

# GN3 Security activities

Baiba Kaskina (SigmaNet), Maurizio Molina (DANTE)  
TF-CSIRT, Hamburg, 25.01.2010.

- Started April 1<sup>st</sup> 2009
- 4 Years
- SA2: multidomain services
  - Extending / engineering GÉANT2 developments
  - IP Network monitoring, Layer2 or wavelength circuit setup, cross border fiber activation
- SA2/T4: support the secure development and deployment of multidomain services

# Survey: Multi-domain anomalies handling in NRENs

Baiba Kaskina (SigmaNet), Maurizio Molina (DANTE)  
TF-CSIRT, Hamburg, 25.01.2010.

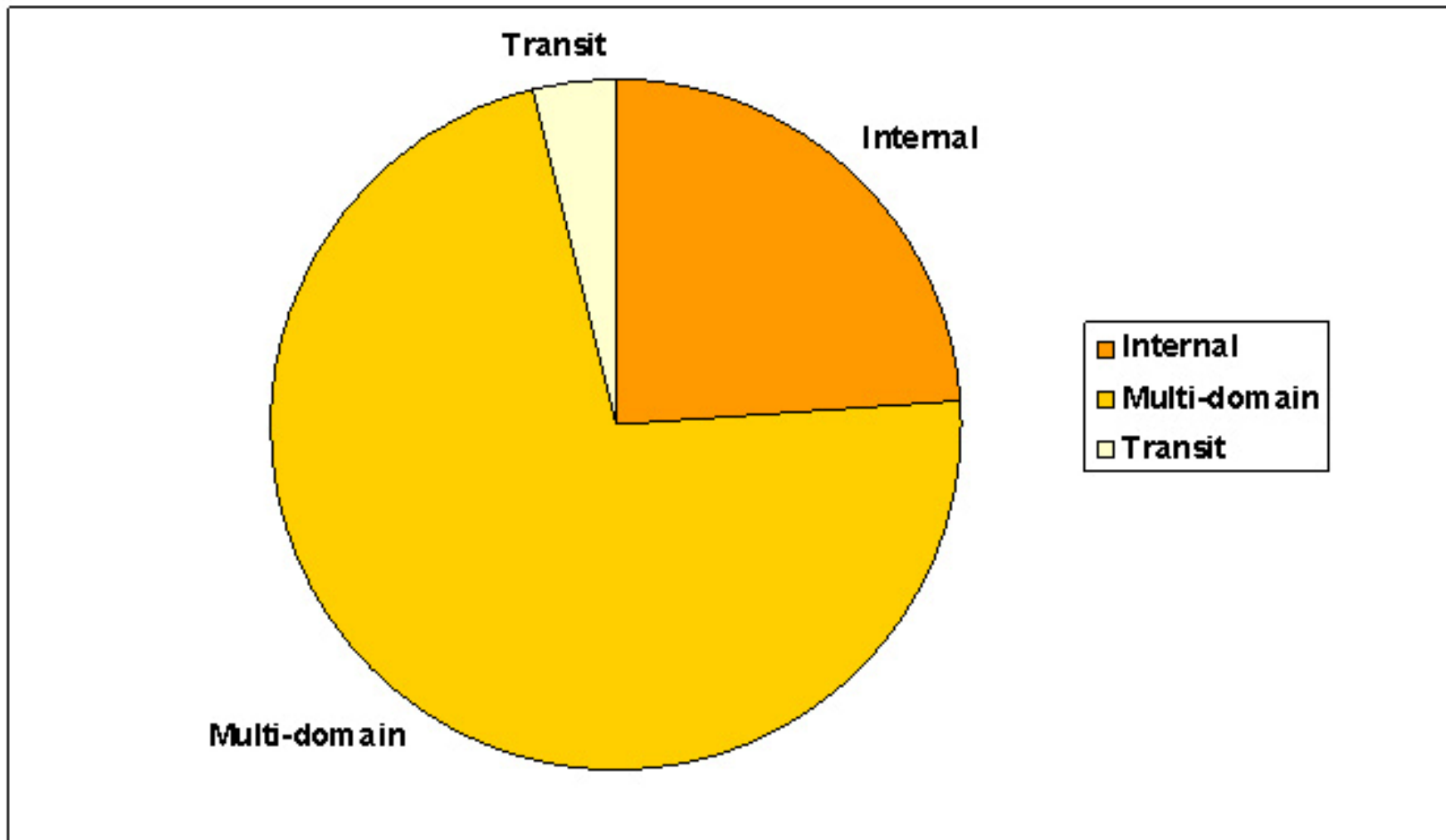
## About the survey

- Aim: get detailed picture on how **multi-domain** anomalies are handled
- 36 Questions
  - *Anomaly classification (types and severity)*
  - *Tools for detecting anomalies*
  - *Workflows and procedures (including LEA)*
- 38 NRENs invited
- 22 answers received

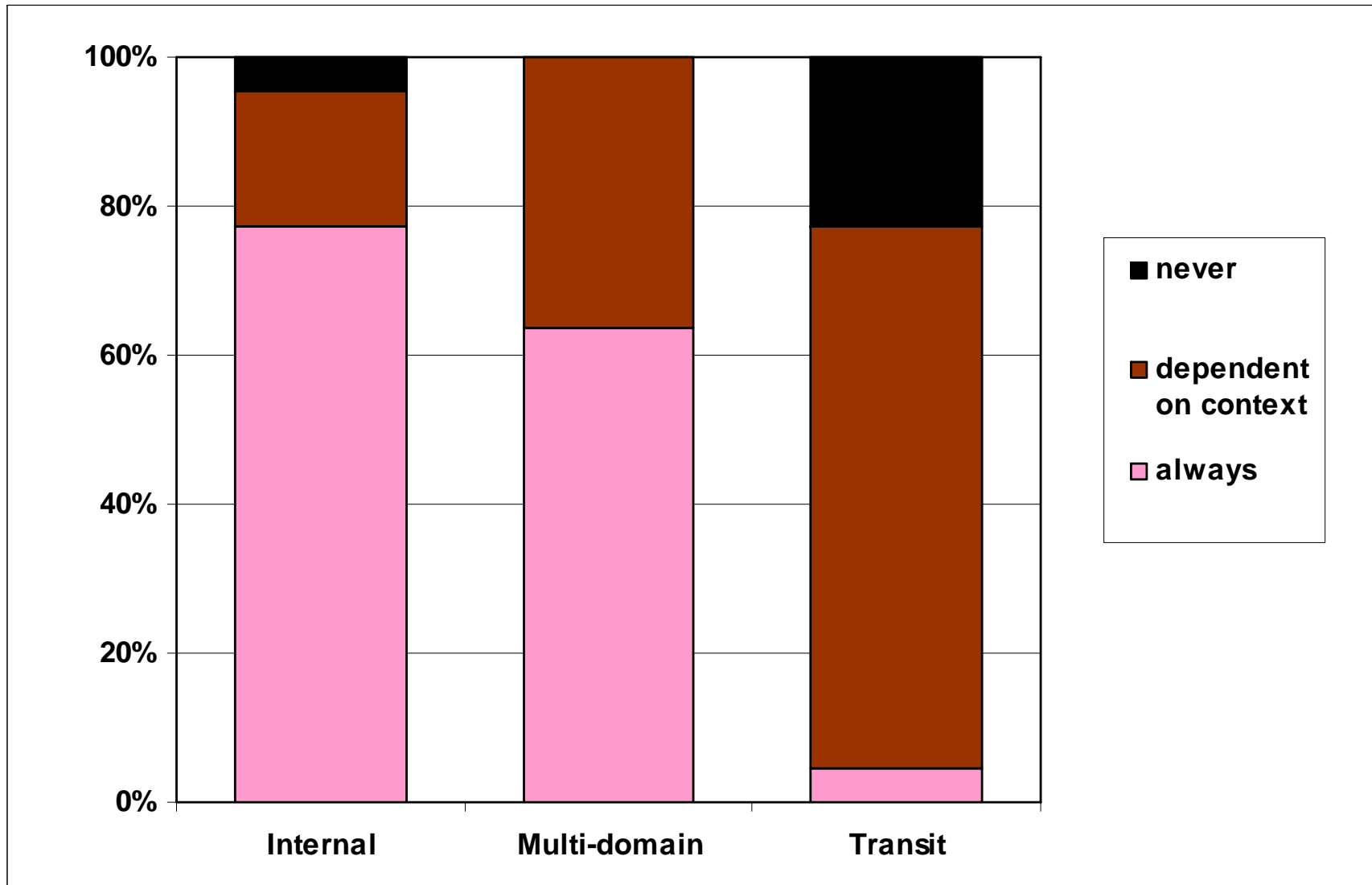
- **Anomaly classification (types and severity)**
- Tools for detecting anomalies
- Workflows and procedures (including LEA)

- **Multidomain anomaly:** at least one end host not belonging to your constituency
- **Transit anomaly:** all involved end host do not belong to your constituency, but traffic transits through your network
- **Internal anomaly:** all involved end hosts belong to your constituency

# Split of anomalies



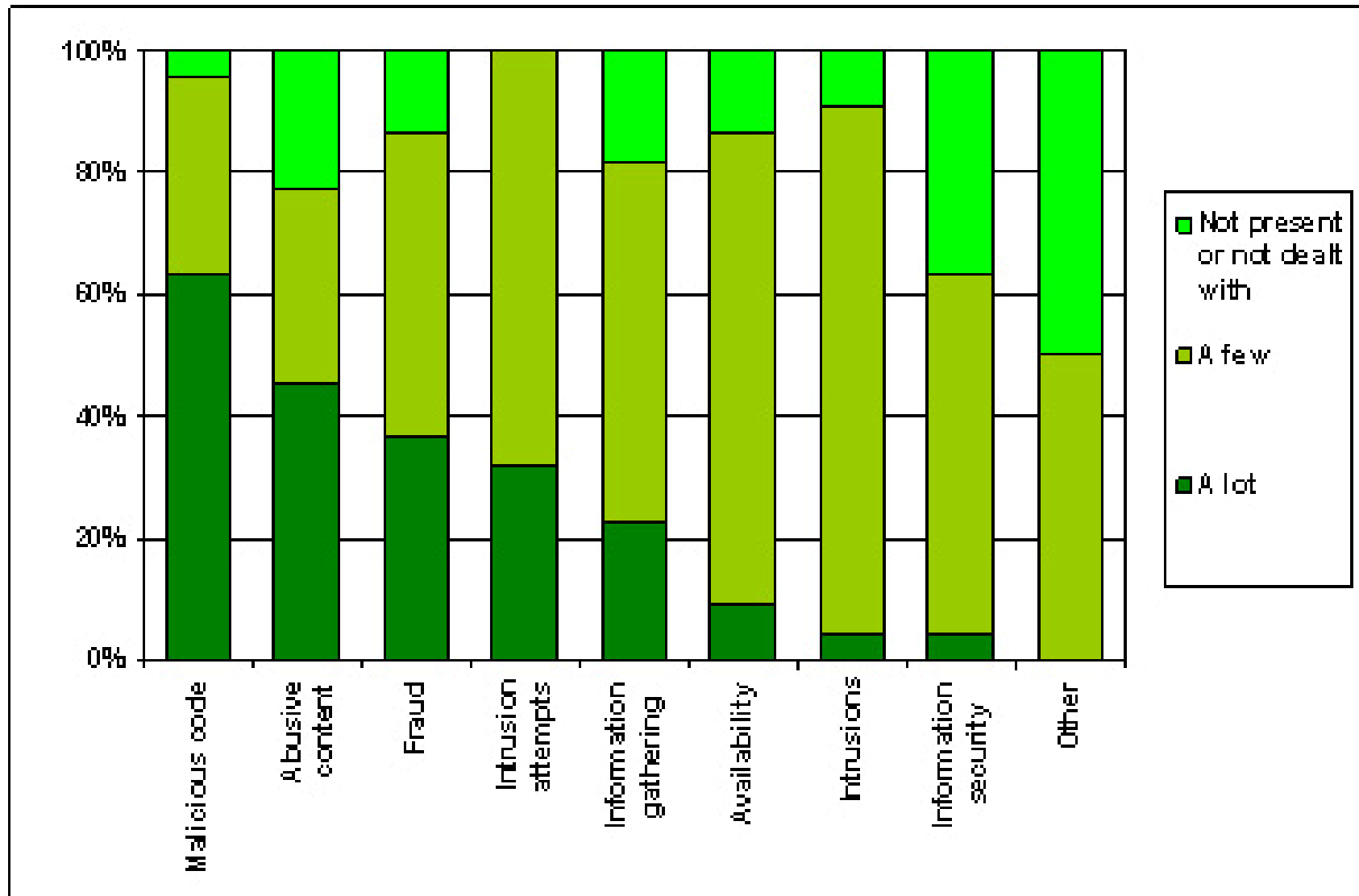
# Handling of different anomalies



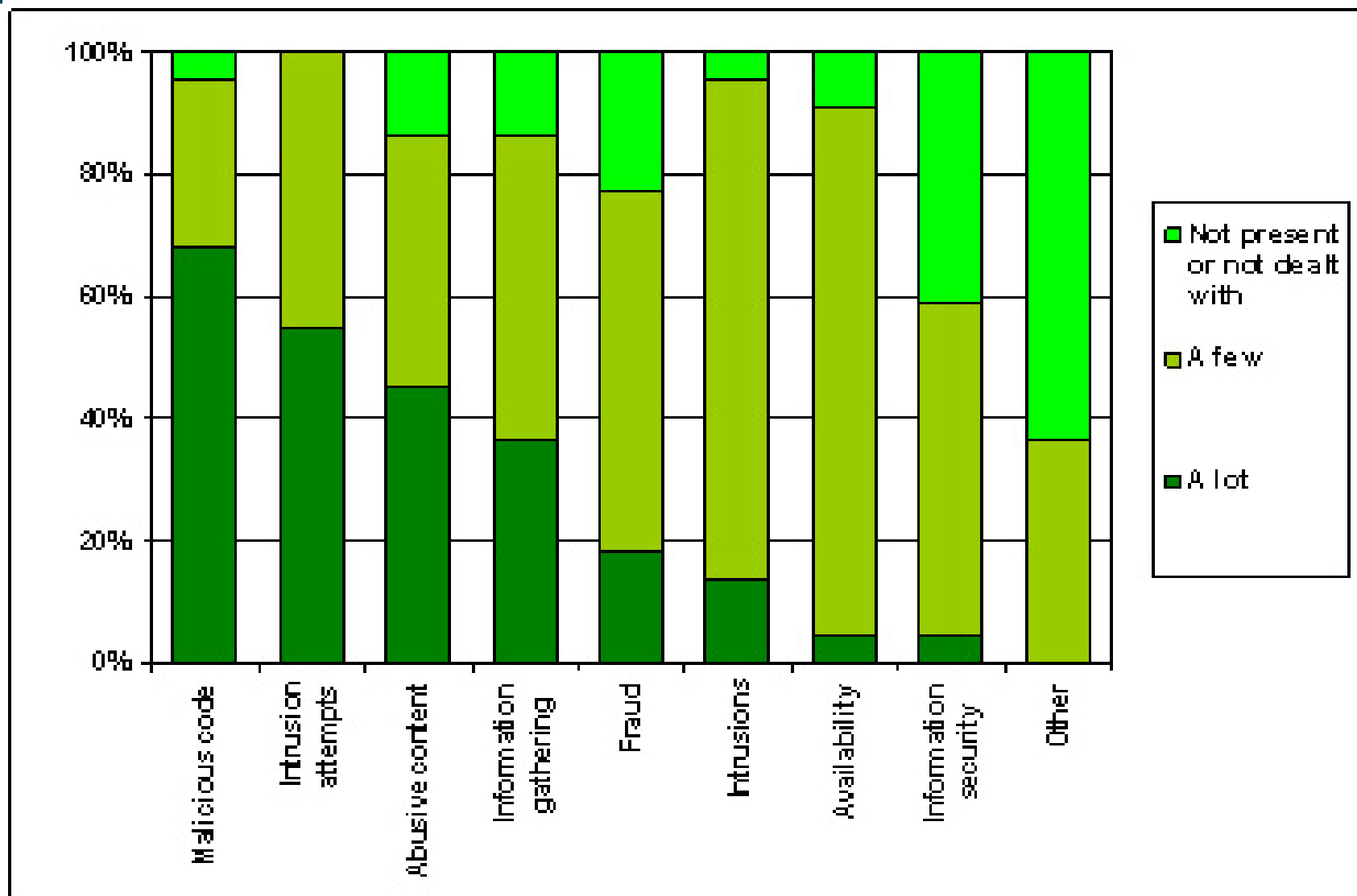
Average anomalies per day (total)

26,8

# Type of anomalies originating from the constituency

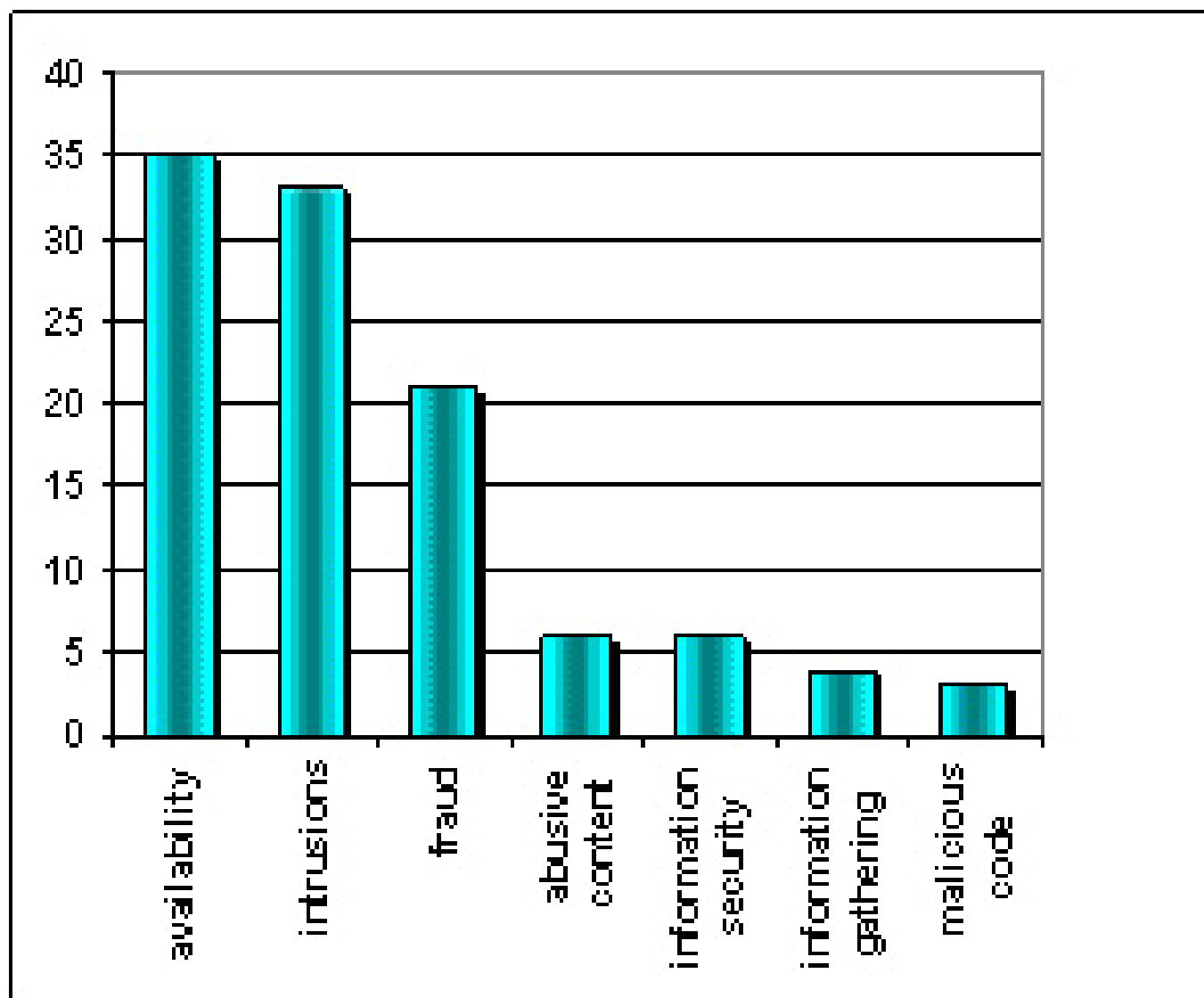


# Type of anomalies targeting the constituency

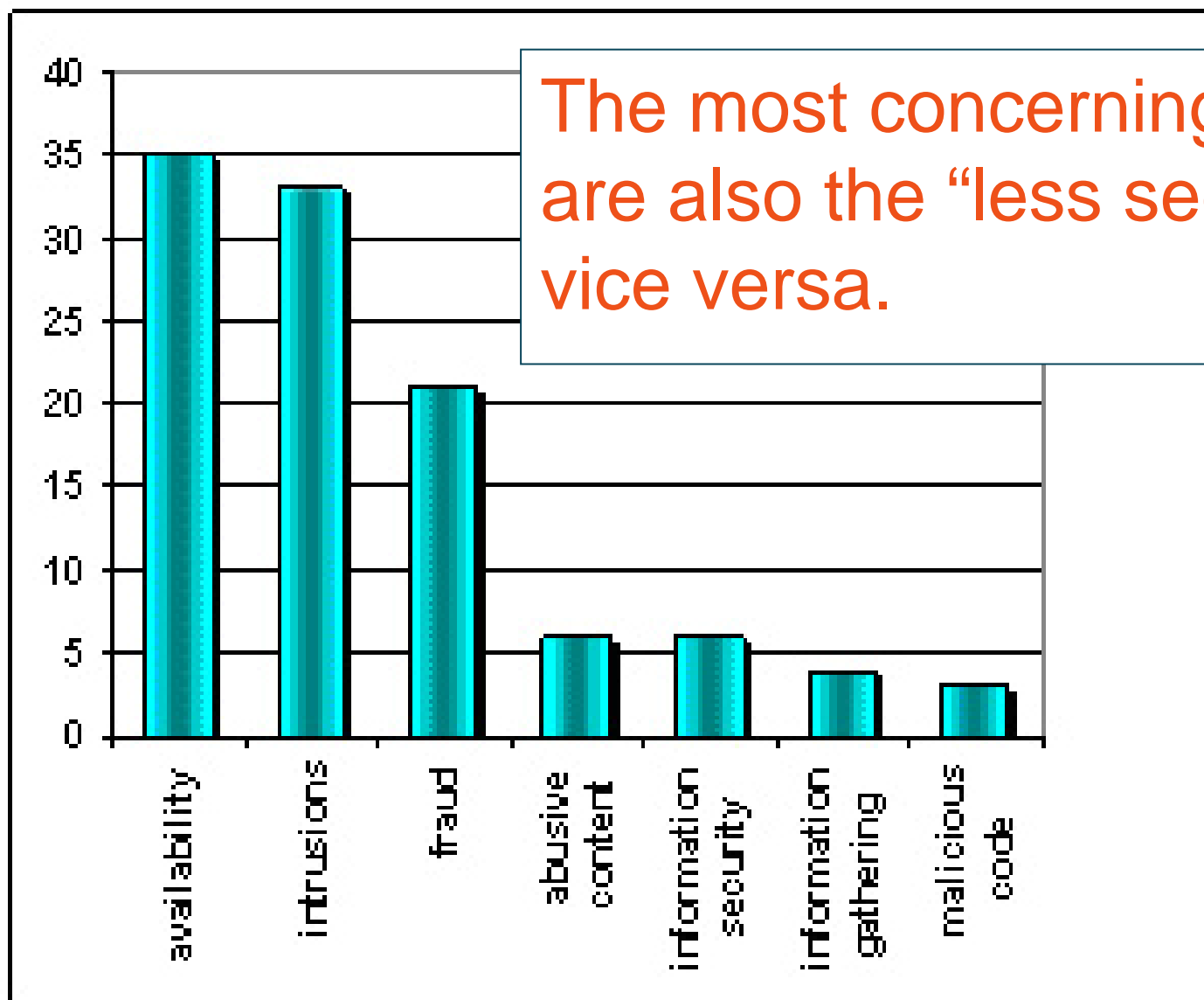


Incident types used by eCSIRT.net

# Most concerning types of anomalies



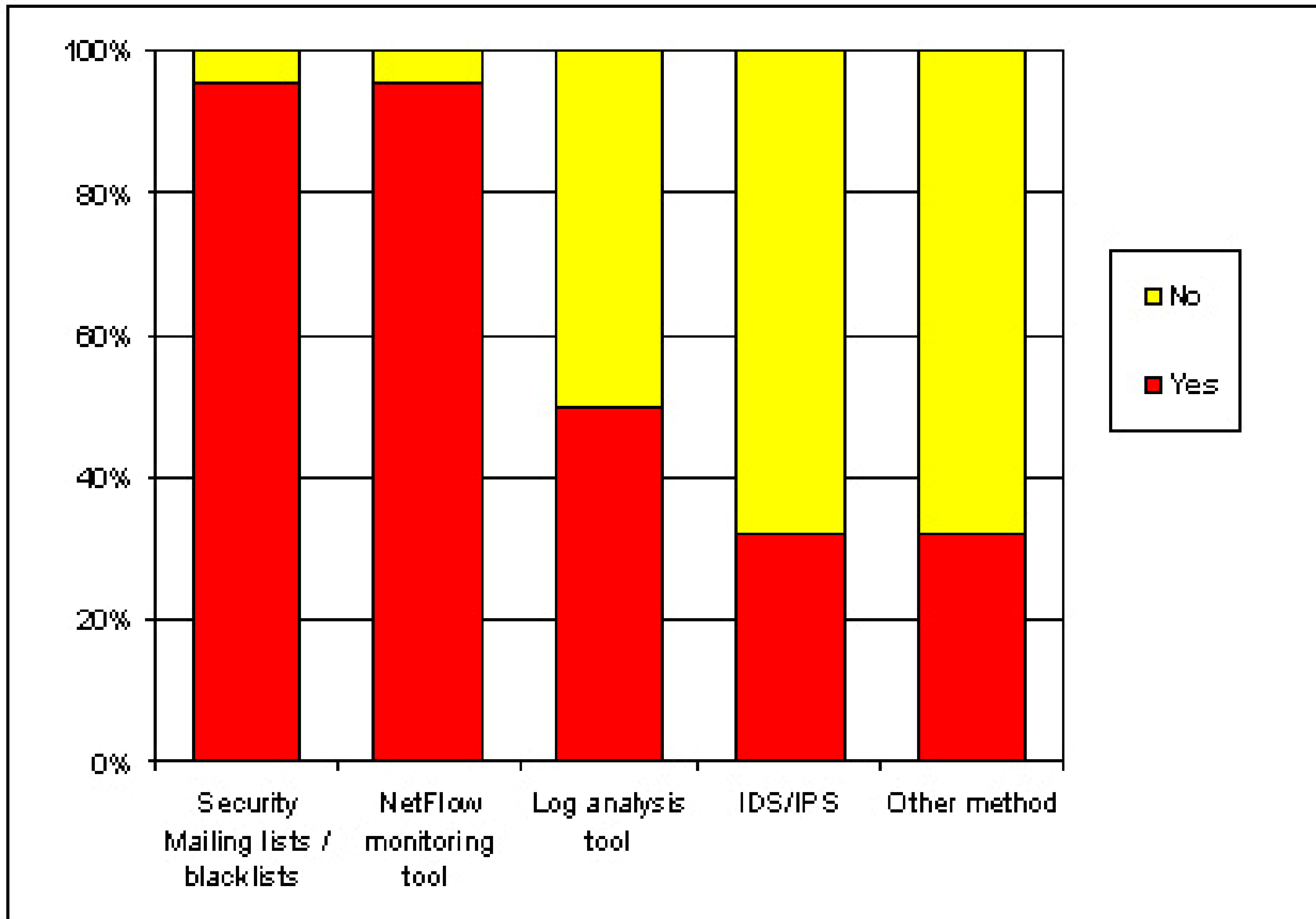
# Most concerning types of anomalies



The most concerning types are also the “less seen”, and vice versa.

- Anomaly classification (types and severity)
- **Tools for detecting anomalies**
- Workflows and procedures (including LEA)

# Anomalies detection methods

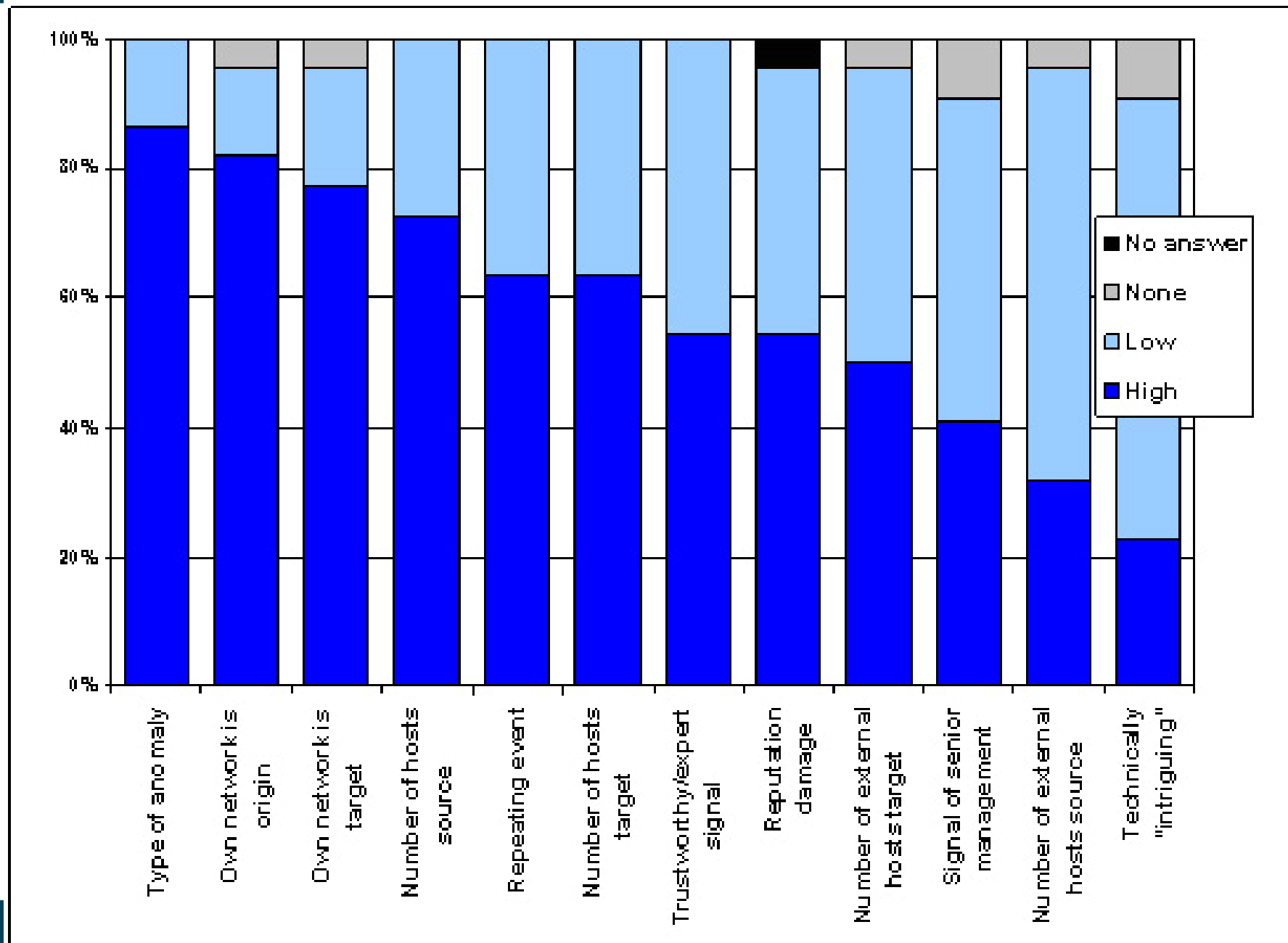


## Other anomalies detection methods

- Honeypots
- DNS Blackholing SPAM Traps
- Darkspace detectors
- Police reports
- DFN - CarmentiS
- Common sense & general intelligence 😊

- Anomaly classification (types and severity)
- Tools for detecting anomalies
- Workflows and procedures (including LEA)

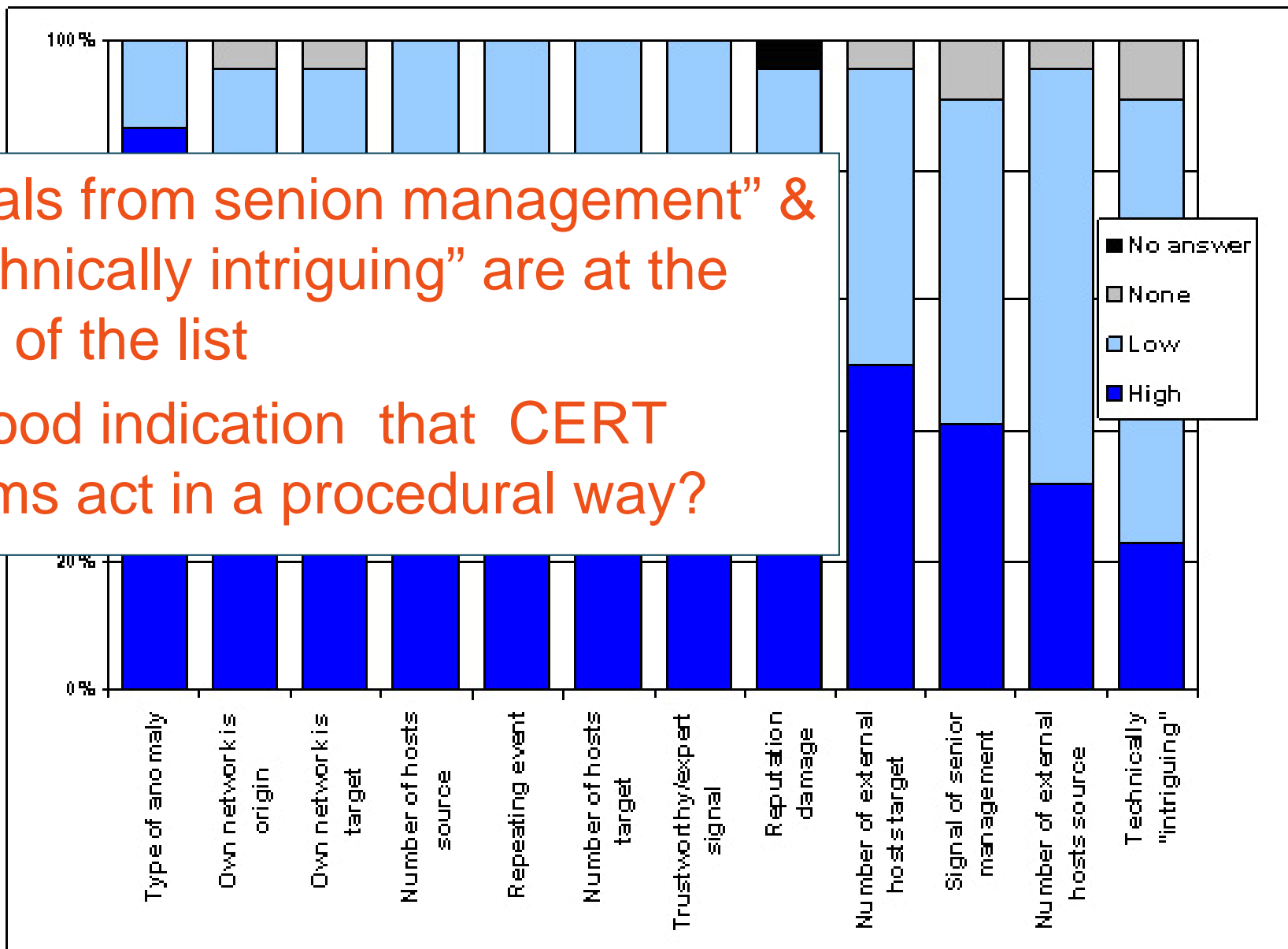
# Importance of factors to prioritize anomalies handling



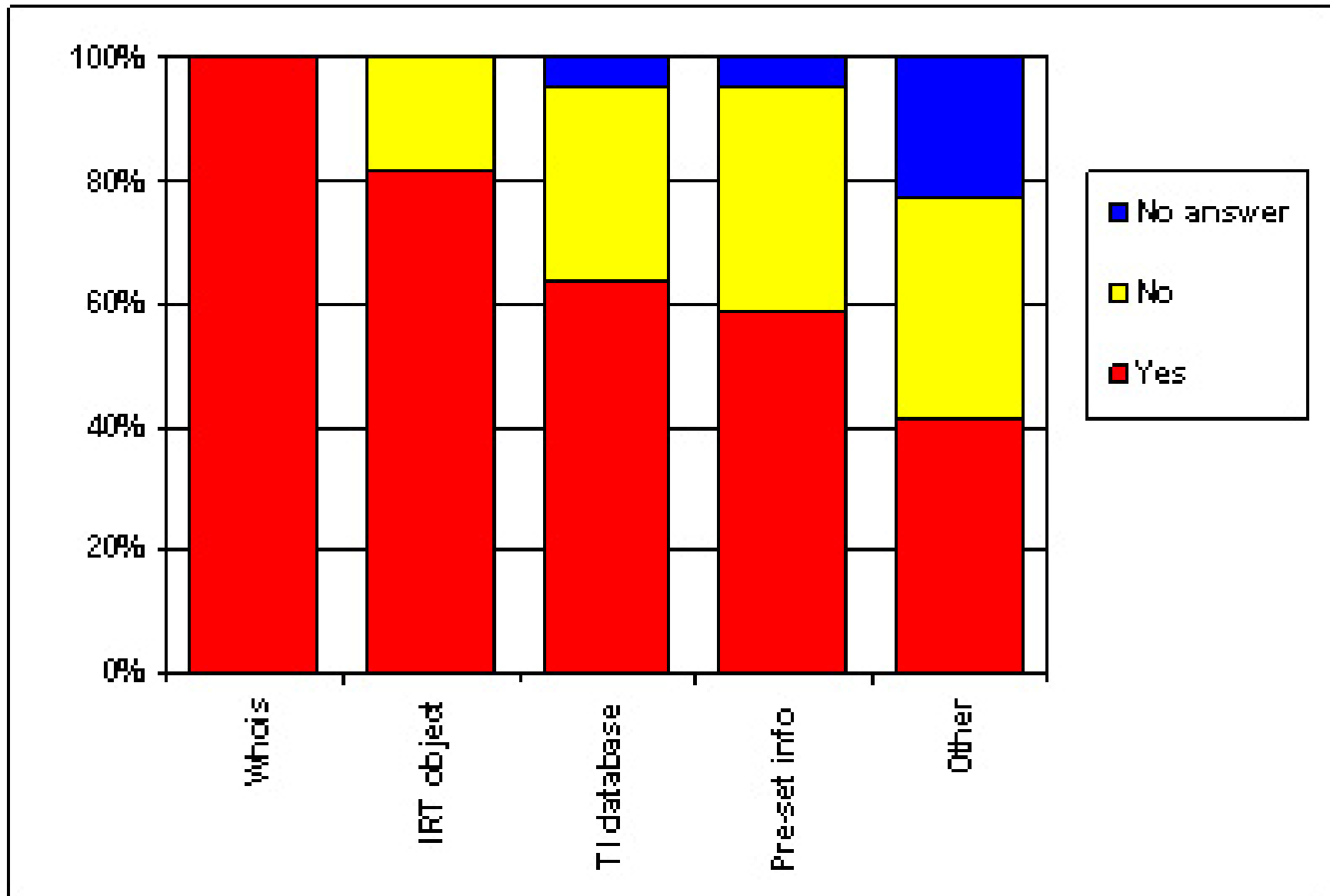
# Importance of factors to prioritize anomalies handling



“Signals from senior management” & “technically intriguing” are at the end of the list  
=> good indication that CERT teams act in a procedural way?



# How to identify the administrative foreign end?

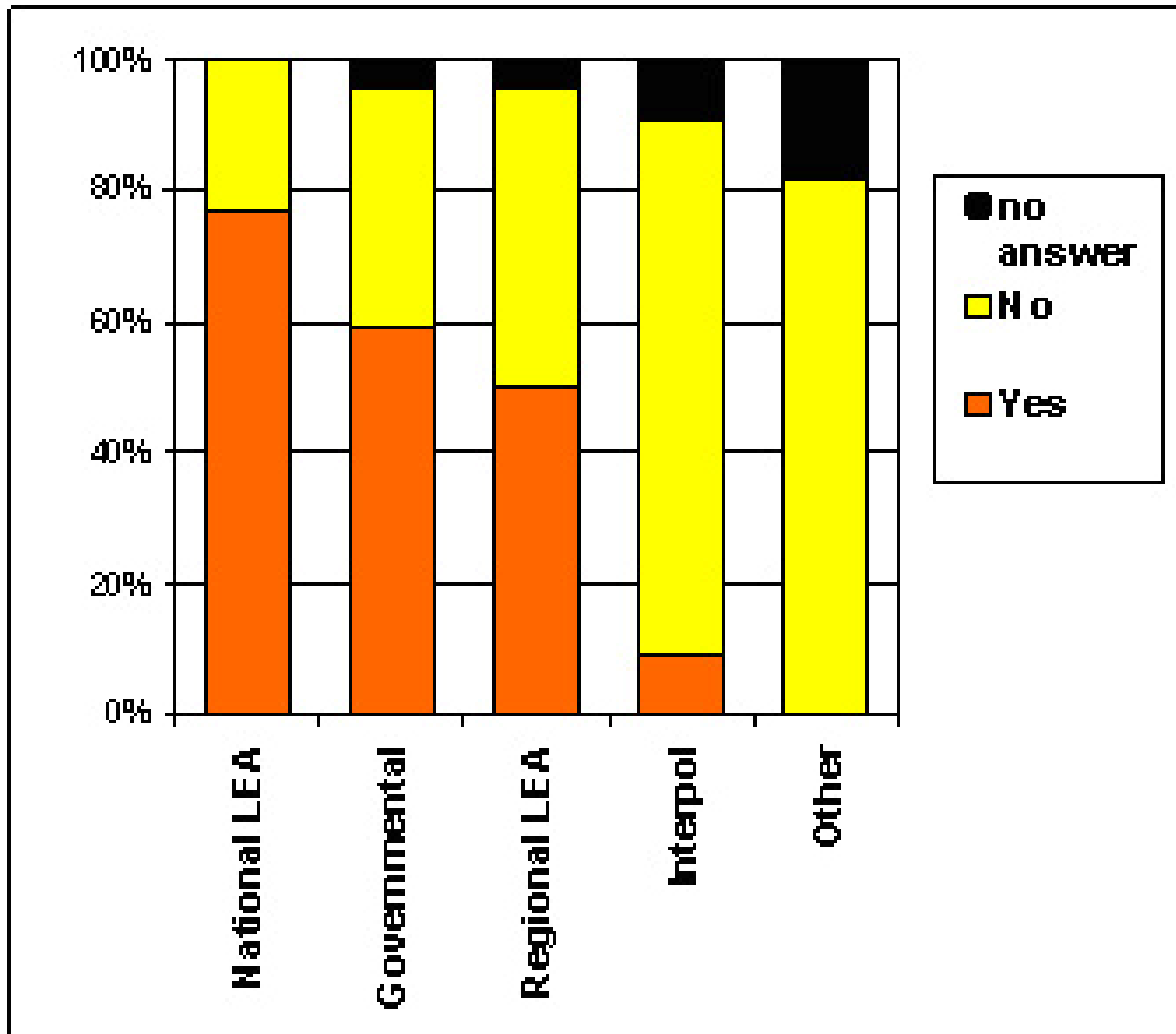


## Other methods to identify administrative foreign end



- Local, personal contacts
- FIRST contacts data base
- Business card collection
- Domain registry entries
- Google 😊

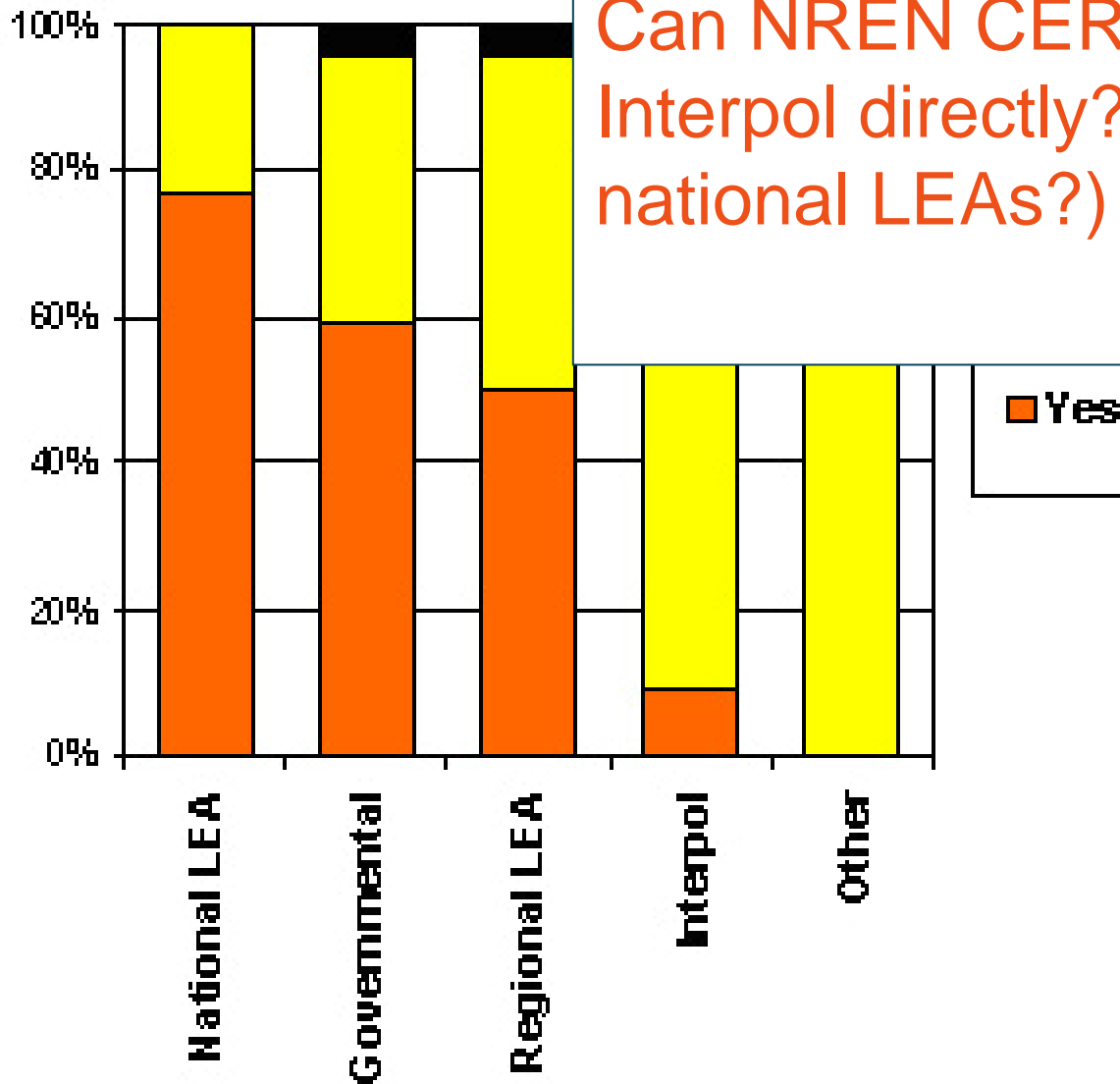
# Experience in cooperation with LEA



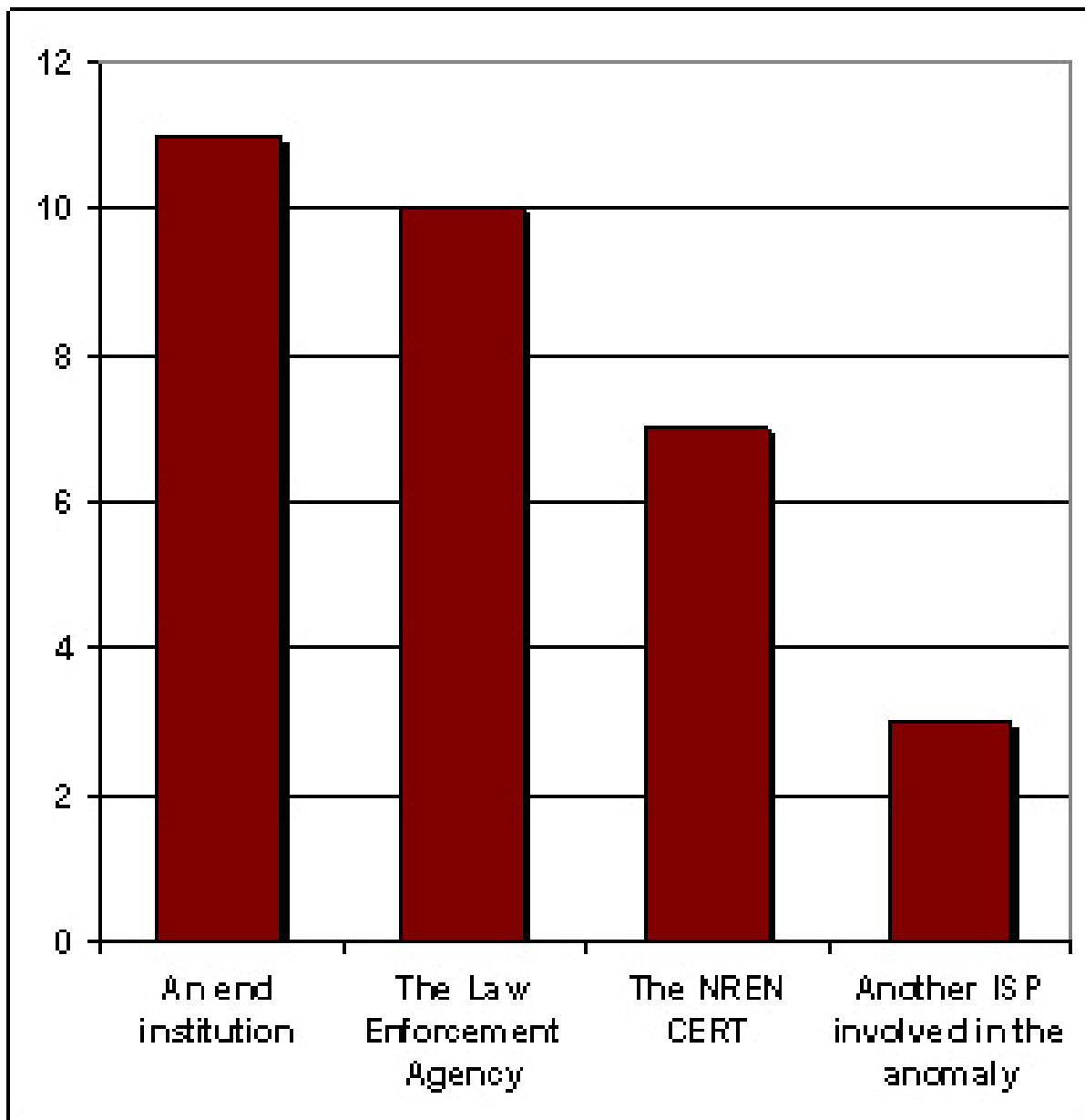
# Experience in cooperation with LEA



Can NREN CERTs cooperate with Interpol directly? (By-passing national LEAs?)



# Who initiates cooperation with LEA?



# More contributions?



- Your NREN has not replied yet???
  - Talk with us to find out!
  - It's still possible to contribute!
- Extend survey to other TF-CSIRT teams (non-NREN)?
  - If interested, contact:
    - [baiba@nic.lv](mailto:baiba@nic.lv) or [maurizio.molina@dante.net](mailto:maurizio.molina@dante.net)

**Thanks to all NRENs who  
replied !!!**

**Questions???**