Incident response made better by agile robots

Antti Kiuru
Head of Coordination Centre

Finnish Communications Regulatory Authority
National Cyber Security Centre

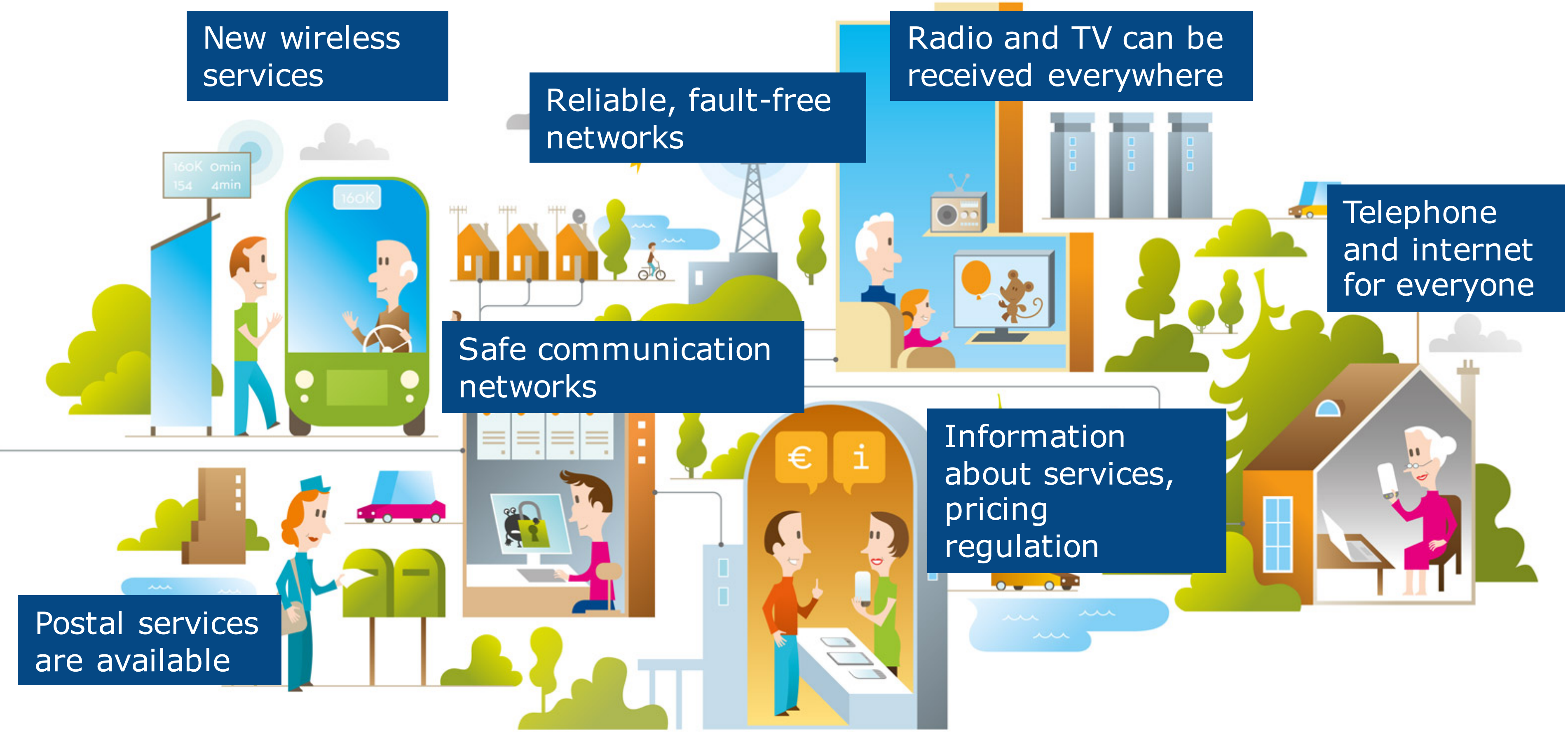
Agenda

- Who we are as FICORA and NCSC-FI
- How our team works and how we do our thing
- What kind of tools do we have and how did we end up building those
- Something about robots as promised

Who we are

FICORA and the National Cyber Security Centre of Finland

FICORA, Finnish Communications Regulatory Autority



New wireless services

Reliable, fault-free networks

Radio and TV can be received everywhere

Telephone and internet for everyone

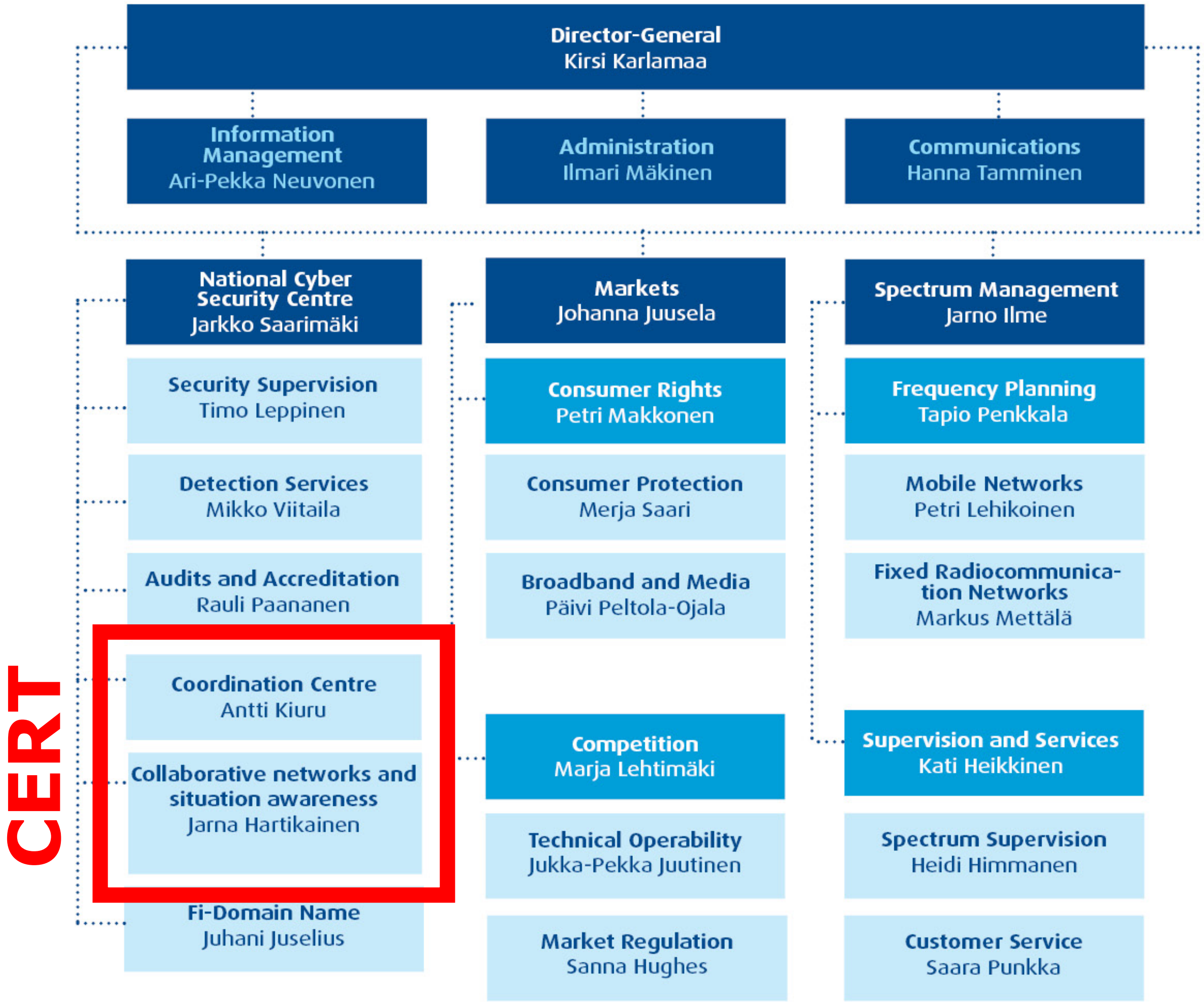
Safe communication networks

Information about services, pricing regulation

Postal services are available

National Cyber Security Centre of Finland

- Resiliency of communications networks
- **CERT-FI** and NCSA-FI migrated to NCSC-FI in 2014
- Provides information security services to Gov & CIP
- Runs the national early warning and monitoring network
- Is the national 24/7 contact point



Director-General
Kirsi Karlamaa

Information Management
Ari-Pekka Neuvonen

Administration
Ilmari Mäkinen

Communications
Hanna Tamminen

National Cyber Security Centre
Jarkko Saarimäki

Security Supervision
Timo Leppinen

Detection Services
Mikko Viitaila

Audits and Accreditation
Rauli Paananen

CERT

Coordination Centre
Antti Kiuru

Collaborative networks and situation awareness
Jarna Hartikainen

Fi-Domain Name
Juhani Juselius

Markets
Johanna Juusela

Consumer Rights
Petri Makkonen

Consumer Protection
Merja Saari

Broadband and Media
Päivi Peltola-Ojala

Competition
Marja Lehtimäki

Technical Operability
Jukka-Pekka Juutinen

Market Regulation
Sanna Hughes

Spectrum Management
Jarno Ilme

Frequency Planning
Tapio Penkkala

Mobile Networks
Petri Lehikoinen

Fixed Radiocommunication Networks
Markus Mettälä

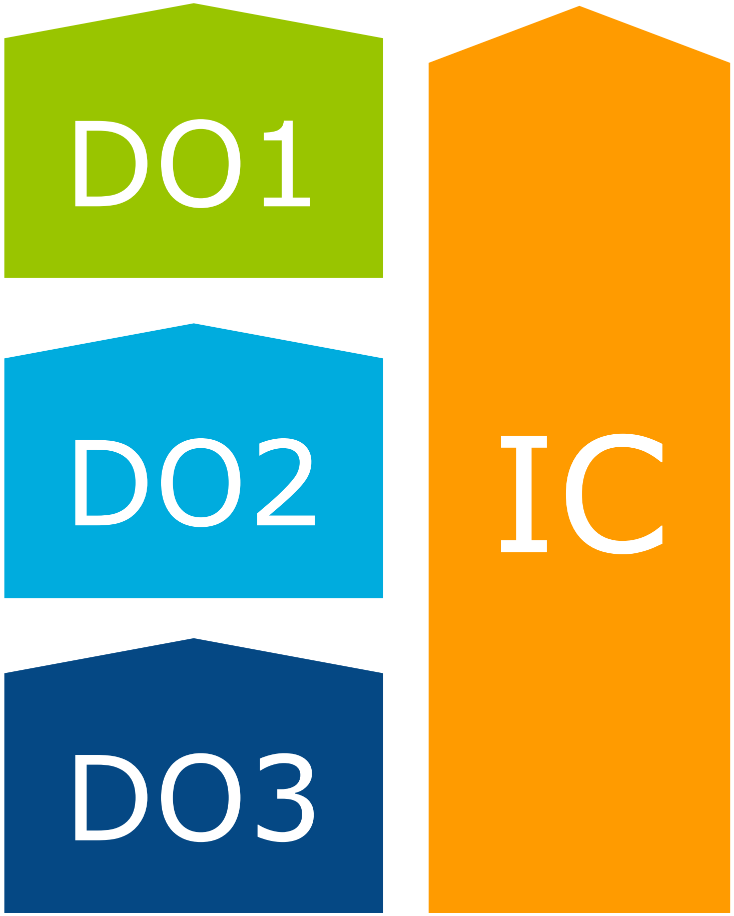
Supervision and Services
Kati Heikkinen

Spectrum Supervision
Heidi Himmanen

Customer Service
Saara Punkka

How the team is built

- The shift is three weeks for duty officers and incident coordinators
- Ops-meetings mon - thu
- End of shift -brief on friday
- Eight duty officers, four incident coordinators


DO1

DO2

DO3

IC

Duty officers vs. incident coordinators

- Duty officers take care of incident response
- Media interviews
- All the regular CERT work
- National early warning and monitoring system
- Vulnerability advisories, social media, blog posts etc

- Incident coordinator takes care that the ball doesn’t drop when duty officers change shifts
- When something big happens, IC gathers a team and starts coordinating the incident
- New way of doing things has it’s advantages
- A strong mandate to do things!

Output from the CERT & NCSC-FI

- Daily news & vuln feed to everyone who wants them
- Continuous reporting to some partners via extranet
- Weekly reports to cooperation partners
- Monthly reports to different sectors
- Advisories, social media

CLASSIFIED

TLP'd

PUBLIC

FIRST THINGS FIRST

Solving daily tasks with automation

Different problems, different solutions

- How do you handle a load of abuse messages
- How do you handle *load of abuse handling

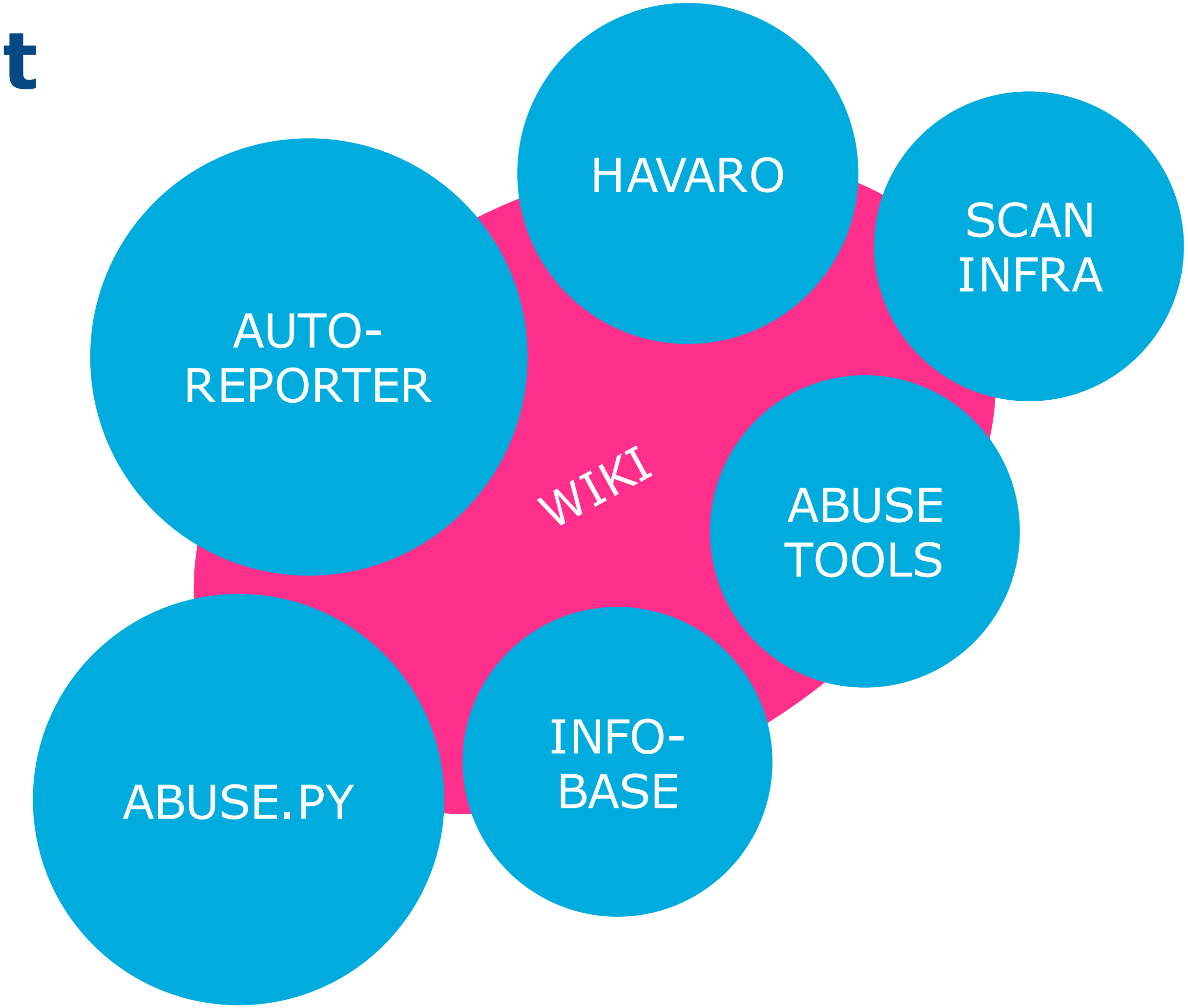
- How do you figure out what threats your priority clients are facing
  - » ... have you maybe seen them before?

- And how do you find out what the rest of the crowd is doing (or more like – not doing)

What drives the development

- We need to do something quick(er!) aka. get rid of manual labor
  - » The regular thing; something escalates quickly!
- Whatever we do, we need it to have standard output!
  - » Telcos need it to use machines to churn the data
  - » Standard output looks more pro than ”hi there”
- You will need ROBOTS.
  - » Quick to adapt (T-800 vs T-1000)
  - » Quick to deploy (rather now than soon)

This is what we've ended up with



Getting FIRST hand information about threats

National early warning and monitoring system

Early warning and monitoring system

HAVARO - the national early warning and monitoring system

For critical infrastructure and government

Exclusive service

Real time threat monitoring within office hours, based on our secret sauce

The National Early warning and monitoring system - HAVARO

- Detects and monitors advanced attacks against gov and critical infrastructure

secret sauce

- Monitors all the traffic going in and out the organization's network

- Ability to see things like 3rd party scans for heartbleed & shellshock etc

Early warning and monitoring system

- Puts IoC's and threat intel into good use
    - Information we couldn't use efficiently otherwise
- Built from bottom up, not always the best way
- Built using mostly open source software
- Gives information how effective some methods are in detecting bad guys (java, flash, known sources of evilness)

Early warning and monitoring system

- We started from honeypots in 2007
- The current model has been in use since 2011
- If you're building something like this, make sure you ask your incident responders opinions all the way
- After the thing grows, it will not be agile and the whole process of growing is far from agile.

What our customers get out of it

- Better situation awareness of their networks
- Realtime threat monitoring with our Extranet
- Ability to use our secret sauce – the IoC's that are unavailable for them otherwise
- Ability to use our services in full capacity; analysis, support, incident response, international cooperation

Autoreporter & Abuse Helper

Handling a *load of abuse handling

Autoreporter & Abuse Helper

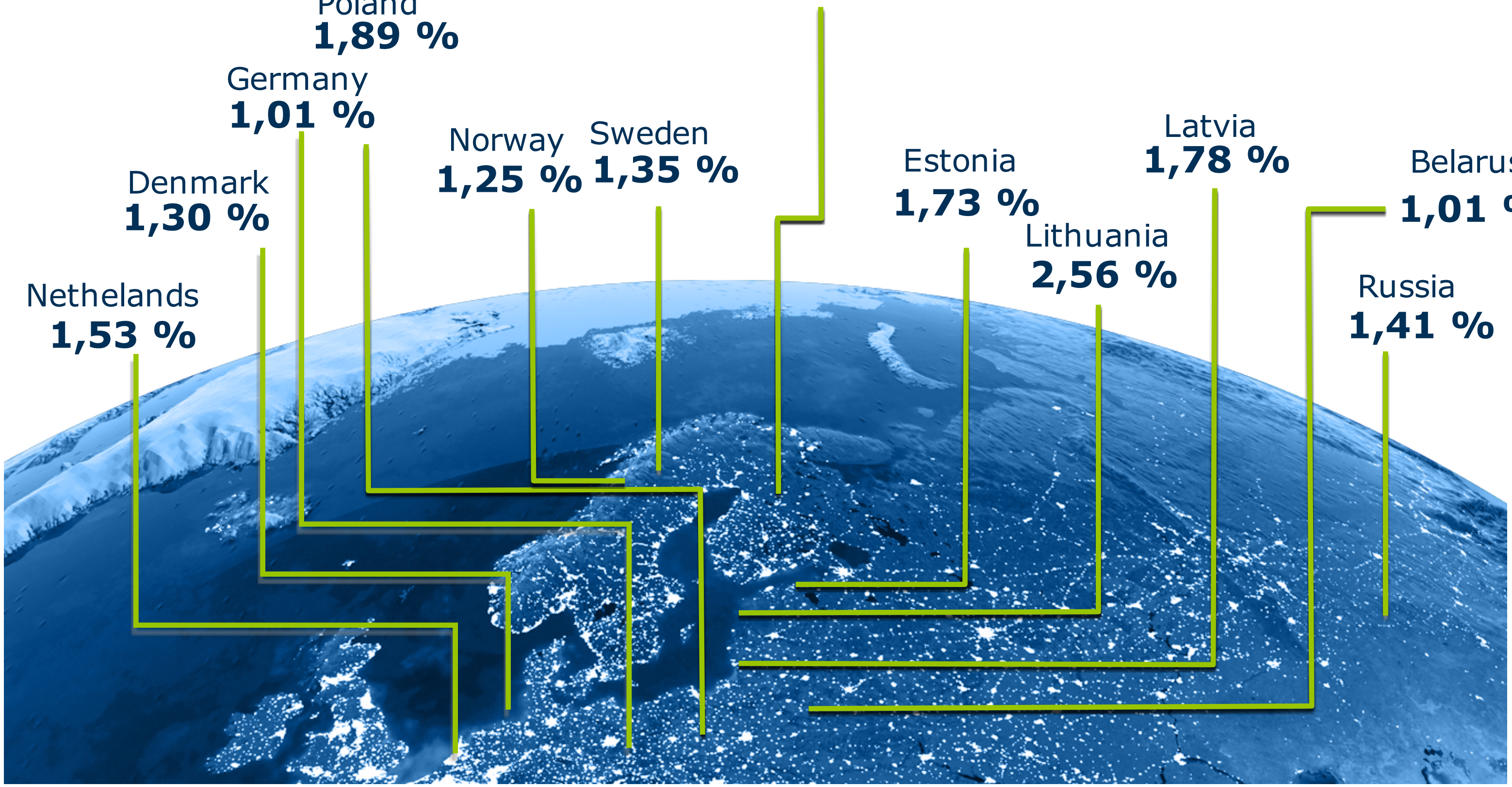
- Getting more data is good, handling it with manual tools is not
- We started collecting data on how Finland looks like from outside
- Some information we get is based on our status as the national CERT, something we get from our other friends

Autoreporter & Abuse Helper

- Automatically and constantly collects data on malware and information security incidents related to Finnish networks
- The incidents are categorized, daily reports are compiled and sent to the network operators
- It's an open source solution that uses XMPP

A comprehensive picture of infection levels in Finland

Incidents from one viewpoint



Finland
0,83 %

Poland
1,89 %

Germany
1,01 %

Norway
1,25 %

Sweden
1,35 %

Denmark
1,30 %

Nethelands
1,53 %

Estonia
1,73 %

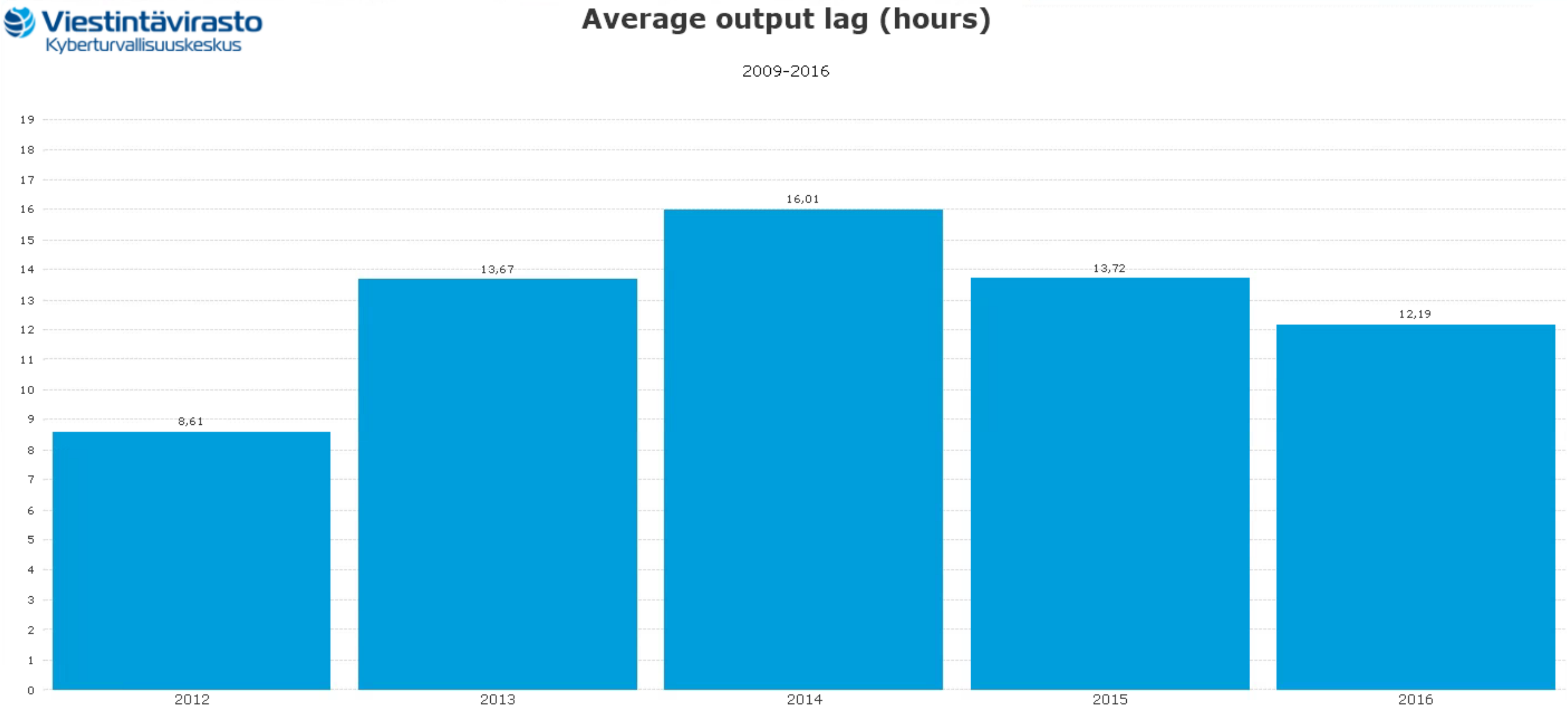
Latvia
1,78 %

Lithuania
2,56 %

Belarus
1,01 %

Russia
1,41 %

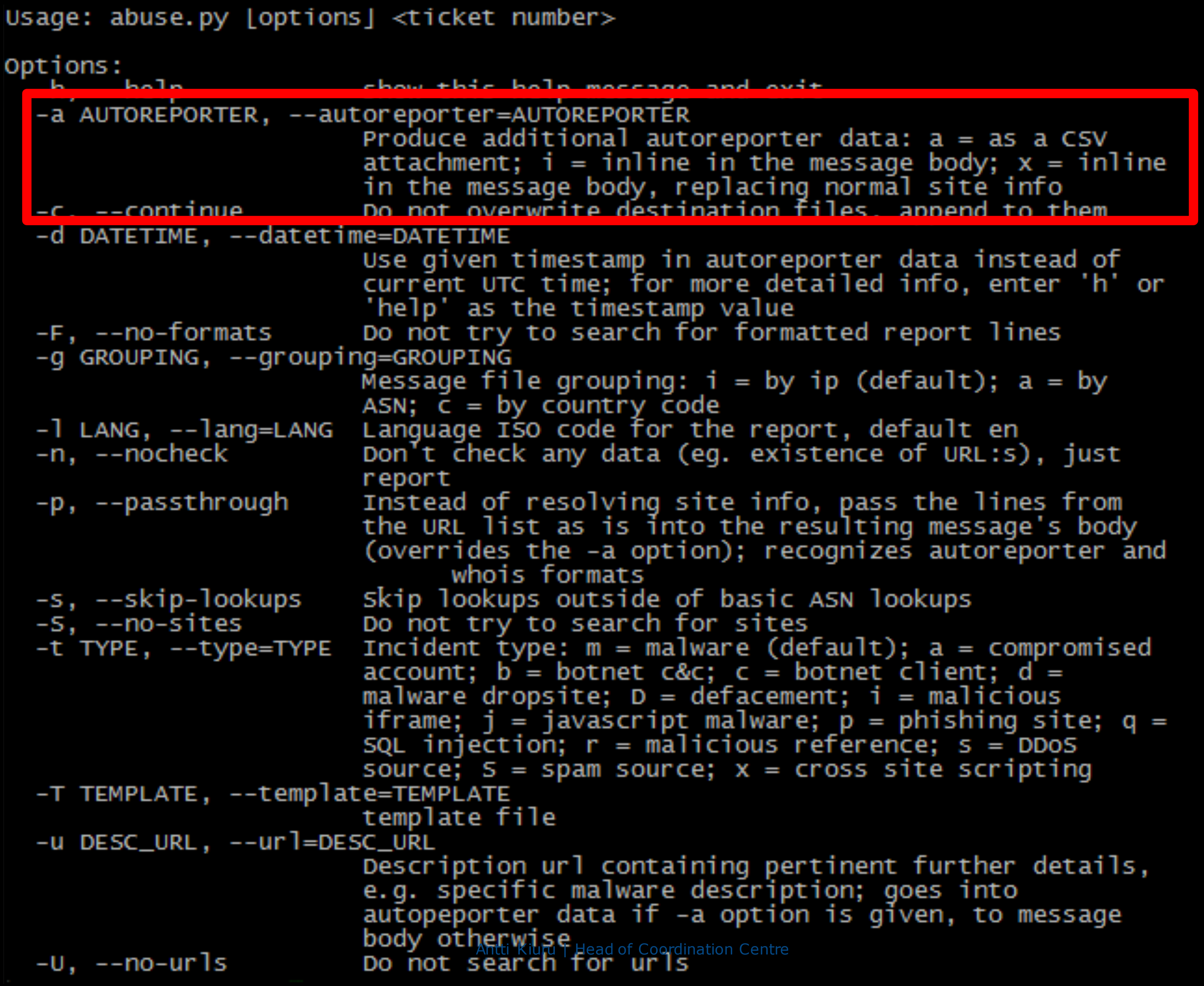
Since things can be measured, lets.



In-house abuse handling tools

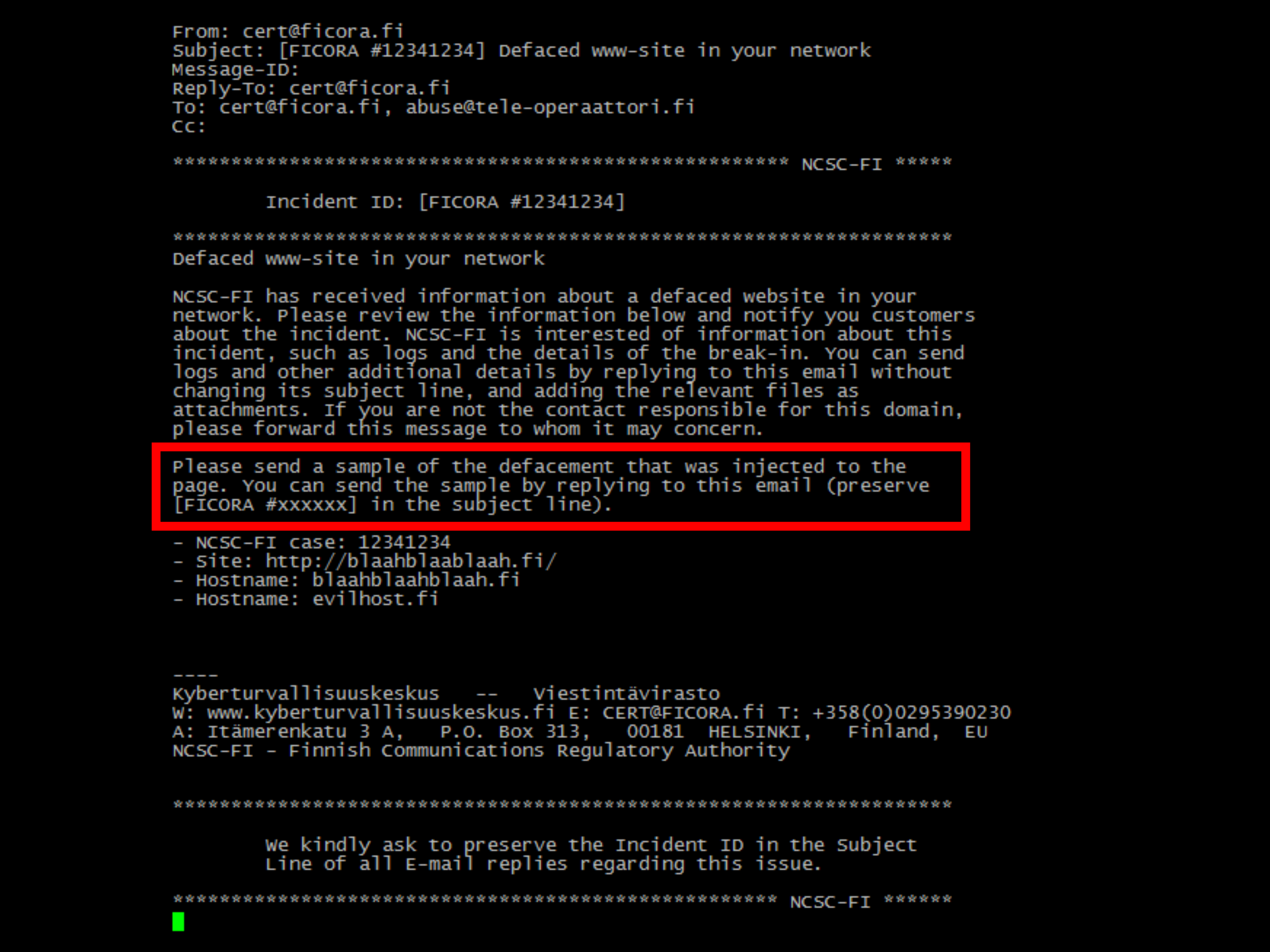
In-house abuse handling tools

- Abuse.py is our versatile abuse handling tool
  - » Uses pre-defined or on-demand templates
  - » Does DNS lookups, whois queries, searches contact-db
- It is an answer to the question; what to do to random notifications from different sources
- And a bunch of other things that end with .py



```
Usage: abuse.py [options] <ticket number>

Options:
  -h, --help            show this help message and exit
  -a AUTOREPORTER, --autoreporter=AUTOREPORTER
                        Produce additional autoreporter data: a = as a CSV
                        attachment; i = inline in the message body; x = inline
                        in the message body, replacing normal site info
  -c, --continue        Do not overwrite destination files, append to them
  -d DATETIME, --datetime=DATETIME
                        Use given timestamp in autoreporter data instead of
                        current UTC time; for more detailed info, enter 'h' or
                        'help' as the timestamp value
  -F, --no-formats      Do not try to search for formatted report lines
  -g GROUPING, --grouping=GROUPING
                        Message file grouping: i = by ip (default); a = by
                        ASN; c = by country code
  -l LANG, --lang=LANG  Language ISO code for the report, default en
  -n, --nocheck         Don't check any data (eg. existence of URL:s), just
                        report
  -p, --passthrough     Instead of resolving site info, pass the lines from
                        the URL list as is into the resulting message's body
                        (overrides the -a option); recognizes autoreporter and
                              whois formats
  -s, --skip-lookups    Skip lookups outside of basic ASN lookups
  -S, --no-sites        Do not try to search for sites
  -t TYPE, --type=TYPE  Incident type: m = malware (default); a = compromised
                        account; b = botnet c&c; c = botnet client; d =
                        malware dropsite; D = defacement; i = malicious
                        iframe; j = javascript malware; p = phishing site; q =
                        SQL injection; r = malicious reference; s = DDoS
                        source; S = spam source; x = cross site scripting
  -T TEMPLATE, --template=TEMPLATE
                        template file
  -u DESC_URL, --url=DESC_URL
                        Description url containing pertinent further details,
                        e.g. specific malware description; goes into
                        autopeporter data if -a option is given, to message
                        body otherwise
  -U, --no-urls         Do not search for urls
```



```
From: cert@ficora.fi
Subject: [FICORA #12341234] Defaced www-site in your network
Message-ID:
Reply-To: cert@ficora.fi
To: cert@ficora.fi, abuse@tele-operaattori.fi
Cc:

***************************************************** NCSC-FI *****

        Incident ID: [FICORA #12341234]

*******************************************************************
Defaced www-site in your network

NCSC-FI has received information about a defaced website in your
network. Please review the information below and notify you customers
about the incident. NCSC-FI is interested of information about this
incident, such as logs and the details of the break-in. You can send
logs and other additional details by replying to this email without
changing its subject line, and adding the relevant files as
attachments. If you are not the contact responsible for this domain,
please forward this message to whom it may concern.

Please send a sample of the defacement that was injected to the
page. You can send the sample by replying to this email (preserve
[FICORA #xxxxxx] in the subject line).

- NCSC-FI case: 12341234
- Site: http://blaahblaablaah.fi/
- Hostname: blaahblaahblaah.fi
- Hostname: evilhost.fi



----
Kyberturvallisuuskeskus   --   Viestintävirasto
W: www.kyberturvallisuuskeskus.fi E: CERT@FICORA.fi T: +358(0)0295390230
A: Itämerenkatu 3 A,   P.O. Box 313,    00181  HELSINKI,   Finland,  EU
NCSC-FI - Finnish Communications Regulatory Authority


*******************************************************************

        We kindly ask to preserve the Incident ID in the Subject
        Line of all E-mail replies regarding this issue.

**************************************************** NCSC-FI ******
```

Other handy stuff

- Inspect-js - A quick tool for handling lists of compromised Finnish websites at once

  1. Downloads the webpage by pretending to be a real browser
  2. Splits the files by website/domain
  3. Spits out to single file what was found to be malicious in the sites
  4. .. And with some awk and sed, talks to abuse.py !

- Comes in handy when you have 100 malicious URL’s to process

Infobase

- Simply put, it’s a centralized storage for mining data from random input
- Mining your own data can be challenging, especially the way of presenting it
- Answers to the question if we’ve seen a certain IP address or a hostname pop up somewhere before
  - » Question we ask ourselves and get asked quite a lot
- In someway, infobase is one of the two systems that glues the whole thing together

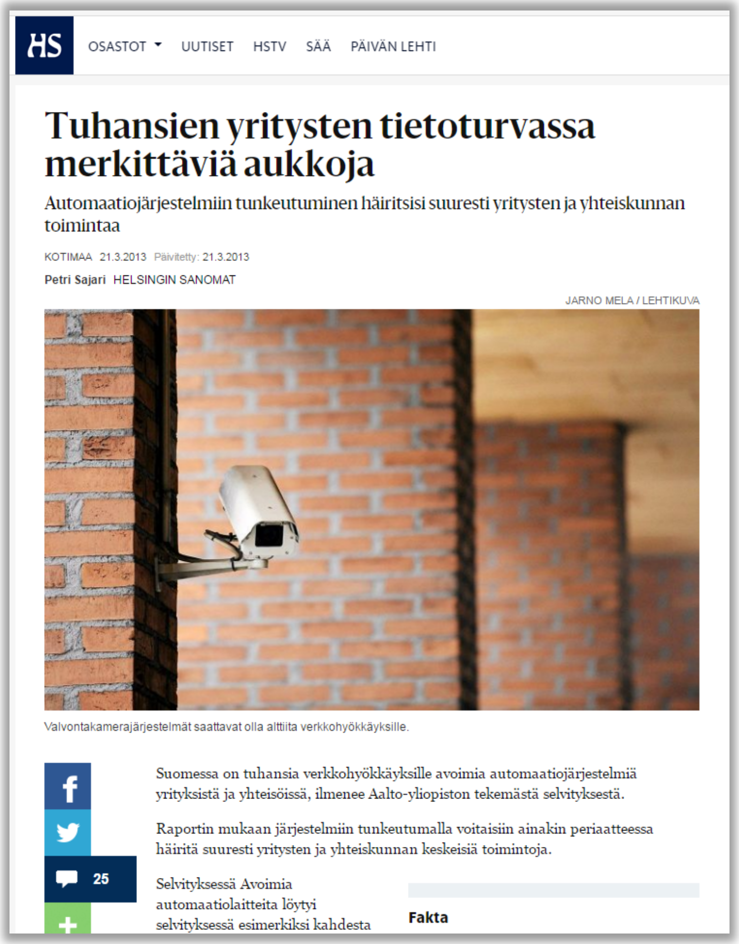
Scan all the things!

Being proactive for a change

Scanning for ICS and SCADA

- A report on open scada devices in March 2013
- Aalto University used SHODAN to get information
- SHODAN's nice but we needed more

Scanning for ICS and SCADA



Tuhansien yritysten tietoturvassa merkittäviä aukkoja

Automaatiojärjestelmiin tunkeutuminen häiritsisi suuresti yritysten ja yhteiskunnan toimintaa

KOTIMAA 21.3.2013 Päivitetty: 21.3.2013

Petri Sajari HELSINGIN SANOMAT

JARNO MELA / LEHTIKUVA

Valvontakamerajärjestelmät saattavat olla alttiita verkkohyökkäyksille.

Suomessa on tuhansia verkkohyökkäyksille avoimia automaatiojärjestelmiä yrityksistä ja yhteisöissä, ilmenee Aalto-yliopiston tekemästä selvityksestä.

Raportin mukaan järjestelmiin tunkeutumalla voitaisiin ainakin periaatteessa häiritä suuresti yritysten ja yhteiskunnan keskeisiä toimintoja.

Selvityksessä Avoimia automaatiolaitteita löytyi selvityksessä esimerkiksi kahdesta

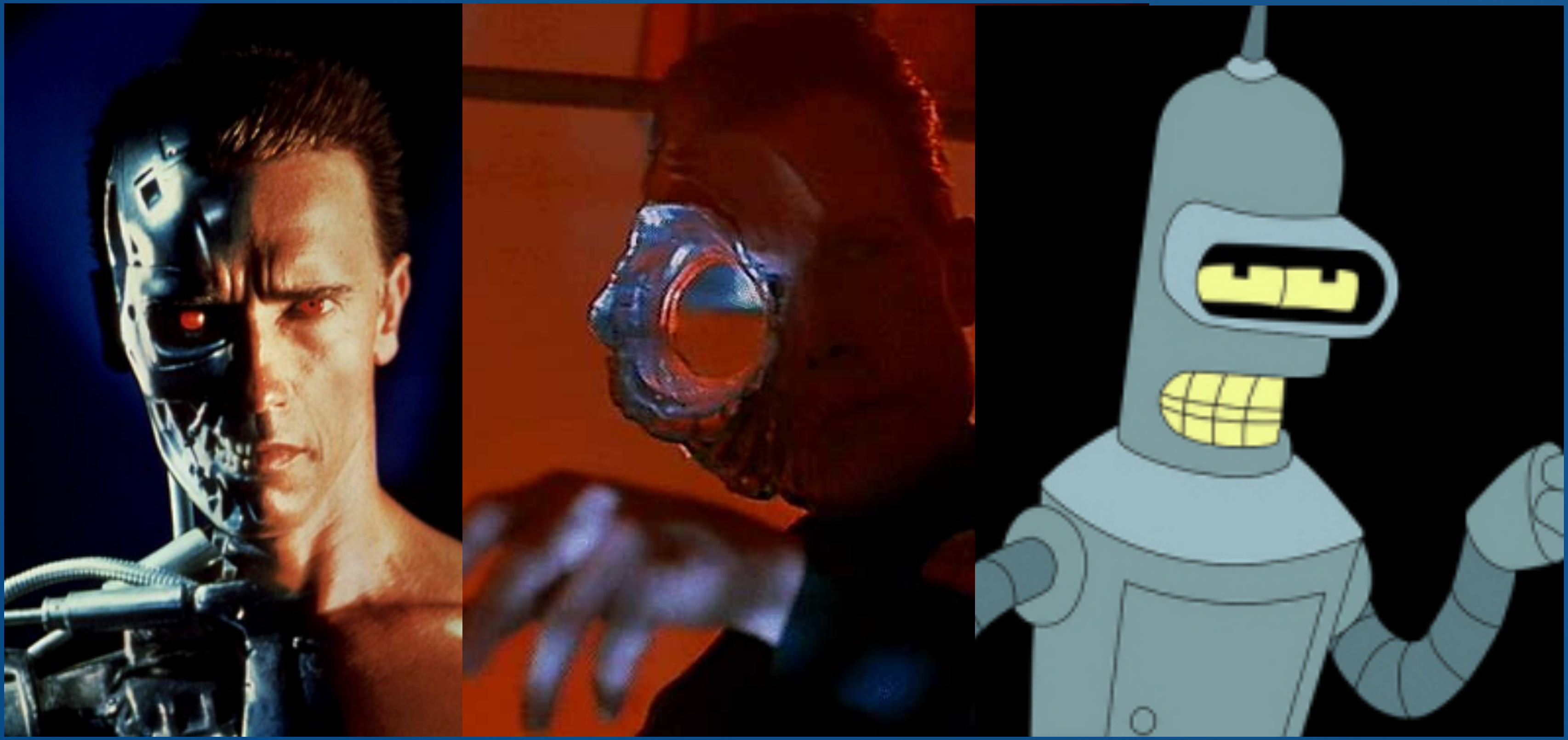
- What we've found are mostly building automation things
- Some serial equipment, traffic cameras AND scada equipment
- As it turns out, it is not illegal to have a vulnerable or open service on the internet

Heartbleed incident 2014

- Nobody knew for sure how many vulnerable services there were
- We repeated the scans several times to see if the notification process and publicity was effective or not
- In one way, it was a gamechanger for us
- No more looking for just open SCADA/ICS

Seize the moment

- Open, exploitable services pose a common problem to us all
  - » They end up being DDoS sources, TDS, proxies, C2's
- In the past we scanned for Kaminsky DNS bug and open resolvers
- If we could scan for DNS affected services .. Maybe we could do it to other things as well?
- Heartbleed, Shellshock, open NTP's, bad SSL certificates, other things that pose a threat



To conclude

.. And finally something about the robots

Lessons learnt from sw development

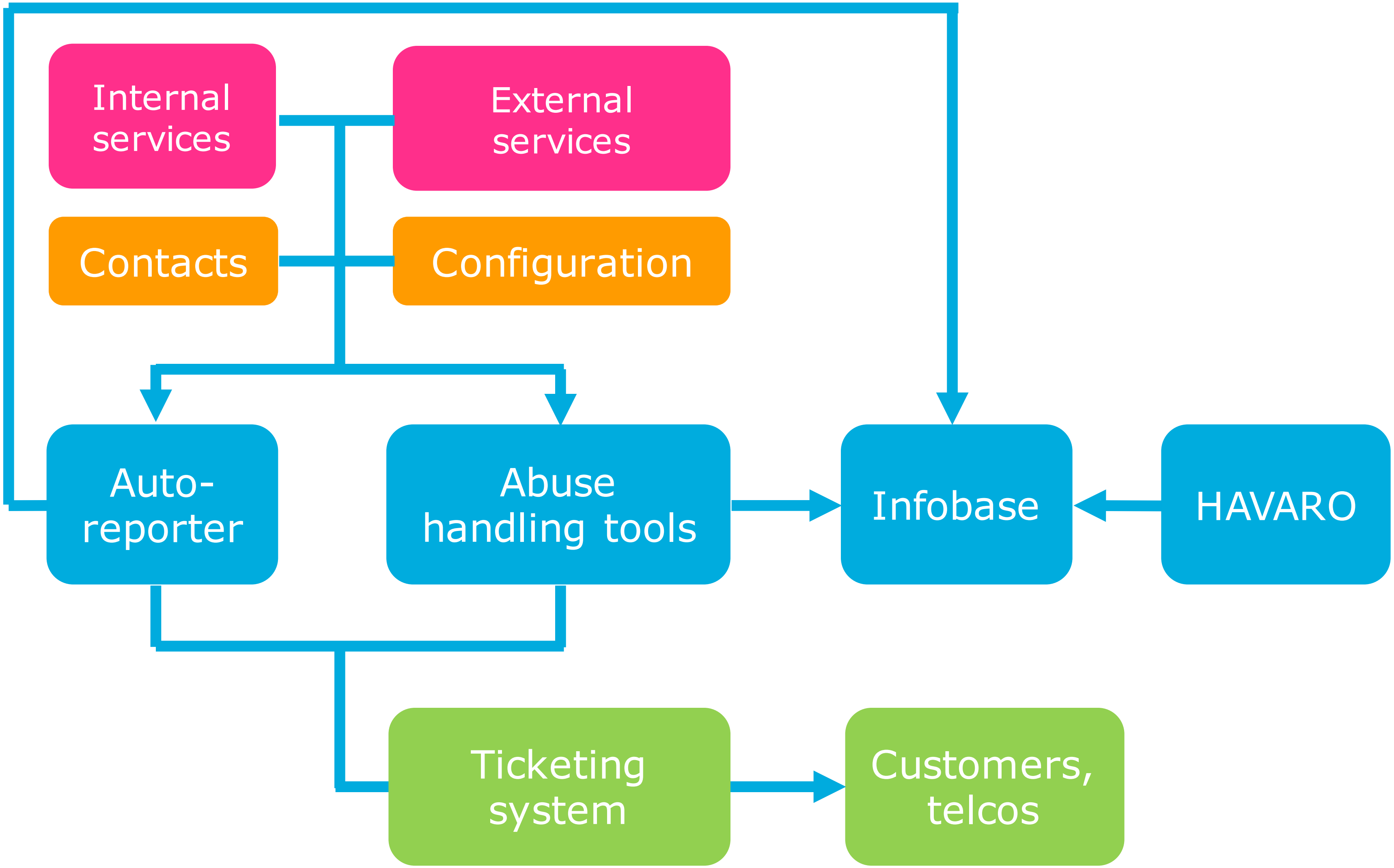
- Doing things without going tools first but focusing more on the problem itself often pays off
- It allows us to use the existing solutions for solving multiple problems
- Using existing OSS is sometimes troublesome
- (I actually started this presentation tools first)

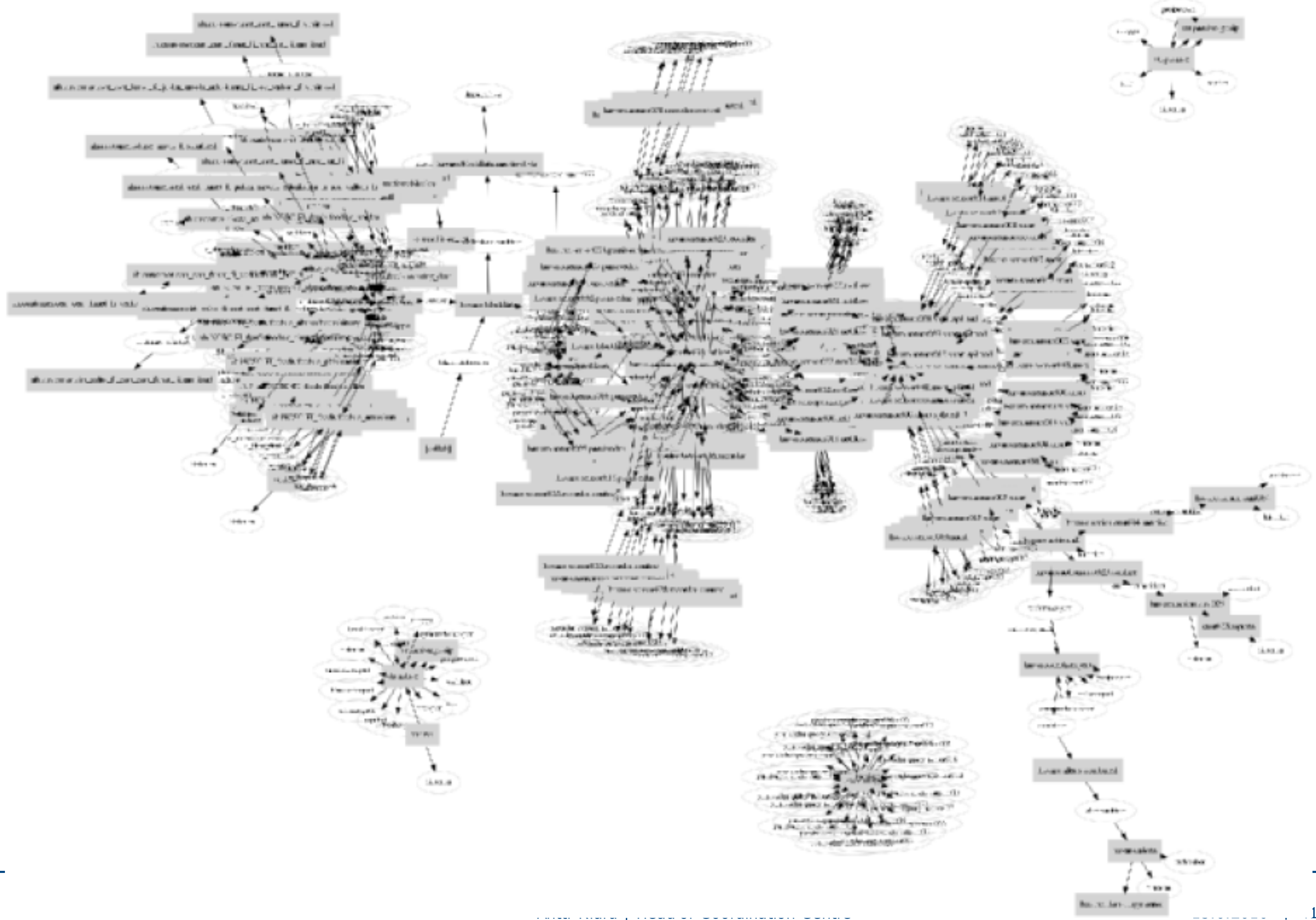
Lessons learnt from sw development

- Project planning
- Dedicated developers
  - » Who understand the current systems, talk python, etc
  - » Outsource them? You'll need money in any case
    - For using money you need plans
      - » Pro grade plans require pro grade planners
        - **NOT SO AGILE ANYMORE**
- Justification for using resources
  - » People taken to DEV cave shouldn't do IR
  - » Money and time could be used elsewhere

The robots.

- As said, our Autoreporter runs on Abuse Helper.
- HAVARO is based on similar technique
- We have tons of robots on XMPP channels that can be used for same things by different tools
  - Passive DNS lookups
  - Whois queries
  - Contact information fetching
- We use these robots to help solving something quickly
  - We develop new ones as needs emerge, if some datasource decides to change format from IODEF to Json or so


Internal services
External services
Contacts
Configuration
Auto-reporter
Abuse handling tools
Infobase
HAVARO
Ticketing system
Customers, telcos



When fiddling with robots

- Aim to be proactive, reactive and creative when needed. Build your own tools when you need to do something else than do routine manual stuff.
- Seize the moment when you need to. It helps with things like establishing your organization's position and maybe even with funding
- Don't build tools to do stuff, build tools to allow you to focus on more important things

QUESTIONS?