



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Cyber security challenges in the European Union

CyberAgent Workshop

Dănuț MAFTEI, PhD
danut.maftei@dnsc.ro



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ



National Cyber Security Directorate (DNSC)

- *Emergency Ordinance no. 104/2021* -

- The **national-level competent authority** for national civilian cyberspace, including the management of risks and cyber incidents
- Created under the authority of the **Government**
- Under the direct coordination of the **Romanian Prime Minister**
- Target of **1063 staff members** by 2030



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ



National Cyber Security Directorate (DNSC)

Mission

Ensuring the cyber security of the national cyberspace, in close collaboration with all competent authorities and relevant actors

Vision

The Directorate aims to become an international-class institution that firmly positions Romania as a recognized leader in cybersecurity



Directorate's key roles and responsibilities, by law (1/2)

- **Competent authority at national level for the national civilian cyberspace**, including the management of risks and cyber incidents
- **Strategy and planning** - carries out the Government's policy in the field of cyber security and establishes at the national level the public strategies and policies in the field of cyber security
- **National competent authority for regulation, supervision, and control** - ensures the regulation and management of the Romania's cyber security and national civilian cyberspace
- **National CSIRT + Governmental CSIRT + Governmental PSIRT**
- **Coordination, implementation, guidance, support of sectoral CSIRTs**
- **Alerting, prevention, awareness, and training function**
- **Cooperation and collaboration** - ensures the cooperation framework to carry out specific cyber security activities, research, information exchange, training, education, awareness, project development
- **National cyber security certification authority**



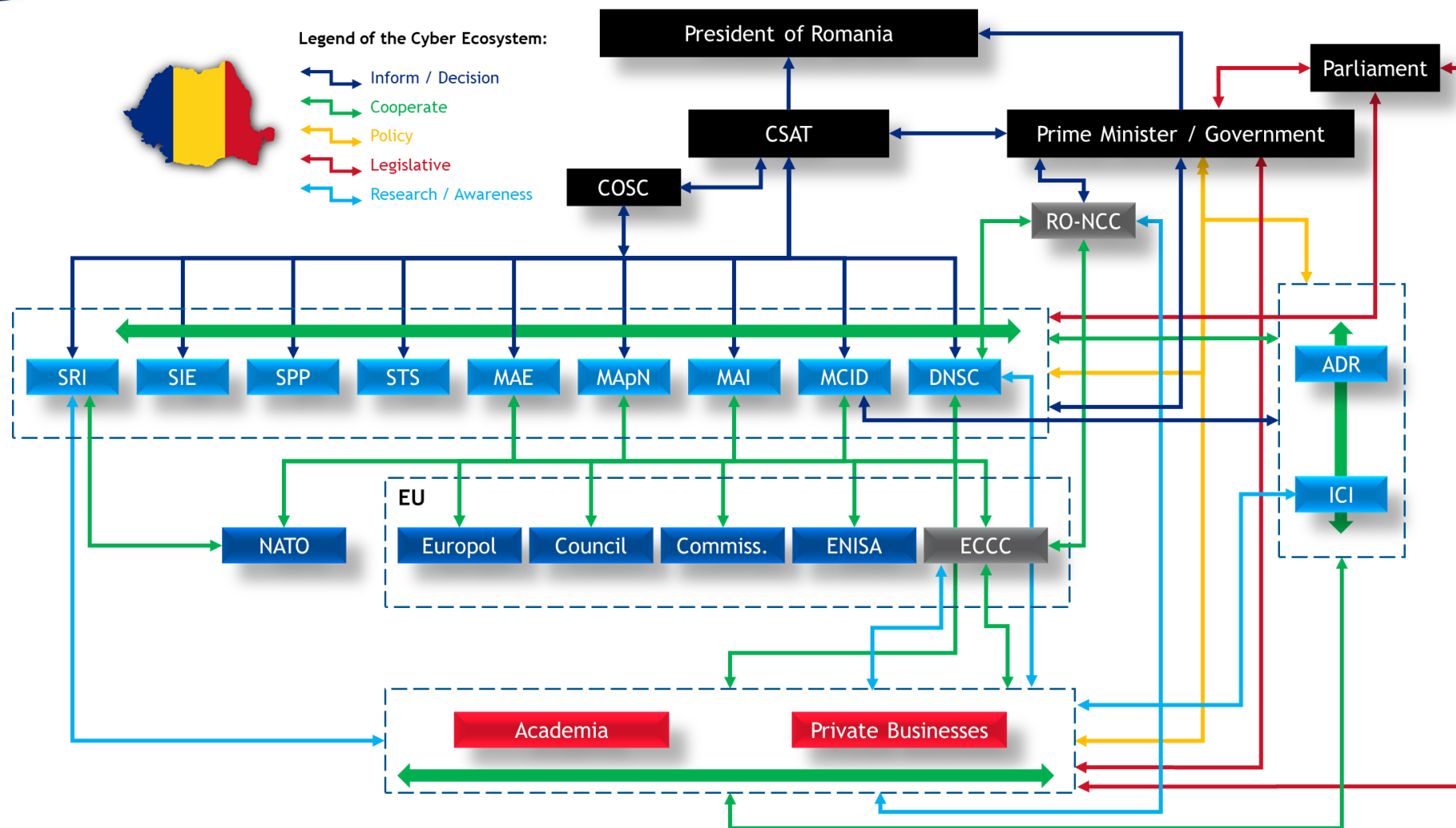
Directorate's key roles and responsibilities, by law (2/2)

- Ensuring compliance and unitary approach for cyber infrastructures
- Representation function - performs, on behalf of Romania, the representation role in national, regional, European, and international bodies and organizations, acting as a national authority for its domain
- Research and development function
- Analysis and forecasting function - evaluates & analyses cyber security developments, issues alerts, analyses, newsletters and forecast bulletins
- Identification, evaluation, monitoring and mitigation of cyber risks at national level
- National centre for managing cyber crises in peacetime
- Performing cyber security assessment of new technologies
- Evaluation and certification function
- The function of education and training in the field of cyber security
- Management of projects and services



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Romanian cyber security ecosystem





DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Cyber security challenges in the EU

Fundamental challenges:

- **Cyber attacks against citizens, state institutions, critical information infrastructure, ESO etc.**
- **Securing network and information systems in the EU**
- **Cyber policies and legal framework**
- **National cyber security strategies**
- **Education**
- **Experts vs. not enough skilled personnel**
- **Digital skills; Cyber training**
- **Cyber awareness**
- **The ``Weakest Link`` / Human Error**
- **Retention of human resources**
- **Capacity building (DNSC Romania – as an example)**
- **Women in cyber**
- **Pragmatic public-private partnerships**



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

EU legal framework on cyber issues

- **Cooperation**
 - National cooperation
 - Regional cooperation
 - International cooperation
- **Cooperation - CSIRTs, LEAs, Judiciary, DPAs**
- **Sharing Information**
- **Trust**
- **Incident reporting – lot of the cases under reported**
- **Detection platforms (sensors - commercial vs open sources)**
- **Single source dependencies**
- **Cyber security certification**
- **Privacy; Protection of personal data**
- **Cyber espionage**
- **Disinformation, fake news etc.**
- **Hybrid activities (GERASIMOV "DOCTRINE")**



Cybersecurity is a journey, not a destination!

QUESTIONS?

Dănuț MAFTEI, PhD
danut.maftei@dnsc.ro



Note

TLP:GREEN = Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.

Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels.

TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity / defense community.

Source: <https://www.first.org/tlp/>