RUNNING A SPECIALISED CYBERCRIME UNIT IN ROMANIA

Marius-Daniel CUCIURIANU

Head of Cybercrime Department

ROMANIAN NATIONAL POLICE

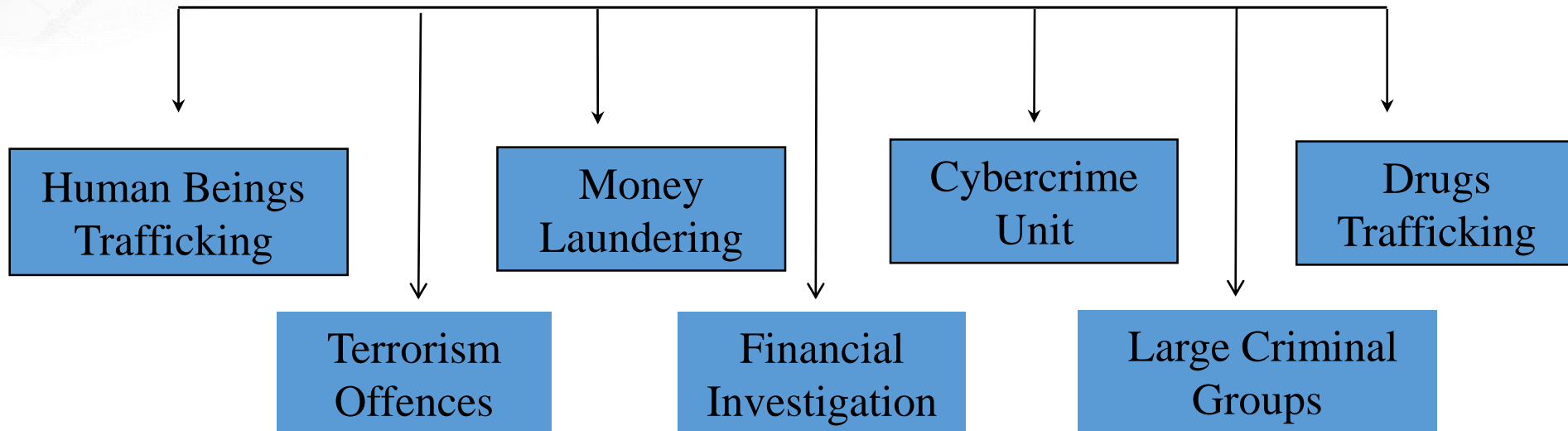*Bucharest Organized Crime Unit*

marius.cuciurianu@politiaromana.ro

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

ROMANIAN NATIONAL POLICE
Bucharest Cybercrime Unit

ROMANIAN NATIONAL POLICE

Organised Crime Unit

- Human Beings Trafficking
- Terrorism Offences
- Money Laundering
- Financial Investigation
- Cybercrime Unit
- Large Criminal Groups
- Drugs Trafficking

C-PROC – Glacy + Project - Council of Europe webinar on the Establishment and functioning of specialised cybercrime units, on 29 April 2020
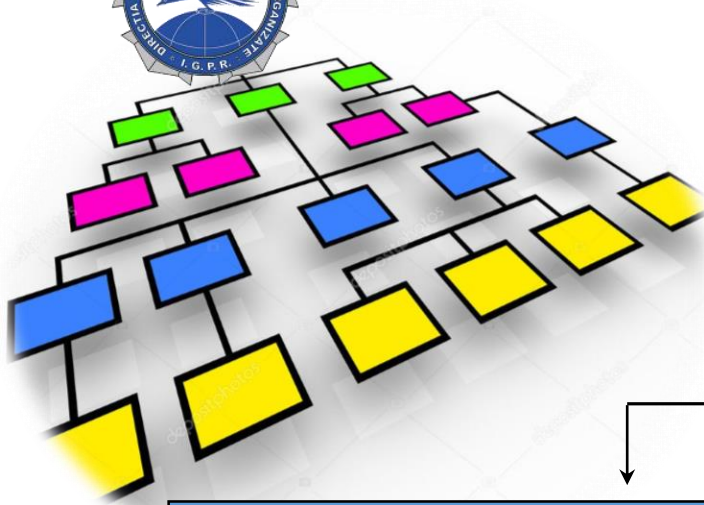
ROMANIAN NATIONAL POLICE
Bucharest Cybercrime Unit

Central Cybercrime Unit (38 staff)

| **On-line / Payment Fraud** (10 staff) | **Digital Forensics** (10 staff) | **On-line Child Abuse** (10 staff) | **Cyber attacks** (8 staff) |

Local capacities (170 staff)

| **15 Local Cybercrime Units** (8-10 staff) | **27 Local Organised Crime Units** (2-3 staff) |

1. On-line Frauds and frauds committed with electronic payment instruments:

- **-** Electronic commerce related - Internet frauds,
- - Credit card related – skimming, phishing, card not present fraud

2. Digital Forensics: **-** Forensic examination / digital data extraction
- - Live access to a computer sistem
- **-** Data preservation requests and processing internet traffic

3. On–line Child Abuse : **- Child Pornography by use of computer**
- - Producing of CSEM
- - Offering, making available, promoting of CSEM
- - Distributing or transmitting of CSEM
- - Procuring for oneself or another of CSEM
- - Possessing, without right, oc CSEM with in a computer system or data storage device

4. Computer – related crimes: - Crimes against / through computer systems; unauthorized computer / data access or transfer
- - Illegal interception of data transmitted by a computer or data which is not publicly available
- - Illegal alteration, deletion or deterioration of a electronic data or restriction of access at that data
- - Serious hindering of a computer operation system by introducing, transmitting, altering, deleting or restricting the access to the electronic data
-

STRATEGY: make history
- Fighting cybercrime / **war** on cybercrime
- take the **lead** and win
- build to **last** / why / how / what

PILLARS:
- **Information** / intelligence / relevant / follow up / reputation
- **Innovation** (there is only one challenge – technology / perspective)
- **Partnerships** / old / new / priorities / find common grounds / involve / build trust

HEART and ENGINE:
- **People** / direct contact / proactive
- **Analysis** capacities / processing pipelines / machine learning / efficient, automatic forensic / SOPs

2020 CHALLENGES:

- **Phishing** campaigns and mobile malware distribution using links or files with information / advice on COVID 19

- **Ramsomware** on health care facilities / hospitals / private health centres

- **Attacks** against critical infrastructure holding personal data of COVID 19 patients

- On-line **frauds** on health / sanitize / personal protection products for financial profit

- Ongoing JIT with Latvia and Estonia (with Eurojust and Europol support) on phishing activities

- SIM SWAP scam has become an everyday criminal act

HORIZONTAL SUPPORT

- Human trafficking / sexual exploitation of children
  (using public platfoms to advertise the services)

- First responders (live mobile digital forensics) to
  public health crimes *(susupects returned from COVID hot zones)*

- Open source intelligence, social media monitoring *(of people disrespecting quarantine / isolation)*

- Cyber patrolling / darknet / deep web markets / communities *(involved in illegal transations of medicine and drugs)*

- Digital forensics analysis *(in urgent criminal cases regarding public health crimes)*
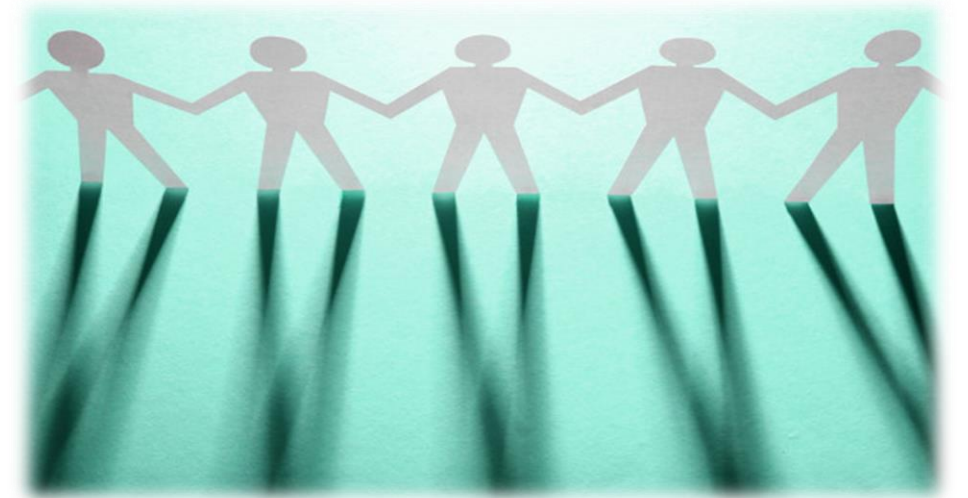
HORIZONTAL SUPPORT

- Profiling capacity *(on severe crimes / terrorism investigations)*

- Victims identification / localization *(minors, people with limited capacity, responsibility)*

- Identification of High Value Targets / cyber *intelligence (leaders or key members of OCGs)*

- Data preservation / international cooperation assistance *(in cross border investigations)*

- Liaison with private sector (payment service providers, ISPs, financial institutions, delivery services)

- Support operations / mobile teams / digital (forensics) training
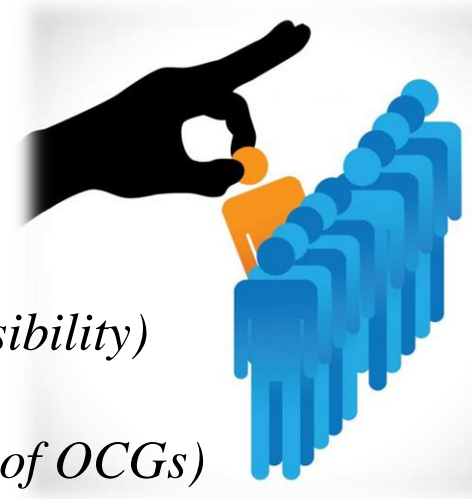
Thank you for your attention!

Marius-Daniel CUCIURIANU
Head of Cybercrime Department
ROMANIAN NATIONAL POLICE
Bucharest Organized Crime Unit
marius.cuciurianu@politiaromana.ro

Mobile: 0040 722686064