Cyber Security capabilities
FICORA’s experience as a CERT & NRA
World's safest networks? – Mostly harmless at least

Microsoft SIR, March 2017: Locations with low concentrations of malware hosting sites included Finland (4.1), Taiwan (5.3), and Turkey (5.3).
NCSC-FI as a department of FICORA
The Telecommunications Administration Centre

Radio Frequency, Telecommunication, TV licences
Steering of postal operations
Fi-domain names
Economic regulation
Protection of privacy, information security, supervision of TV and radio operations

The Finnish Communications Regulatory Authority (FICORA)

CERT-FI
Handling of undeliverable postal items
Short-term TV and radio licences, supervision of universal service
Broadband 2015 project
NCSA-FI
The National Cyber Security Centre (NCSC-FI)
The Public Regulated Service (PRS)

Different roles support creating situational awareness and providing services to different customers

- National Computer Emergency Response Team
  - Critical infrastructure
  - Government
  - ISPs
  - Citizens

- National Communications Security Authority
  - Assessment of information systems and telecommunications arrangements

- National Regulatory Authority
  - Supervision of ISPs
  - Privacy of electronic communications
An example of how CERT and NRA functions play together

- Autoreporter is one of our services
  - Since 2006
  - It automatically and constantly collects data on malware and information security incidents related to Finnish networks
    - "How Finland looks like from outside"
  - Some information we get, is based on our status as the national CERT, and some information we get from our other friends
  - The incidents are categorized, daily reports are compiled and sent to the network operators
    - Operators are obliged by law to take care of their information security
    - Legislation also gives operators rights to take action in order to preserve network and service security
In 2013 something happened

Autoreporter handled ~ 500 000 incidents
A study showed that something wasn't right with one of the ISPs.
How we handled that?

- We invited the ISP to a meeting
  - Showed what we had noticed
  - Asked, why is that
  - Discussed with the ISP what to do about the situation

- The ISP changed its abuse processes
  - We saw in Autoreporter change back to normal
  - No administrative, regulatory intervention was needed
    - It is, after all, every ISP's own benefit to take care of their information security
Behind our success: Pure luck or something smarter?

- Yes, we are a regulator, but we see ourselves also highly as a service organization
  - CERT and NCSA functions are easy for everyone to see as a service
  - It is good to remember that also NRA serves the whole society
  - Our mindset is to provide positive support to the community
    - Focus is, what can we give, not what we can get
    - Assistance first, compliance when storm has calmed

- Without data we're useless
  - ISPs are obliged by law to report on specific incidents
  - The rest tell us on voluntary basis
    - In practice, 99.9 % of all cases
  - "World" expects us to mitigate the problem – "Finland" expects us to provide help
Behind our success: Pure luck or something smarter?

- Co-operation is essential
  » Without a deeply networked community we would not be strong
  » Sharing experiences and lessons learned creates a positive spin that will feed itself
  » Will only function properly if a sufficient level of trust is established between the parties

- Information security legislation, sometimes seen as a restriction, is actually an enabler for us and the Finnish network owners
  » Very strict law on privacy both at work & home, but also efficient tools for solving incidents