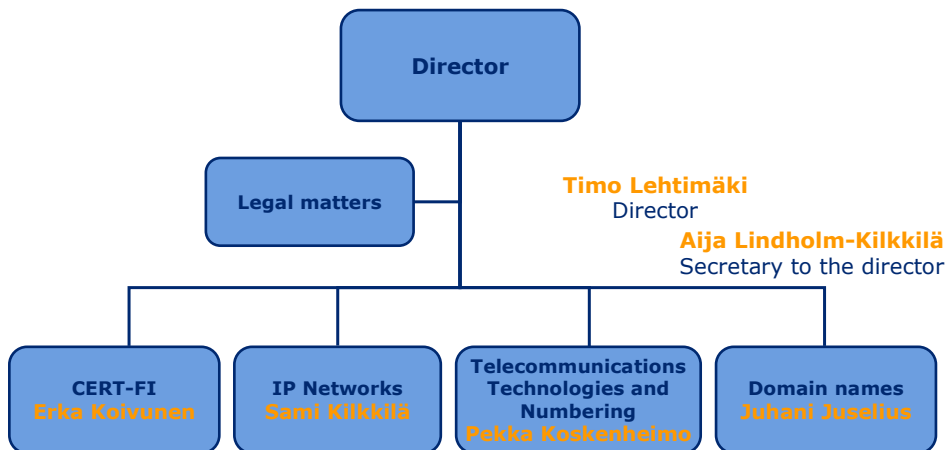
## Agenda

- CERT-FI background
- Ingredients of a successful response plan
- Is it not just DDoS..

Organisation



Organisation



### Statutory duties

- **collecting information** on information security incidents and threats to network services, communications services and value-added services and on significant faults and disturbances in these services
- **investigating** information security incidents and threats to network services, communications services and value-added services and significant faults and disturbances in these services
- **disseminating** information on security matters
- **monitoring** (on its part) protection of privacy and information security in telecommunications

### The national CERT authority

#### Essential services

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

On duty 24/7/365

#### VAROITUS!

4.3.2007 **WordPress ohjelmistoversion 2.1.1 iakelupaketti sisältää ohjelmakoodia**  
06/2007 WordPress on yleisesti käytetty ohjelmisto blog-tyyppisten www-sivujen ohjelmiston jakelupalvelimena toimivalle wordpress.org -palvelimella.

24.2.2007 **Haavoittuvuuksia Firefox- ja Thunderbird-ohjelmistoissa**  
05/2007 Firefox-selainohjelmistosta sekä Thunderbird-sähköpostiohjelmistosta versiot. Kyseiset versiot korjaavat ohjelmistoista useita eri haavoittuvuuksia.

#### Tietoturva nyt!

26.3.2007 **Hyväksikäyttömenetelmä Windowsin MDAC-haavoittuvuus**  
18.19 Windowsin helmikuussa korjaamaan MDAC-haavoittuvuuteen on julkaistu hyväksikäyttömenetelmä, joka mahdollistaa hyökkääjän suorittavan omia...

26.3.2007 **Tilastoja ja julkaisuja tietovuodoista**  
16.29 Tietovuodot ovat saaneet viime kuukausina mediassa runsaasti huomiota. Lisääntyvä siirtäminen verkkopalveluissa ja sähköisissä tietokannissa.

26.3.2007 **Korjaamattomat Microsoft-haavoittuvuudet**  
16.18 Kaikkiin viime kuukausien aikana julkaistuihin Microsoft-haavoittuvuuksiin korjauksia. ISC SANS ja eEye jäljittävät näitä korjaamattomia haavoittuvuuksia.

#### Haavoittuvuudet

27.3.2007 **Haavoittuvuus Sun Java System Directory Server (ns-sla)**  
015/2007 Sun Java System Directory Server on LDAP-pohjainen hakemistopalvelin palvelunestohyökkäyksen mahdollistava haavoittuvuus. Haavoittuvuus...

27.3.2007 **Kaksi haavoittuvuutta WordPerfect-kirjasto libwpd:ssä**  
014/2007 WordPerfect-dokumenttien lukuun monissa ohjelmistoissa, kuten OpenOffice, käytetyistä libwpd-kirjastosta on löydetty kaksi haavoittuvuutta, joiden...

27.3.2007 **Kaksi OpenOffice ja StarOffice-haavoittuvuutta**  
013/2007 OpenOfficesta ja StarOfficesta on löydetty kaksi haavoittuvuutta, joiden avulla suorittavan kohdejärjestelmässä omia komentojaan. Haavoittuvuus...

## CERT-FI

### Cooperation

#### Active cooperation with authorities in Finland

- exchange of information and procedural cooperation

#### CSIRT actors in Finland

- the information security organisations of telecommunications operators, IT service houses and major organisations
- other Finnish actors in the sector, such as software and information security companies

#### CIP cooperation

- power companies, industrial plants, banks and insurance companies, nationwide commercial chains and other actors that are vital for the critical infrastructure

#### International cooperation

- cooperation partners on every continent and in all time zones



Medicinal **EMERGENCY SUPPLY** Agency  
The responsible for products of medicinal products



## Our customers

#### With Finnish networks we mean:

- AS:s located in Finland or controlled by a Finnish entity
- FI-domain names
- Telephone networks related to country code +358
- Other networks owned or operated by a Finnish entity

#### With Finnish network services we mean:

- Network services owned or operated in Finland or by a Finnish entity

## Finland – a quiet place



19/09/2007

CERT-FI

9

## Finland – an internet green zone..



19/09/2007

CERT-FI

10

## Ingredients of a success in controlling a major network disturbance

- Legal framework
  - Network operators have a **right** and **mandate** to investigate and resolve a network issue
    - needs traffic data processing
  - Coordinative unit (a national CERT) has a right to receive and disseminate information related to the case – both at national and international level
  - Criminal code has appropriate statues that can be applied to malicious network activity – the mandate for law enforcement community for their actions

## Major ingredient: working cooperation among ISP:s

- Network operators must see security issues as a non-competitive area
- **Cooperation under a national coordinative CSIRT umbrella**
  - national CSIRT as a major information feeder to ISP:s regarding malicious network activity
  - regular meetings of ISP abuse handlers
  - mailing lists
  - private IRC server for all players in the information security field
  - a high level of trust among the key players in the area
    - *takes time to develop!*

## Major ingredient: working cooperation inside government

- Forum for coordinative CERT, law enforcement, security services, central government IT functions cooperation
- Appropriate reporting channels and facilities in place and in use
- A forum for the ISP:s and governmental units to network

## Major ingredient: international cooperation

- The national coordinative CSIRT and key ISP:s must have working international relations at operational level
  - contacts that used on daily work – not just something that is stored in a “open in an emergency” –folder
- Appropriate trust and information handling structure (TLP)
- Issues on protectively marked information exchange
- Channels must be ready for immediate communication and coordination
  - network incidents can’t wait the opening of office next morning

## Observations of CSIRT / LE coordination

- International law enforcement community is too slow to react on immediate effects of a major network issue
- National coordinative CSIRT:s have a major role on the needed actions
  - they know their own constituency (= country)
  - they have the needed international relations
  - a need to contact LE directly in another country or through their national CSIRT in some cases?
- Issues on cases spanning the globe
  - how to coordinate incident handling with LE so that the incident handling won't disturb LE activities – globally?!

## CERT-FI role in the Estonian cyberriots

- Incident coordination assistance to CERT-EE
  - processing of attack data to ISP:s internationally
  - CERT-FI automated abuse case processing tools in good use
  - Crisis coordination IRC
- Keeping Finland informed
  - central government
  - ISP:s
  - media
- Keeping our international partners informed
  - EGC
  - FIRST



## It is not just DDoS..

More concerning issues:

- Targeted attacks
  - information theft / monitoring on critical infrastructure, high-tech, government etc.
- Identity theft in its various forms
  - Trust on e-banking and e-commerce
- "Rogue" ISP:s, hosting service providers
  - How these are allowed to operate?
  - A **major** source of malicious activity in the net




Telephone: +358 9 6966 510

E-mail: [CERT@FICORA.fi](mailto:CERT@FICORA.fi)

WWW: [www.CERT.fi](http://www.CERT.fi)

Public alerts and advisories can be obtained  
(in Finnish):

- Email alert service
- SMS alert service (pay-per-subscription)
- CERT-FI WWW pages
- RSS newsfeed 
- YLE teletext page 848 