



**Romanian
Cybercrime
Unit**

**EU Policy
Cycle**

**Capacity
building**

Threats

Thank you



Cybercrime in Romania

Romanian Cybercrime Unit

- As part of Romanian National Police in 2003 was established a Romanian Cybercrime Unit
- As cybercrime is consider a serious crime, Cybercrime Unit is organized under the Directorate of Combating Organized Crime

***Central
level***

***National
level***

Central level

- Provides cyber expertise for the territorial units
- Strategic planning and capacity building both national and international
- Central Cybercrime Unit is organized on four different bureaus

***NCMP and
eFrauds***

***Cyber
Attacks***

CSE

***Digital
Forensic***

Non Cash Means of Payment and Internet Frauds



Cyber Attacks



Child sexual exploitation



Digital forensic



National level

15 x Services for Countering Computer Crimes
(6-7 officers / local cybercrime unit)

27 x Services for Countering Organized Criminality
(1-2 officers / local services cybercrime)



**Romanian
Cybercrime
Unit**

**EU Policy
Cycle**

**Capacity
building**

Threats

Thank you



Cybercrime in Romania



Capacity building

Central Cybercrime Unit very active in the area of capacity building both at national and international level

CyberEx

***Cyber
South***



***Romanian Center of
Excellence in the area of
Cybercrime
CyberEx***

Cybercrime training is essential

Not just for police but also for prosecutors and judges

Started with a train the trainer programme

Cyber South

CyberSouth is a joint project of the European Union (European Neighbourhood Instrument) and the Council of Europe.

CyberSouth aims to strengthen legislation and institutional capacities on cybercrime and electronic evidence in the region of the Southern Neighbourhood in line with human rights and rule of law requirements.

Initial priority areas: Algeria, Jordan, Lebanon, Morocco and Tunisia

Romanian Cybercrime Unit supported the project with assessment and study visits



**Romanian
Cybercrime
Unit**

**EU Policy
Cycle**

**Capacity
building**

Threats

Thank you



Cybercrime in Romania

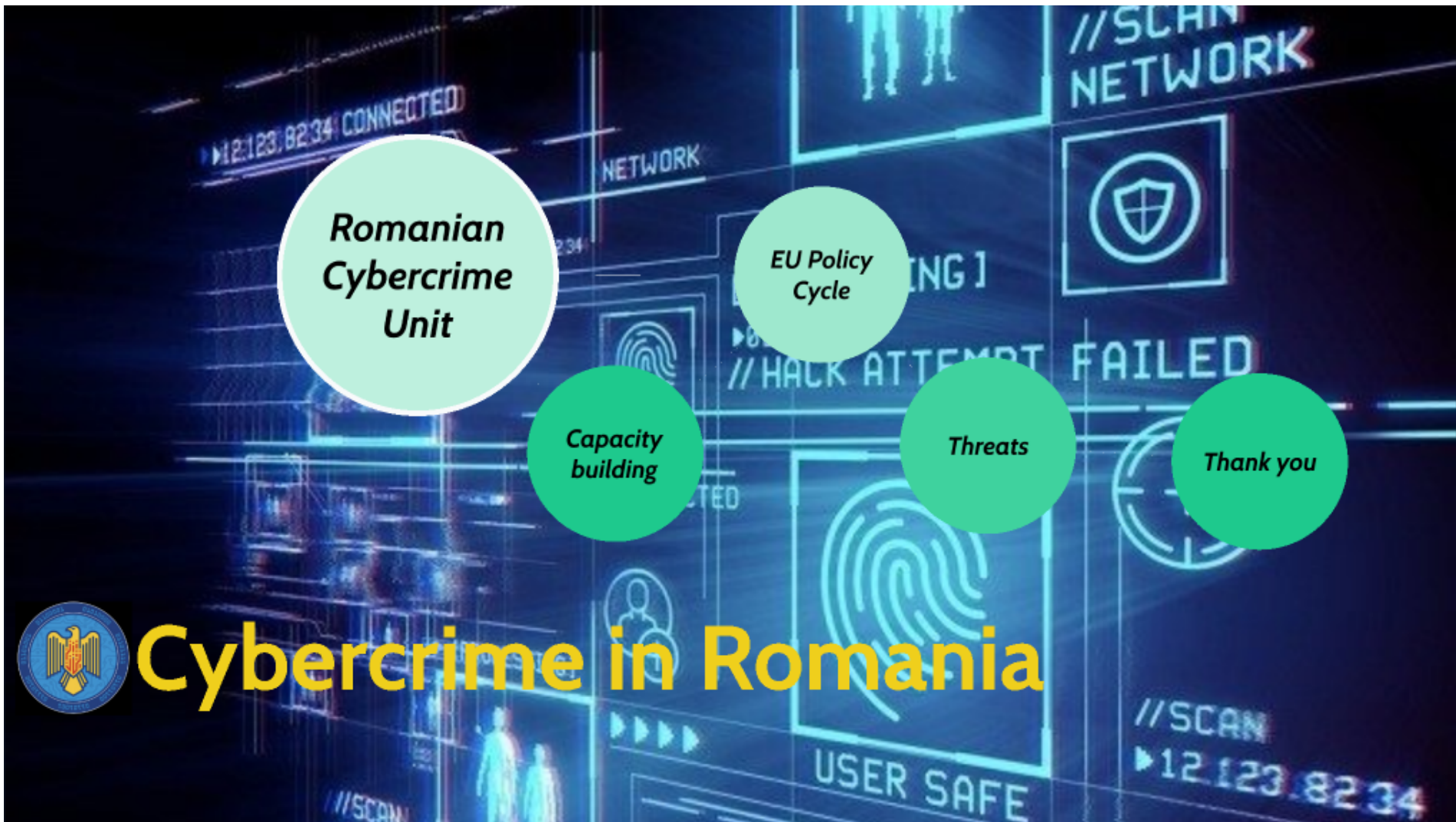


**Leading positions within EMPACT
Cybercrime framework**

- **Driver** Non Cash Means of Payment Frauds
- **CoDriver** Attacks against Information Systems
- **Participant** Child Sexual Exploitation

In 2010, the EU set up a four-year policy cycle in order to create a greater measure of continuity for the fight against serious international and organised crime.

Calls for robust and coordinated action to target the most pressing criminal threats facing the EU



Threats

National and International threats identified based on EMPACT, IOCTA and CERT-RO yearly reports



Ransomware

*Cyber attacks
against banking
infrastructure*

Live streaming CSE

Ransomware

One of the biggest threat identified at national and EU level



The background features a dark blue grid pattern. The words "ATTEMPT FAILED" are written in a light blue, sans-serif font across the top. Below the text, there is a circular target symbol with a crosshair in the center. A large, semi-transparent green circle is overlaid on the grid, containing the main text.

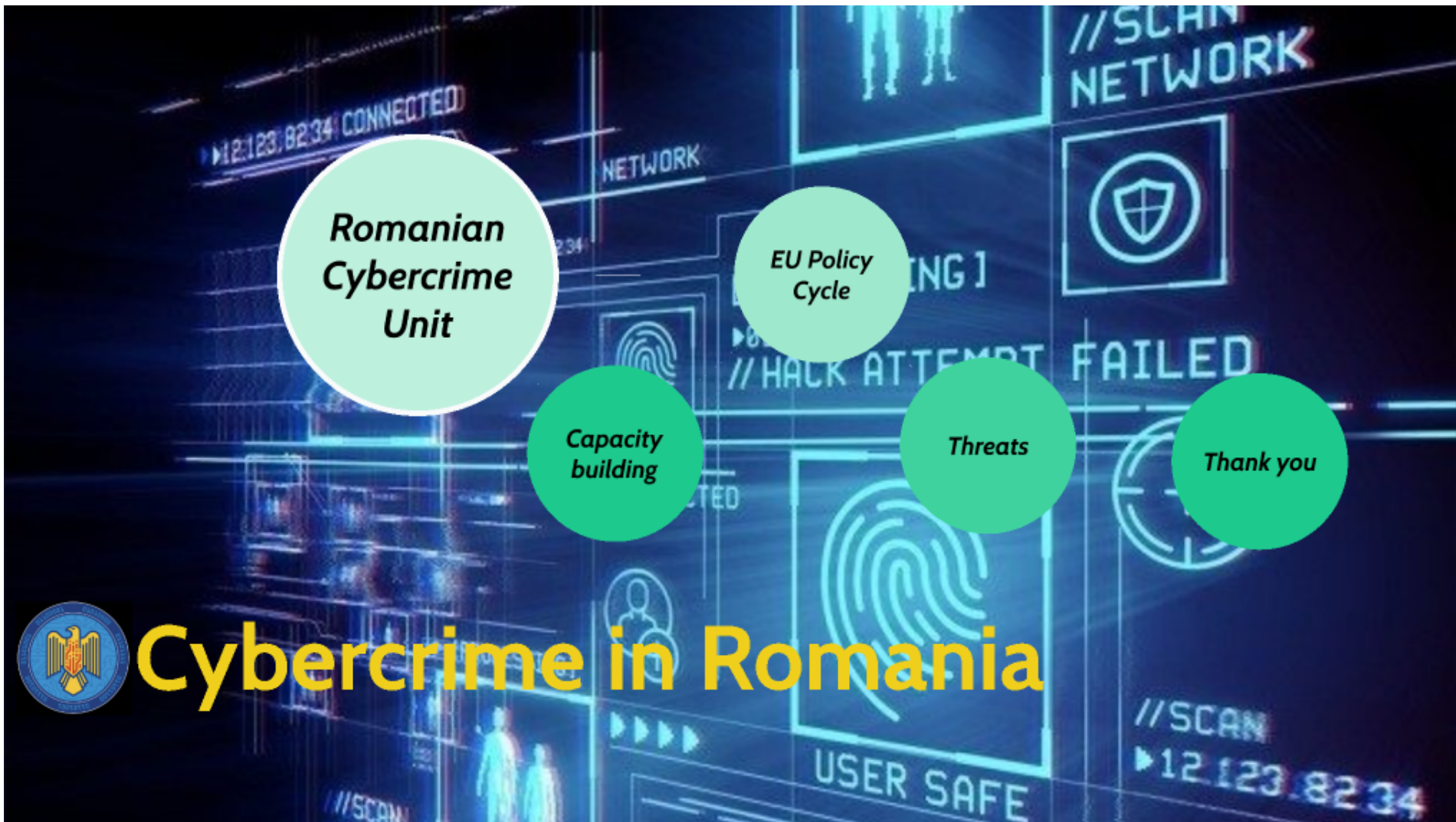
Cyber attacks against banking infrastructure

Complex and highly sophisticated attacks
with losses of millions



Live streaming shows

A worrying trend of the live sexual shows
with minors



**Romanian
Cybercrime
Unit**

**EU Policy
Cycle**

**Capacity
building**

Threats

Thank you



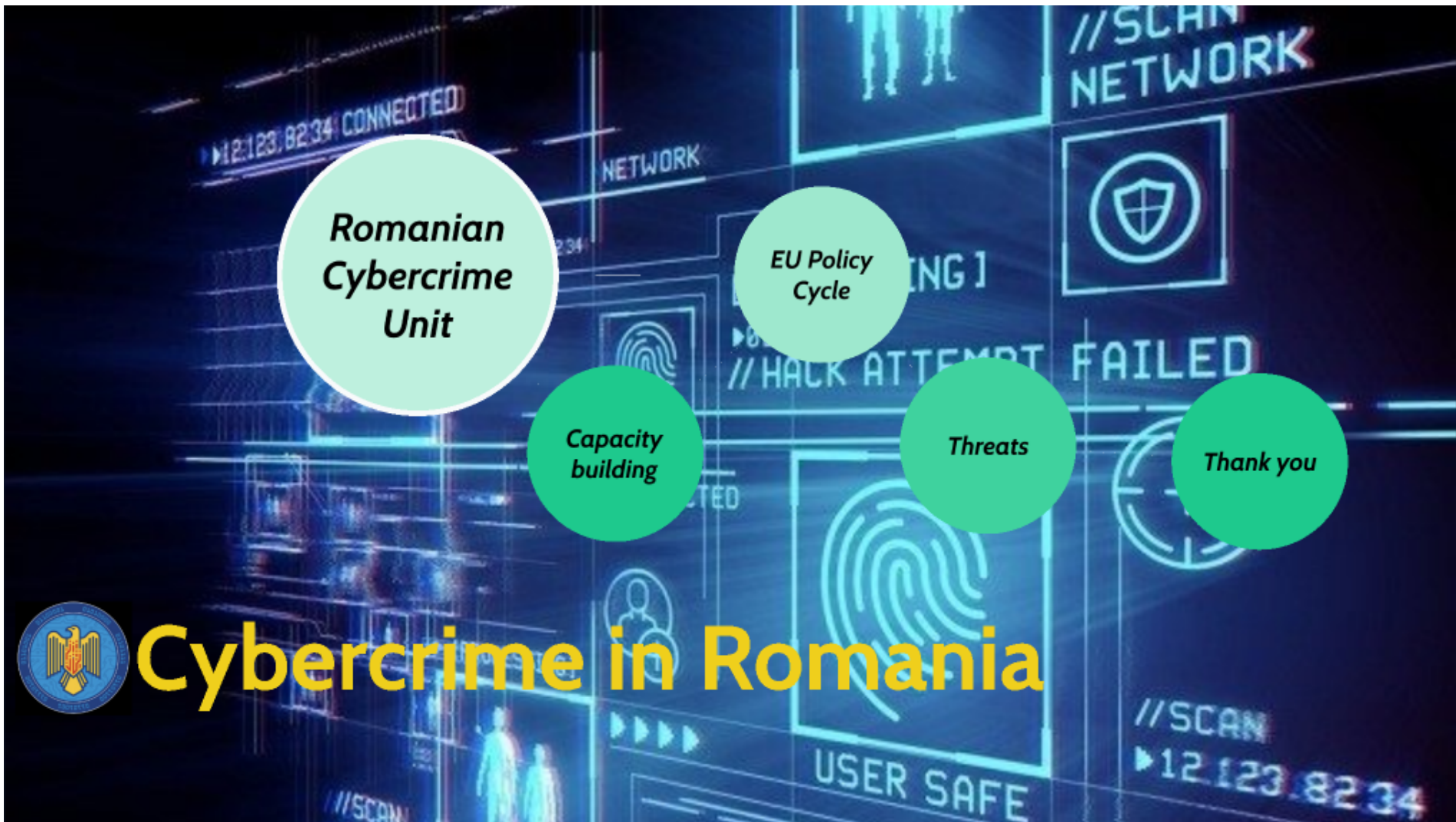
Cybercrime in Romania



Questions?

Thank you

Catalin ZETU
Central Cybercrime Unit
Head of Cyber Attacks
catalin.zetu@politiaromana.ro



**Romanian
Cybercrime
Unit**

**EU Policy
Cycle**

**Capacity
building**

Threats

Thank you



Cybercrime in Romania