ITUEvents

# ITU Regional Cybersecurity Forum for Europe and CIS

27 – 28 February 2020
Sofia, Bulgaria

Follow us on twitter: @ITU_EUR & @ITUMoscow
www.itu.int/go/EURCIS_CSForum20

ITU Regional Initiative for Europe on enhancing trust and confidence in the use of ICTs

ITU Regional Initiative for CIS on the development and regulation of infocommunication infrastructure to make cities and human settlements inclusive, safe, and resilient

POLICIES & STRATEGIES | CERTIFICATION FRAMEWORKS | DATA PROTECTION | SECURITY CHALLENGES | 5G, eSIM IoT, AI

Hosted and co-organized by:

REPUBLIC OF BULGARIA
State e-Government Agency

REPUBLIC OF BULGARIA
Ministry of Transport, Information Technology and Communications

ITU

REPUBLIC OF BULGARIA

State e-Government Agency

# Incident Response and Management

**Vasil Grancharov**

**Director of Network and Information Security Directorate,**

**Head of CERT Bulgaria**

**vgrancharov@e-gov.bg**

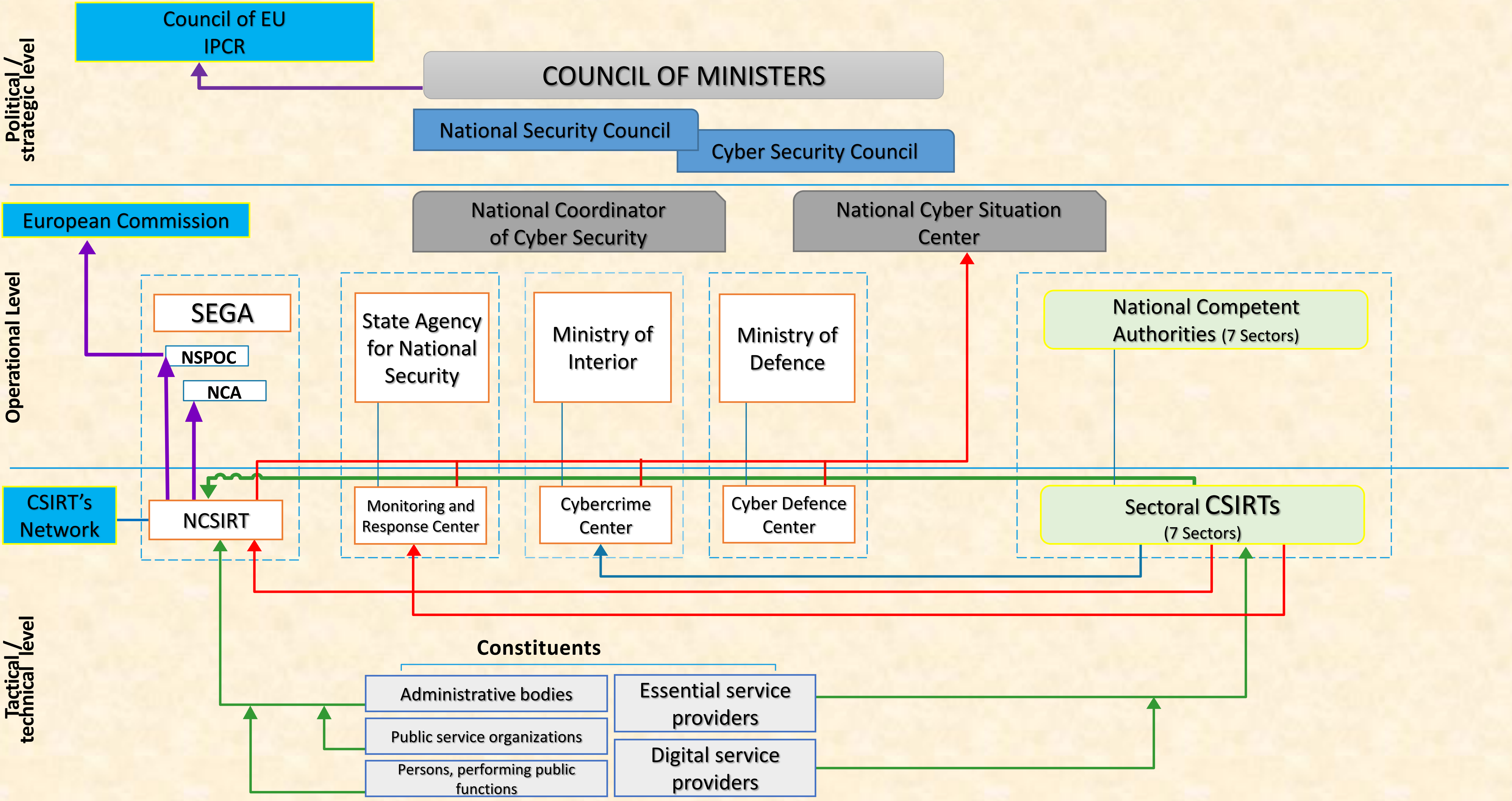
# Policies in NIS

# Scope of the NIS Directive (2016/1148)

- Achieving high common level of network and information security
- Building trust
- Capacity building
- Development of capabilities
- Developing public private partnership
- Pan-European collaboration on the matters of cyber incident preparedness and management

# What has been done in Bulgaria?

- The Cyber Security Act;
- Designation of the administrative bodies, to which the National Competent Authorities on network and information security are to be created;
- Adoption of a methodology for the identification of the operators of essential services in accordance with the requirements of the Cyber Security Act;
- Identification of the Operators of Essential Services;
- Adoption of the Ordinance for the Minimal Requirements of Network and Information Security
- Round table with the NCA and the OES for in regard to clarification of their roles and responsibilities in accordance with the Cyber Security Act;
- Cyber Security Council and the Regulations for its operation.
- A methodology named “Methods and rules for compliance assessment of the network and information security measures in accordance with the ordinance of minimal requirements for network and information security”.


Political / strategic level
Council of EU
IPCR
COUNCIL OF MINISTERS
National Security Council
Cyber Security Council
Operational Level
European Commission
National Coordinator of Cyber Security
National Cyber Situation Center
SEGA
NSPOC
NCA
State Agency for National Security
Ministry of Interior
Ministry of Defence
National Competent Authorities (7 Sectors)
CSIRT's Network
NCSIRT
Monitoring and Response Center
Cybercrime Center
Cyber Defence Center
Sectoral CSIRTs (7 Sectors)
Tactical / technical level
Constituents
Administrative bodies
Public service organizations
Persons, performing public functions
Essential service providers
Digital service providers

# SERVICES BY SECTORS - SUBSECTORS

## ENERGY

**Electricity**

production, transmission, distribution, sale

**Oil**

extraction, transportation, refining, storage

**Gas**

extraction, transmission, distribution, storage

## TRANSPORT

- Air transport
- Rail transport
- Water transport
- Road transport

## BANKING

- lending
- investment intermediation

## FINANCIAL MARKET INFRASTRUCTURES

- operating or managing trading venues
- Central counterparties

## HEALTH SECTOR

- health counseling services
- emergency medical care
- provision of beds,
- Provision of life support activities

## DRINKING WATER SUPPLY AND DISTRIBUTION

- transfer / delivery of drinking water
- distribution of drinking water
- drinking water treatment

## DIGITAL INFRASTRUCTURE

- IXPs
- DNS service providers
- TLD name registries

# Reporting of incidents - Annex 7 to Art. 31, para. 2

**Up to 2 hours**

Initial notification of an incident including::

- Details of the person submitting the notification
- The organization that is affected
- Contact person (for incident resolution purposes)
- Date and Time
- Type of incident
- Short description of incident
- Cross-border impact
- Impact on other essential services
- Impact system (to be completed if information is available)
- Source of attack
- Mitigation measures
- Public affairs recommendation

**Up to 5 days**

Send detailed information about:

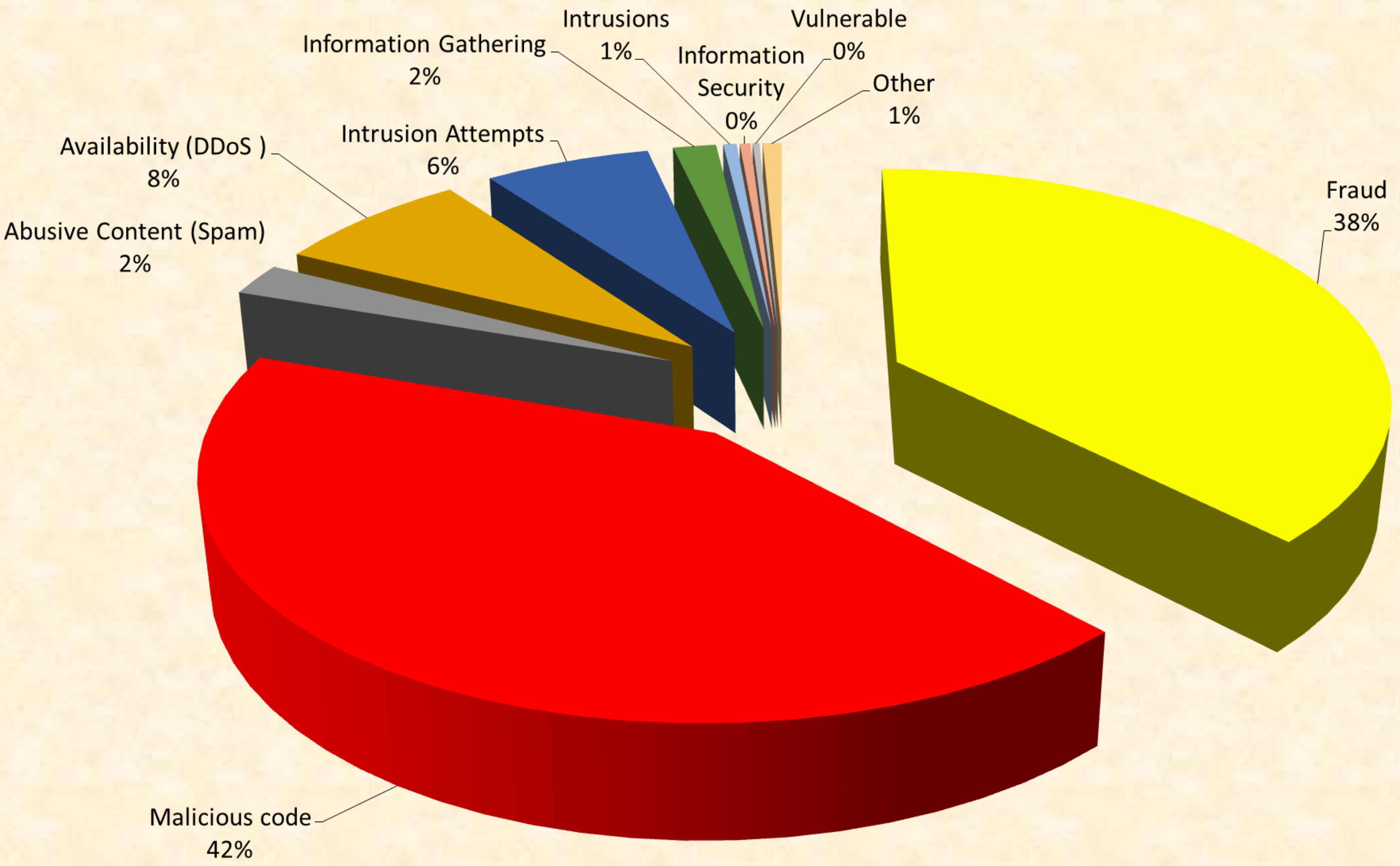
- Attack Mechanism
- Actions taken
- Need for corrective action
- Analysis of artifacts
- Public affairs recommendation

# Reactive Services (incident handling)

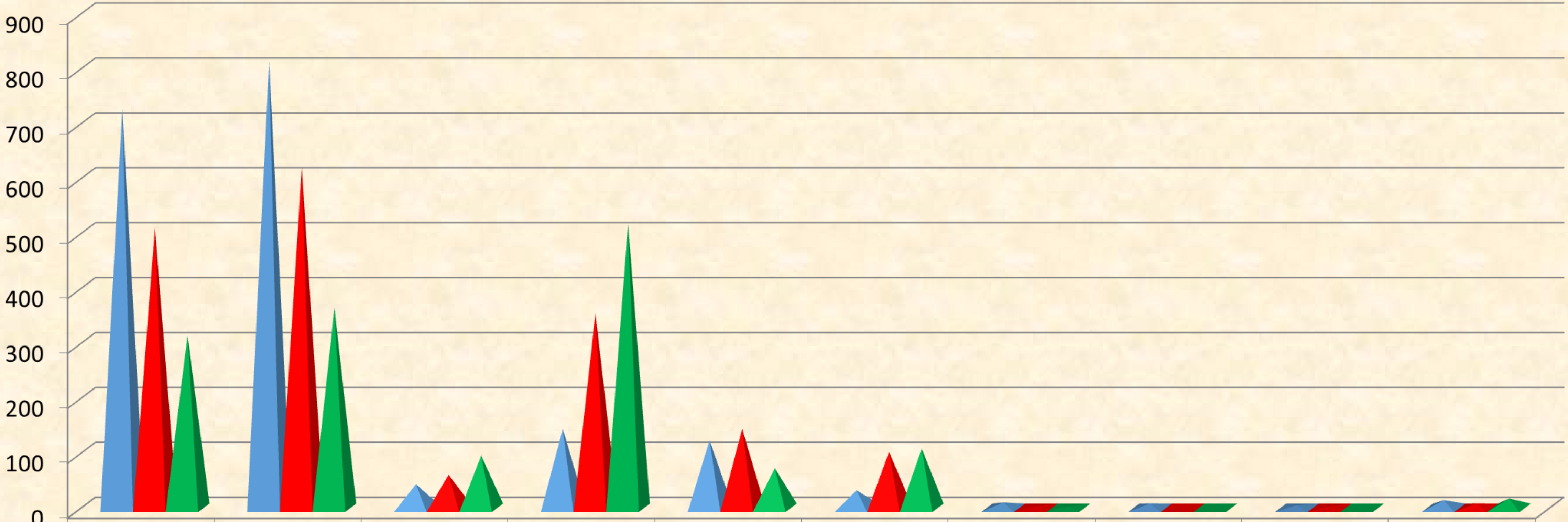
# Incidents handled for the last three years

| | 2019 | 2018 | 2017 |
|---|---|---|---|
| Received signals | 3 311 | 2 382 | 1 951 |
| Affected IP addresses | 2 288 293 | 640 265 | 139 192 |
| Sent emails | 21 883 | 12 560 | 5 174 |
| Registered incidents | 1 919 | 1 804 | 1 491 |

# Type of incident 2019



# Registered incidents on annual basis



| | Fraud | Malicious code | Abusive Content (Spam) | Availability (DDoS ) | Intrusion Attempts | Information Gathering | Intrusions | Information Security | Vulnerable | Other |
|---|---|---|---|---|---|---|---|---|---|---|
| 🟦 2019 | 726 | 814 | 43 | 144 | 123 | 32 | 10 | 8 | 5 | 14 |
| 🟥 2018 | 510 | 620 | 60 | 354 | 144 | 102 | 3 | 0 | 3 | 8 |
| 🟩 2017 | 314 | 364 | 95 | 518 | 72 | 108 | 3 | 0 | 0 | 17 |

# Types of incidents. Comparison between 2018 and 2019

| | |
|---|---|
| Fraud (Phishing) | ⬆ |
| Malicious code | ⬆ |
| Spam | ⬇ |
| DDoS | ⬇ |
| Intrusions attempts | ⬇ |
| Information Gathering | ⬇ |
| Intrusion | ⬆ |
| Unauthorized access and modification of information | ⬆ |
| Vulnerabilities | ⬆ |
| Others | ⬆ |

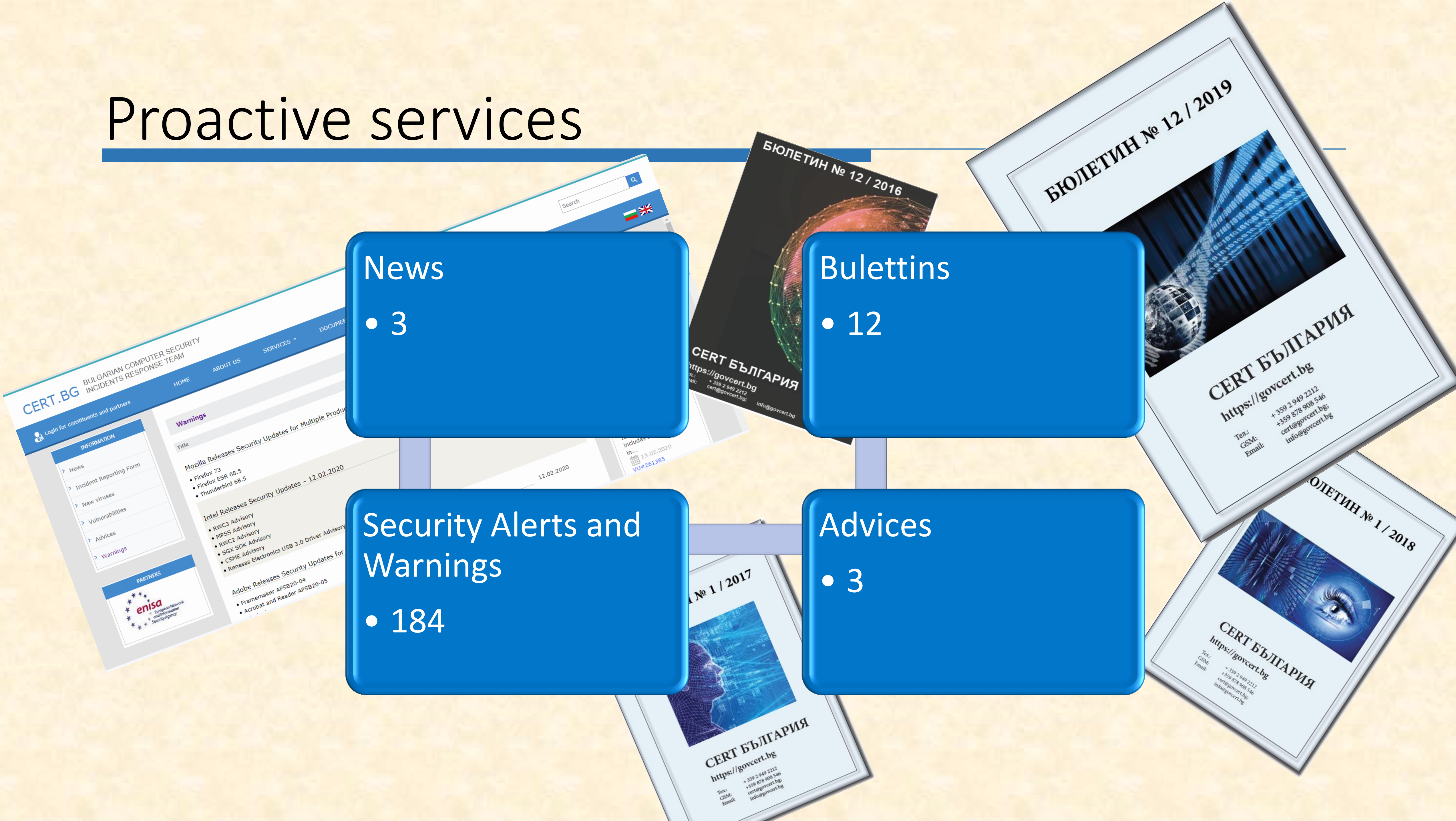
# Proactive services

- Scanning for vulnerabilities of sites, owned by our constituents – 11
- Training of the NIS employee of the administrative bodies, NCA, OES, and DSP ~ 650 people
- Revision of the compliance with the requirements in accordance with The Ordinance for the minimal requirements for NIS.

# Proactive services

- Instructions on how to reduce the risk of a potential security breach and data theft, as well as a plan for the implementation of the guidelines with which increase the level of network and information security
- Guidelines for raising the level of network and information security in regard to local and European elections.
- Exemplary standard operating procedures in cases of network and information security incidents.
- Self-assessment table.

# Proactive services



News

- 3

Bulettins

- 12

Security Alerts and Warnings

- 184

Advices

- 3

CERT.BG BULGARIAN COMPUTER SECURITY INCIDENTS RESPONSE TEAM

Search

HOME ABOUT US SERVICES DOCUMEN

Login for constituents and partners

INFORMATION

- News
- Incident Reporting Form
- New viruses
- Vulnerabilities
- Advices
- Warnings

PARTNERS

enisa European Network and Information Security Agency

Warnings

Title

Mozilla Releases Security Updates for Multiple Produ

- Firefox 73
- Firefox ESR 68.5
- Thunderbird 68.5

12.02.2020

Intel Releases Security Updates – 12.02.2020

- RWC3 Advisory
- MPSS Advisory
- RWC2 Advisory
- SGX SDK Advisory
- CSME Advisory
- Renesas Electronics USB 3.0 Driver Advisory

Adobe Releases Security Updates for

- Framemaker APSB20-04
- Acrobat and Reader APSB20-05

includes in 13.02.2020 VU#261385

# COOPERATION

- International
  - CSIRT Network (NIS Directive)
  - Cooperation Group (NIS Directive)
- National
  - ISP
  - Law Enforcement
    - ✓ Cybercrime
    - ✓ SEGA

# Projects

# CEF Programme
# 2018-BG-IA-0114 - Capacity Building and  Services Enhancement of CERT Bulgaria (CBSEC-BG)

| | |
|---|---|
| **Total eligible costs:** | **1 298 495 EUR** |
| **CEF-Telecom financing:** | **973 872 EUR** |
| **Duration:** | **24 Months** |

| **№** | **Activity title** |
|---|---|
| 1 | Equipping a Centre for national and international cyber exercises |
| 2 | Equipping a Malware analysis laboratory |
| 3 | Equipping a Forensic analysis laboratory |
| 4 | Building a National CSIRT Network |
| 5 | Joining the MeliCERTes Core Service Platform |
| 6 | Development of a system for monitoring and storage of materials related to the network and information security |

# Internal Security Fund 2014-2020
# BG65ISNP001-6.007-0002-C01 - Building Components of the National Cybersecurity System

| | |
|---|---|
| **Total eligible costs:** | **10 630 098.57 BGN** |
| **Financing by Internal Security Fund:** | **7 972 573.93 BGN** |
| **Duration:** | **41 Months** |

| **№** | **Activity title** |
|---|---|
| 1 | Establishment of a National Cybersecurity Coordination and Organizational Network |
| 2 | Establishment of a National Cyber-Situational Center |
| 3 | Establishment of a National Cybercrime Center |
| 4 | Establishment and development of a National Computer Security Incident Response Team (NCSIRT) |

- **H2020-SU-DS-2018 SU-DS01-2018 Innovation Action**

- **Topic SU-DS01-2018 “Cybersecurity preparedness – cyber range, simulation and economics”**

- **DURATION: 10/2019 – 09/2022**

- **GRANT Agreement No. 833673**

- **22 partners**
- **9 EU member states**
- **Overall budget ≈ 7,3 m**
- **Actual budget ≈ 5,9 m**

FORESIGHT

## Project Coordinator

KEMEA

## Partners

EUROPEAN DYNAMICS

iti Information Technologies Institute

Cybercrime Research Institute

inCITES Consulting S.A.R.L

CENTRIC
Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

MINDS & SPARKS

Abertay University

AIRBUS

OPEN UNIVERSITY OF CYPRUS

ECOLE NAVALE

CYBEXER TECHNOLOGIES

ATHENS
INTERNATIONAL AIRPORT
ELEFTHERIOS VENIZELOS

THALES

РАЗПРЕДЕЛЕНИЕ

CERT.BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

ИНСТИТУТ ПО ОТБРАНА

ieit

ESO

University of Strathclyde Glasgow

UNIVERSITY OF PORTSMOUTH

рахмат
danke
謝謝
ngiyabonga
spas
teşekkür ederim
Баярлалаа
mersi
kia ora
barka
welalin
tack
mahalo
tapadh leat
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
kiitos
dankie
nanni
nandri
dhanyavad
thank you
gracias
хвала
asante
manana
obrigada
tenki
murakoze
bedankt
bayarlalaa
gracie
hvala
mauruuru
köszönöm
akun dankon aciu
enkosi
djiere dieuf
tau
mochchakkeram
дякую
mamnun
chokrane
dziękuję
chnorakaloutioun
gratias ago
gracies
sulpáy
taiku
go raibh maith agat
sobodi
dekuji
sagolun
sukriya
kop khun krap
arigatô
takk
dakujem
trugarez
obrigado
mèsi
didi madloba
ありがとう
tanemirt
grazie
najis tuke
kam sah hamnida
rahmat
terima kasih
rahmet
ευχαριστώ
diolch
dhanyavadagalu
shukriya
merce
мерси
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci