CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

“Regulatory framework for cybersecurity operations and cooperation”.

CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

Summary

General aspects

Global regulatory framework

European regulatory framework Operation and Cooperation

Romanian approach

1. Who is CERT-RO
2. Reports on alerts & incidents
3. Examples of CERT-RO work

Why cyber security

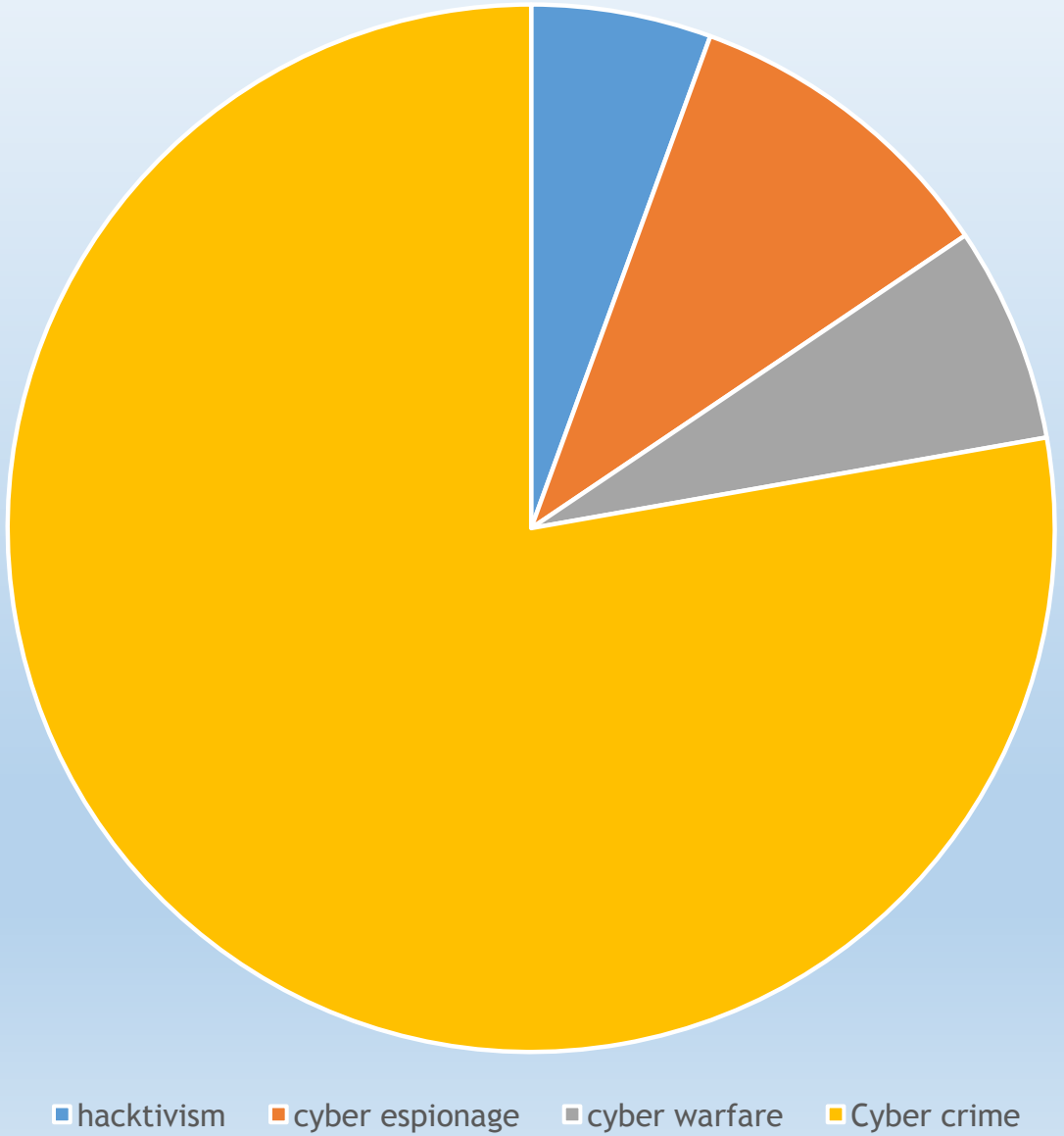
Cyberattacks costs:

Cost/year:	400 billion dollars;
2019 Projections:	2.1 trillion dollars

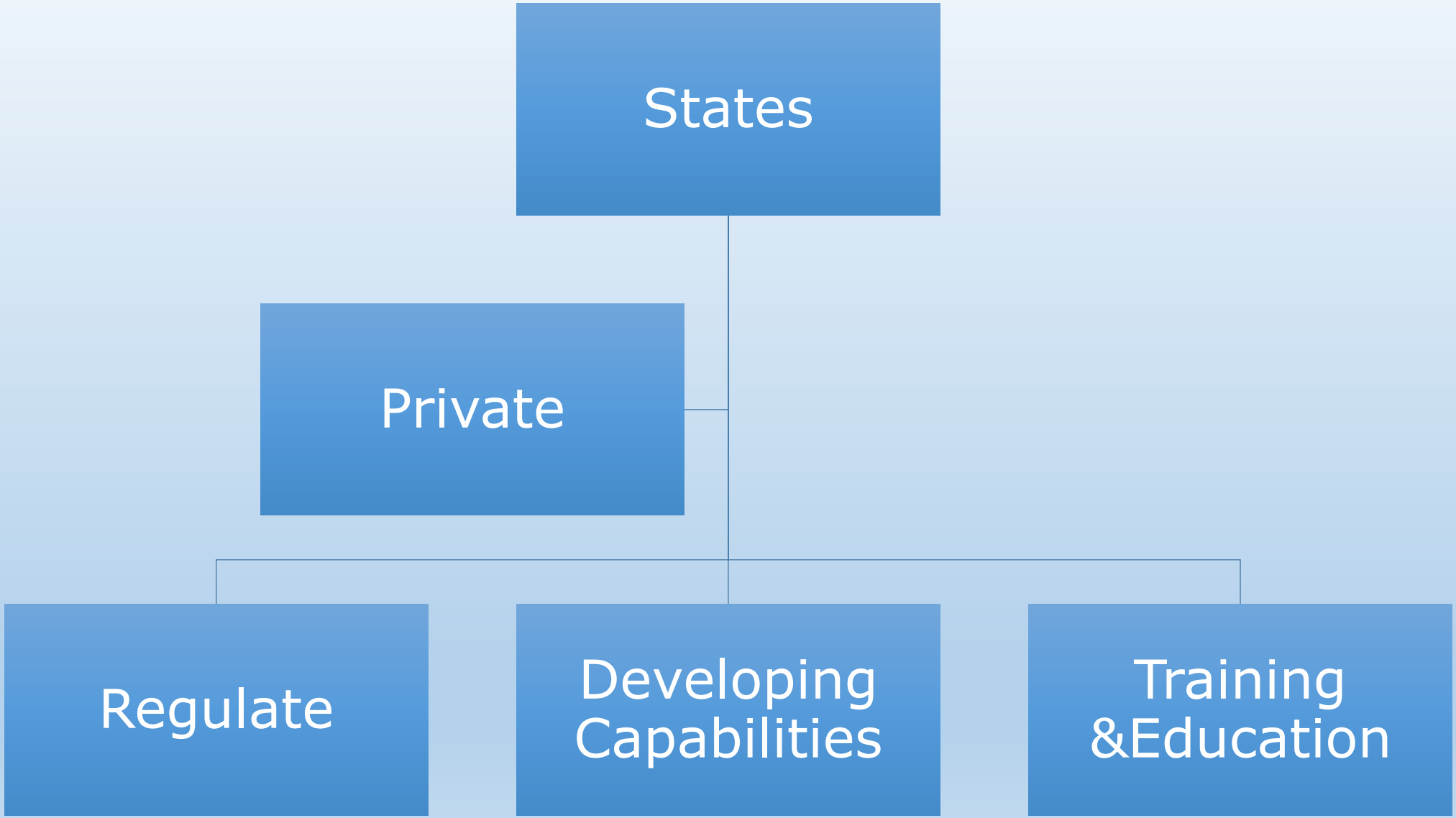
Titania (2017) "Cyber Security Predictions for 2017"
https://www.titania.com/about-us/news-media/cyber-security- predictions-for-2017

Cyber security against what

Hacktivism – 5,56%
Cyber espionage – 10 %
Cyber warfare – 6,67%
Cyber crime – 77,78



What to do?


States
Private
Regulate
Developing Capabilities
Training &Education

Regulatory framework

Global

- Norms for responsible state behaviour in cyberspace – UN Group of Governmental Experts (GGE)
- Application of international law in cyberspace – f.i. Tallinn Manual 1.0 on Cyber Warfare and 2.0 on Cyber Operations below the threshold

Regional – OSCE

- Cyber Security Confidence Building Measures

European Union

- ECSS
- NISD
- GDPR
- EEAS - Developing a Cyber Diplomacy Toolbox to respond to cyber operations

UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security

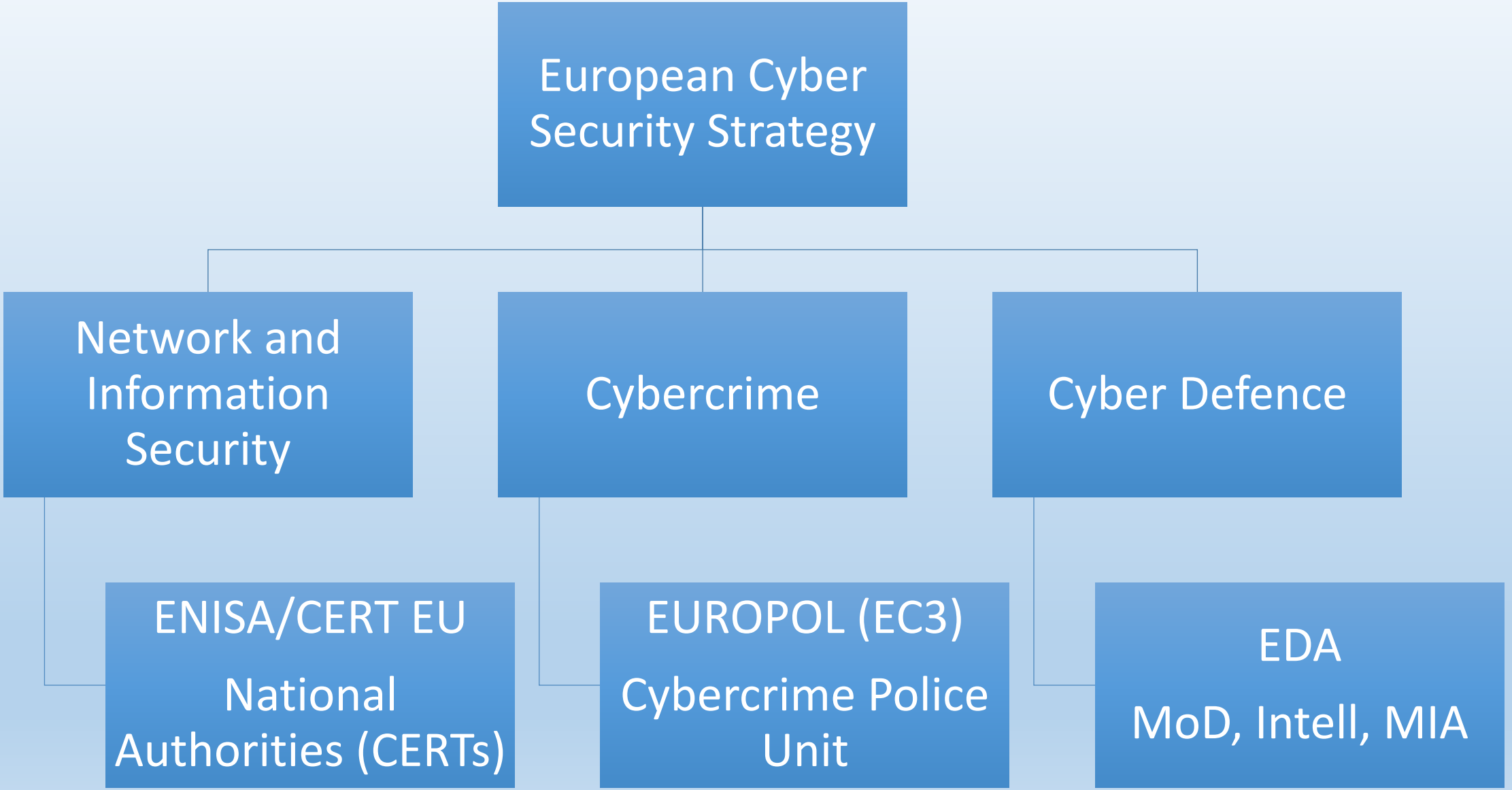
- **GGE members consensus including:**
  - Norms;
  - confidence building measures (CBMs);
  - capacity building.
- **The international law is applicable and essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.**
  - Applicability of **'state sovereignty and the international norms and principles that flow from sovereignty'** to **'state conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory'.**
  - The security of ICTs would need to go **hand-in-hand with respect for human rights and fundamental freedoms** as set forth in the Universal Declaration of Human Rights and other international instruments**.**

OSCE – **Confidence Building Measures** CBM:

- **Providing their national views;**
- **Facilitating co-operation** among the competent national bodies and **exchanging information;**
- **Holding consultations;**
- **Sharing information;**
- **Using the OSCE as a platform;**
- **Nominating contact points;**
- **Providing a list of relevant national terminology.**

Regulatory framework – European level

- The 2013 EU Cyber Security Strategy;
- The 2014 EU Cyber Defence Policy Framework;
- The 2016 Global Strategy for the European Union's Foreign and Security Policy;
- The 2016 Network and Information Security (NIS) Directive;
- 2013 – Directive on attacks against information systems;
- 2011 – Directive on combating the sexual exploitation of children online and child pornography;
- 2001 – Framework Decision on combating fraud and counterfeiting of non-cash means of payment.
- The Joint Communication on a Framework on countering hybrid threats 'a European Union response' JOIN(2016) - 18 final
- The Joint Staff Working Document on EU operational protocol for countering hybrid threats, the 'EU Playbook', SWD(2016) 227 final.


European Cyber Security Strategy
Network and Information Security
Cybercrime
Cyber Defence
ENISA/CERT EU
National Authorities (CERTs)
EUROPOL (EC3)
Cybercrime Police Unit
EDA
MoD, Intell, MIA

Network and Information Security Directive

Main objectives:

- Improving national cybersecurity capabilities;
- Building cooperation at EU level; and
- Promoting a culture of risk management and incident reporting among key economic actors

Subjects

notably operators

operators of essential services (OES)

Digital Service Providers (DSPs).

European capabilities

- The European Network and Information Security Agency (ENISA);
- The European Cyber Crime Centre (EC3) at Europol and
- CERT-EU;
- EDA

22 EU MS - of 28 NATO MS
NATO in the framework of the 2016 Joint Declaration, address these issues for Member States and the EU institutions.

European External Action Service - EEAS

"…to dissuade, to bring about change in policies or activities by the potential attacker"

- International cyber security;
- Capacity building;
- Promoting Budapest Convention on Cybercrime;
- Internet Governance: accountability and stability of Internet;
- Internet freedom and human rights;
- Relations with third countries – Dialogues with key players (U.S., China, India, Brazil, Japan, RoK);
- Relations with partners and international organisations – CoE, OSCE, UN, NATO, OECD etc.

EEAS - CAPACITY BUILDING IN THIRD COUNTRIES

Objectives

to increase third countries' technical capabilities, preparedness, and establish effective legal frameworks to address cybercrime and cybersecurity problems; and at the same time enhance their capacity for effective international cooperation in these areas.

Partners:

Council of Europe and EU Member States

Financial instruments:

1. Instrument contributing to Stability and Peace (IcSP)
2. European Neighborhood Instrument (ENI),
3. Instrument of Pre-accession (IPA)

CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

Romanian CERT

- Established by Government Decision no. 494/2011
- CERT-RO is an independent structure, with expertise in the field of cyber security, that has the capacity to prevent, analyze, identify and respond to cyber security incidents threatening RO national cyberspace.
- Coordinated by the Ministry for Information Society and is fully financed from the state budget.

CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

Types of services

Proactive	Reactive	Support
• Alerts on new threats and vulnerabilities that may affect national cyberspace. • Notices regarding the possibility of major cyber security incidents occurrence. • Technology watch. • Security assessment for partners (audits, network and application pentests etc.) on demand. • Configuration and maintenance of cyber security.	• Alerts and warnings on cyber security incidents that affect or may affect RO organizations. • Incident handling and coordination. • Management of a national database with cybersecurity incidents. • Incident analysis, investigation and malware analysis.	• Awareness activities for the government institutions and partners. • Support the partners in development of their own CERT teams. • Consulting services for securing critical infrastructures. • Involvement in development of national cyber security related regulations, policies and strategies.

CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

What does CERT-RO do? (slide 1)

- Collect alerts from different stakeholders regarding RO IPs and URLs detected as part of different cybersecurity incidents (national contact point).
- Maintain a national database regarding cybersecurity incidents.
- Operates an EWS on cyber-security incidents, based on the alerts received.
- Other services (pen tests, incident handling, tech support for MIS)

CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

What does CERT-RO do? (slide 2)

- Awareness campaigns.
- Cyber security consulting
- Can cooperate with different types of organizations in the field of cyber security and assures the exchange of info between parties;
- No jurisdiction over classified information!
- Types of services: proactive, reactive and consultancy;

CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

Who are CERT-RO partners?

- Cybersec companies
- Banks
- Gov. agencies
- Academia
- ISPs
- Other CERT teams

AVIRA
Microsoft
UniCredit Țiriac Bank
KASPERSKY lab
Bitdefender
CISCO
TEAM CYMRU
GUVERNUL ROMÂNIEI
Ministry for Information Society
FACULTY OF AUTOMATIC CONTROL AND COMPUTERS
ETTI
ROMANIA SRI SERVICIUL ROMAN DE INFORMATII Patria a priori
KrCERT/CC 인터넷침해사고대응지원센터
computer emergency response team CERT-EU for the EU institutions, bodies and agencies
enisa European Network and Information Security Agency
CNCERT/CC 国家互联网应急中心
TF-CSIRT Trusted Introducer
JPCERT CC®
Japan Computer Emergency Response Team Coordination Center
FIRST Improving Security Together

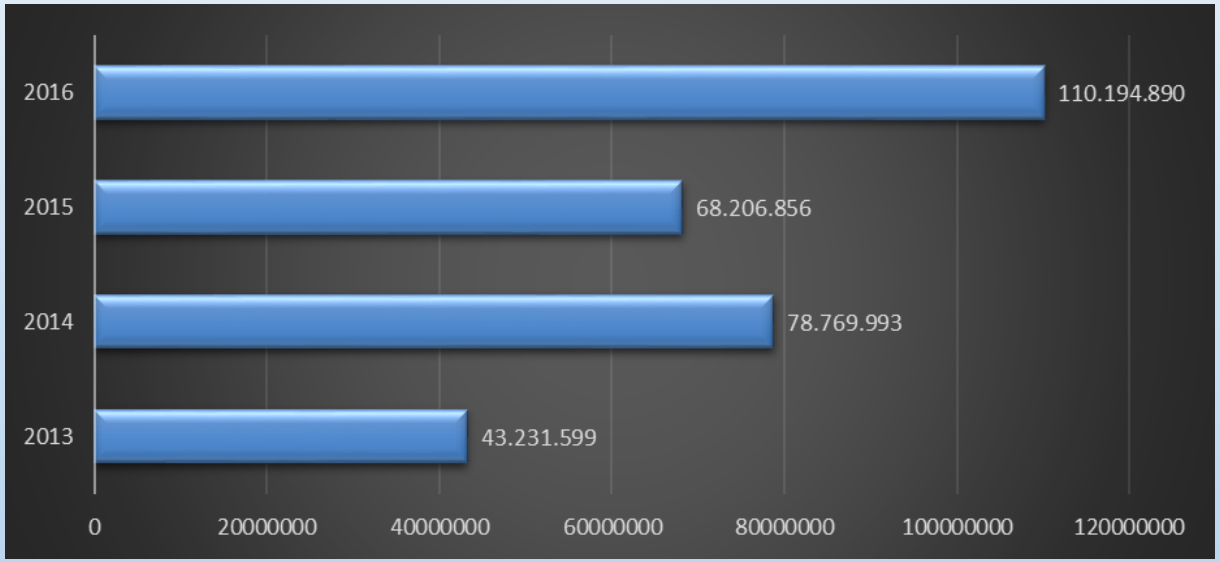
CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

Reports

- First ever official public report on state of cyber security in Romania.
- An analysis of the cyber security incidents reported to CERT-RO.
- Scope: obtaining a general overview of the nature and dynamics of these types of events/incidents, relevant for assessing cyber security risks targeted at the IT&C infrastructures in Romania.

CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

Reports: Alerts processed in past years



110 million alerts

2.9 million IPs

38% all RO IPs

58% vulnera bilities

40% botnets

10 thousand ".ro" domains

CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

Reports: Alerts processed in past years

- Numerous servers that are:
  - Vulnerable
  - Unpatched
  - Poorly configured
  - Not monitored by owner

- Millions of compromised user devices (PCs, phones, tablets, IoT) due to:
  - Unpatched/unlicensed software
  - No security/anti-malware protection
  - No cybersecurity culture

Incidents

Nr. crt.	Incident Type	Count	Percent
1	Vulnerabilities	2,380,120	58.98%
2	Botnet	1,653,096	40.96%
3	Malware	2,071	0.05%
4	Altele	158	0.01 %

- After deduplication of alerts based on IP address and type we obtained around 4 millions of incidents
- 60% Vulnerabilities
- 40% Botnet

Malware Types

Nr. crt.	Malware Family	Alerts count	Percent (%)
1	Sality	4.953.615	34,16%
2	Downadup	2.570.006	17,72%
3	Nivdort	1.979.510	13,65%
4	Ramnit	1.081.592	7,46%
5	Dorkbot	830.914	5,73%
6	Mirai	522.377	3,60%
7	Zeroaccess	312.785	2,16%
8	Virut	277.460	1,91%
9	Conficker	244.371	1,69%
10	Tinba	187.556	1,29%

CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

Examples of CERT-RO work - Awareness

- ✓ Partnership with Agerpres
- ✓ Two cybersecurity courses aiming to familiarize journalists with technology
- ✓ Opportunity to better understand the cybersecurity best practice and challenges
- ✓ Education is key

CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

Examples of CERT-RO work: awareness

- ✓200.000 AV licences (Avira) available on our website for highschool students
- ✓6 courses for magistrates (prosecutors and judges)
- ✓One international conference – with the support and participation of the US Embassy in Bucharest, FBI, Bitdefender, Kaspersky, Avira
- ✓National planers for Cyber Europe 2016 cybersecurity exercise
- ✓National organizers for European Cybersecurity Month (ECSM)

CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

CVD: The need

GD 494/2011 – art. 6 lit. b)

- Mechanism for reporting

No national legal framework for reporting

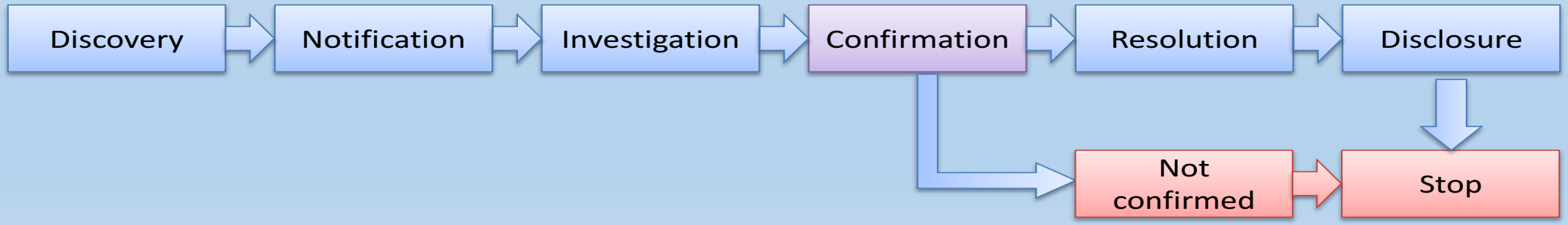
- No international recognized framework for reporting

GFCE initiative

- Romania, The Netherlands and Hungary
- Memorandum based on best practices

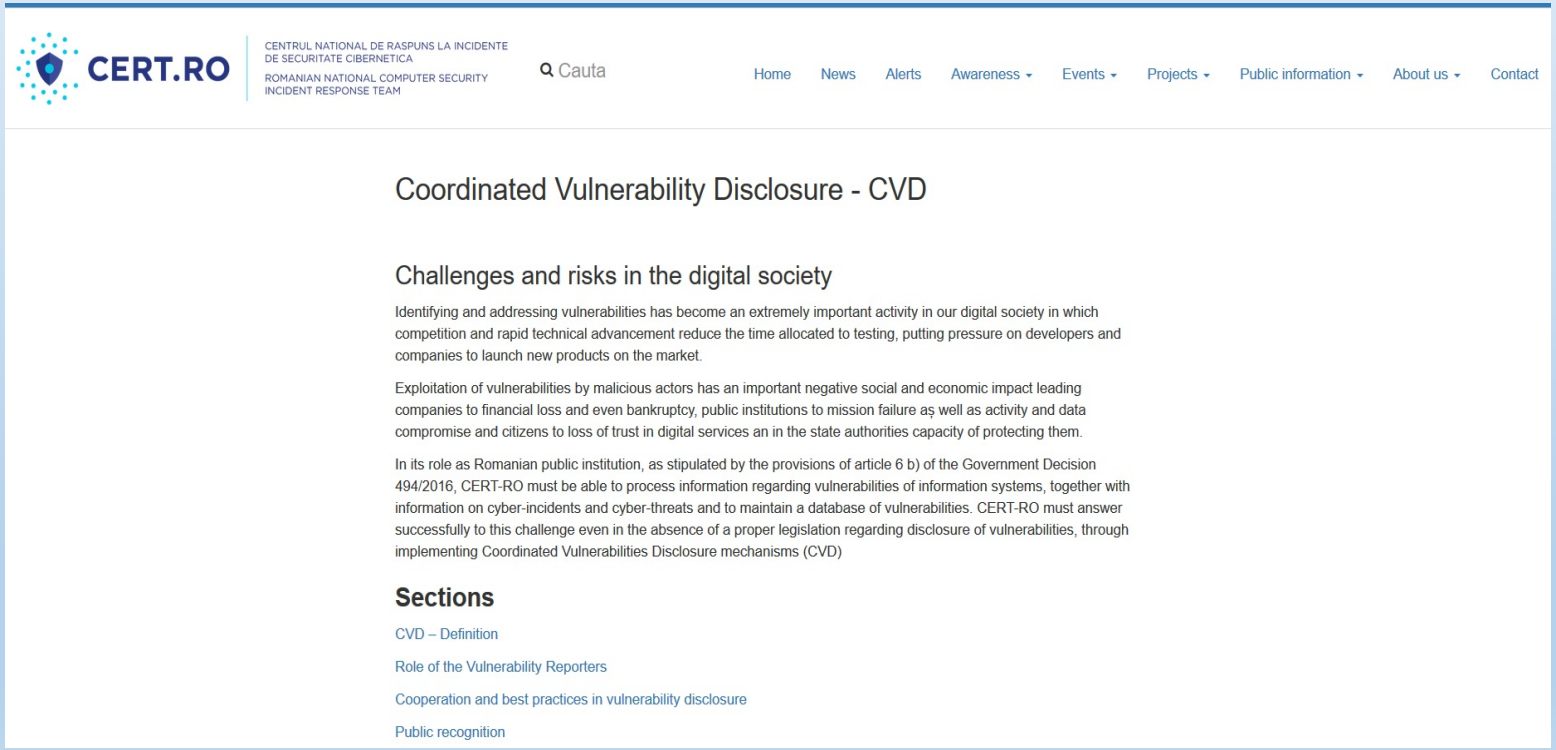
CERT-ROs role

- Based on ENISA best practices and the recommendations in the GFCE draft Memorandum on coordinated vulnerability disclosure, CERT-RO has set in place a CVD mechanism that could help bridge the gap between researchers / cybersecurity enthusiasts and companies.



CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

A description of the mechanism is available on CERT-RO website



- CVD – Definition
- Forms of cooperation and best practices
- CERT-RO role
- Report vulnerabilities through CERT-RO
- CERT-RO Reporting Guide
- Content of reporting to CERT-RO

Practical aspects of CVD

- 3 successfully coordinated cases – last 6 months
    - 2 regarding mobile banking applications
    - 1 regarding academia web based application
- Ensured trust between parties involved
- Maintaining balance between approaches (Researchers/Owners)
- Providing a safe way of reporting for Researchers
- Ensuring that identified vulnerabilities are addressed;
- Minimizing the security risk from vulnerabilities;
- Providing users with sufficient information to evaluate risks from vulnerabilities to their systems;
- Setting expectations to promote positive communication and coordination among involved parties.

Bibliography

- European Commission: http://eur-lex.europa.eu/legal content/EN/TXT/?qid=1505297631636&uri=COM:2017:476:FIN
- European Cyber Security Strategy
- National Workshop on Cyber/ICT security in the context of regional and international security, use of the Internet for Terrorist Purposes, and Cybercrime
- Tashkent 20 – 21 May 2015
- ENISA, A good practice guide of using taxonomies in incident prevention and detection (2017). Available at:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection

CERT.RO

CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

THANK YOU!

www.cert.ro