CSIRT teams and their role in security II.

CEE Peering Day
18 – 19th March 2015
Petra Hochmannová – CSIRT.SK

CSIRT.SK

- **Ministry of Finance of the Slovak Republic**

- **DataCentrum**

  ➢ Organisation of the Ministry of Finance of the SR

  ➢ IT support centre

- **CSIRT.SK**

  ➢ Computer Security Incident Response Team Slovakia

  ➢ As an independent department of DataCentrum

  ➢ Established on July, 1st. 2009

  ➢ National/governmental CSIRT

Mission and activities

- **MISSION:**
  - ➢ To increase the protection of national information and communication infrastructure.

- **ACTIVITIES:**
  - ➢ Response to the information security incidents in Slovakia in cooperation with the owners and providers of impacted parts of the national critical infrastructure, telecommunication operators, ISPs, and other public bodies (police, investigators, and courts);
  - ➢ Awareness raising in the field of information security;
  - ➢ Cooperation with international counterparts and organizations;
  - ➢ Representation of Slovakia in the field of information security internationally.

CSIRT.SK

- Our Active Services:
  - Alerts & Warnings;
  - Incident response;
  - Design of countermeasures;
  - Analysis of ongoing computer security incidents;
  - Provide documentation to help handle certain common incidents;
  - Coordinate responses to incident handling;
  - Risk and vulnerability analysis;
  - Response and analysis of malicious software.
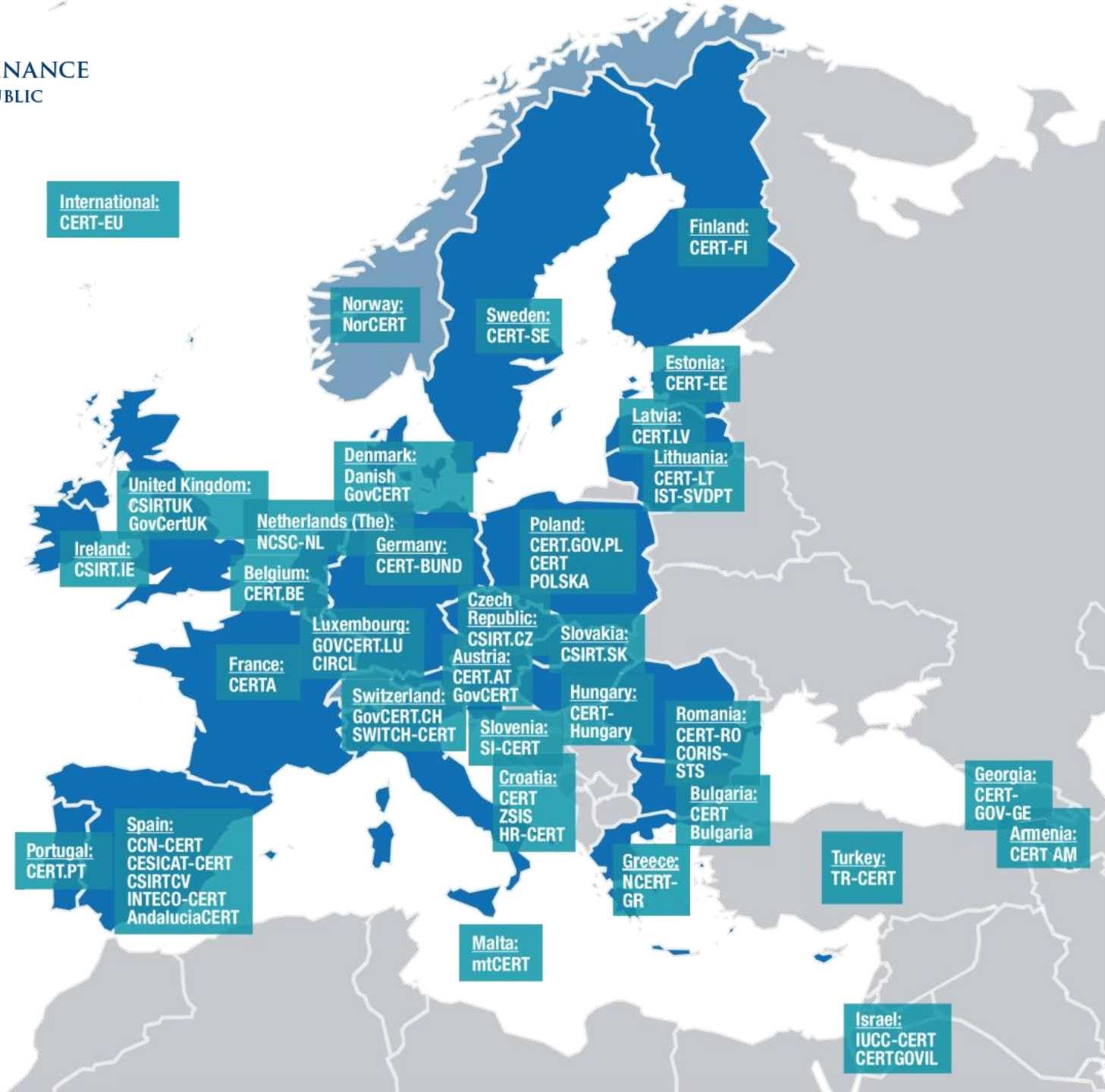
CSIRT.SK

- Our Proactive Services:
  - EXERCISES
    - International exercises
    - Slovak Information Security Exercise;
    - Education and raising awareness in the field of information security;
    - Building technical capabilities;
    - Exercise on critical information infrastructure protection.
  - Penetration testing
  - Threats Monitoring and consultation in the field of ICT
  - Audits
  - Education and training activities

MINISTRY OF FINANCE
OF THE SLOVAK REPUBLIC

Iceland:
CERT.IS

International:
CERT-EU

Finland:
CERT-FI

Norway:
NorCERT

Sweden:
CERT-SE

Estonia:
CERT-EE

Latvia:
CERT.LV

Lithuania:
CERT-LT
IST-SVDPT

Denmark:
Danish
GovCERT

United Kingdom:
CSIRTUK
GovCertUK

Netherlands (The):
NCSC-NL

Germany:
CERT-BUND

Poland:
CERT.GOV.PL
CERT
POLSKA

Ireland:
CSIRT.IE

Belgium:
CERT.BE

Czech
Republic:
CSIRT.CZ

Slovakia:
CSIRT.SK

Luxembourg:
GOVCERT.LU
CIRCL

Austria:
CERT.AT
GovCERT

France:
CERTA

Switzerland:
GovCERT.CH
SWITCH-CERT

Hungary:
CERT-
Hungary

Romania:
CERT-RO
CORIS-
STS

Georgia:
CERT-
GOV-GE

Slovenia:
SI-CERT

Croatia:
CERT
ZSIS
HR-CERT

Bulgaria:
CERT
Bulgaria

Armenia:
CERT AM

Spain:
CCN-CERT
CESICAT-CERT
CSIRTCV
INTECO-CERT
AndaluciaCERT

Portugal:
CERT.PT

Greece:
NCERT-
GR

Turkey:
TR-CERT

Malta:
mtCERT

Israel:
IUCC-CERT
CERTGOVIL

National and International Cooperation

- **Cooperation with:**
  - Public Administration
  - Academia
  - Owners and Operators of CI
  - Teleco Operators
  - Internet Service Providers
  - CSIRT/CERT community
  - Financial Sector
  - Businesses
  - International organizations

Data Sources

1. Impacted Institutions

2. CERT Community

3. Automated Systems

Foreign Data Sources

Own Monitoring

Data Sources

Amount of incidents reports - year 2014
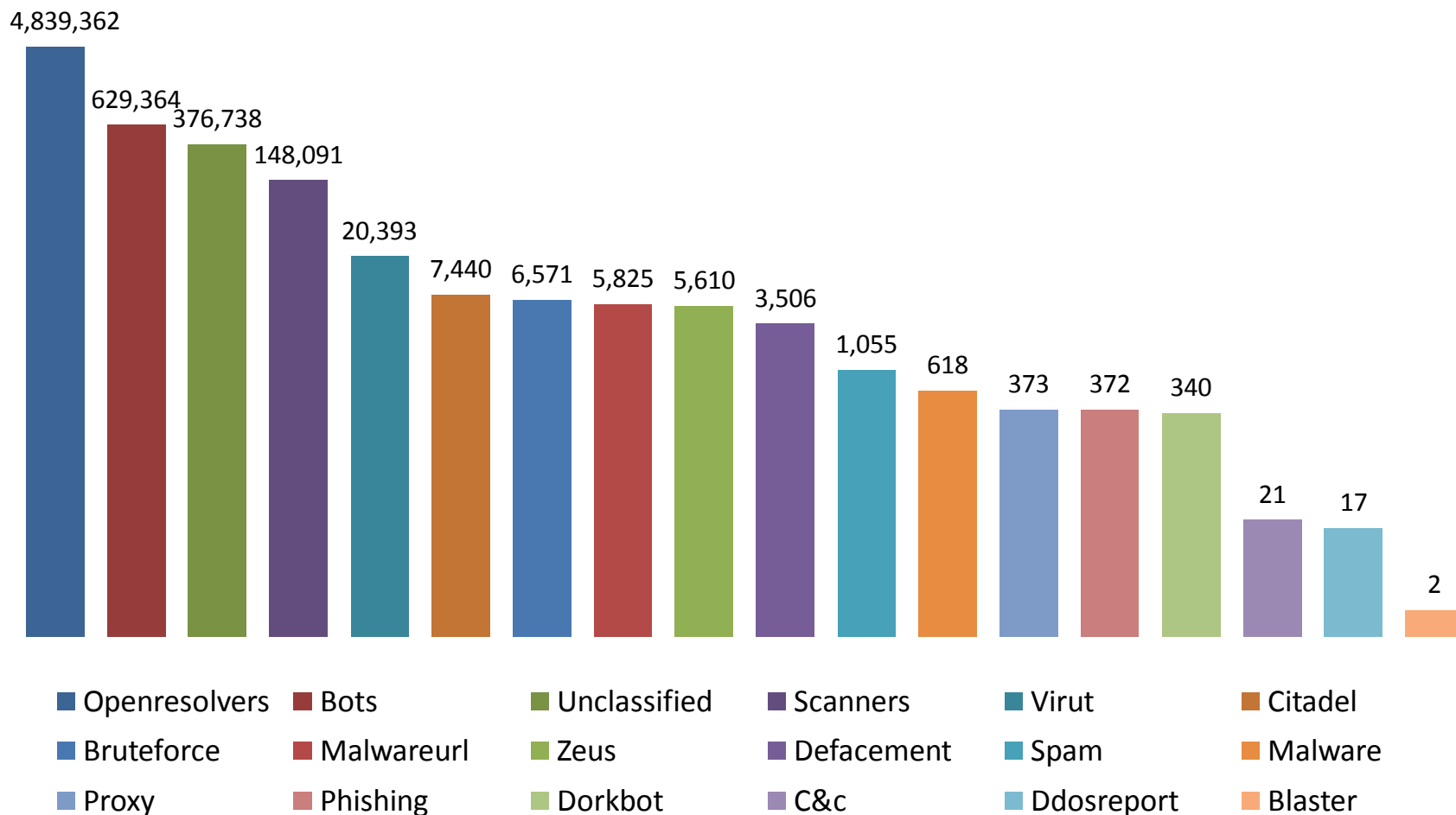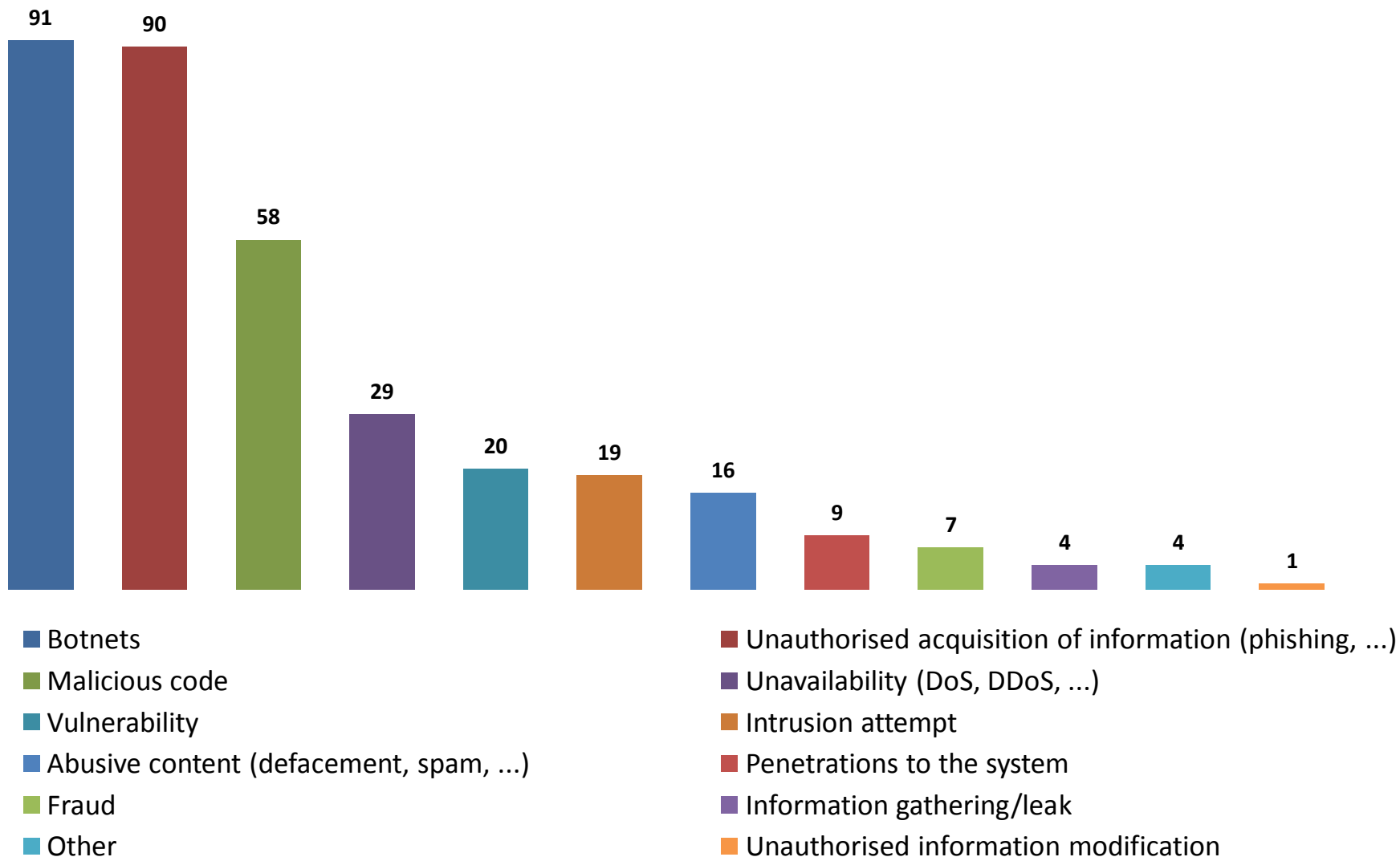
Bar chart of incident reports for year 2014:

- Openresolvers: 4,839,362
- Bots: 629,364
- Unclassified: 376,738
- Scanners: 148,091
- Virut: 20,393
- Citadel: 7,440
- Bruteforce: 6,571
- Malwareurl: 5,825
- Zeus: 5,610
- Defacement: 3,506
- Spam: 1,055
- Malware: 618
- Proxy: 373
- Phishing: 372
- Dorkbot: 340
- C&c: 21
- Ddosreport: 17
- Blaster: 2

DataCentrum

Cintorínska 5, 814 88 Bratislava

www.csirt.gov.sk

tel: 02 59 278 205, 02 59 278 454

e-mail: info@csirt.gov.sk

incident@csirt.gov.sk