

## **Regional workshop**

# **Law Enforcement training strategy on cybercrime and electronic evidence**

**24-25 September, Jordan**

**Cybercrime and electronic evidence training**

**Virgil SPIRIDON**  
**Head of Operations**  
**C-PROC, Council of Europe**

**[www.coe.int/cybercrime](http://www.coe.int/cybercrime)**

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE



# Cybercrime Programme Office (C-PROC)

## Addressed to

- Staff of specialised units dealing with cybercrime /electronic evidence
- Students from Police Academy/School
- Other Police Departments

## Content

- Legislation
- Investigative techniques/tools
- International cooperation
- Electronic evidence

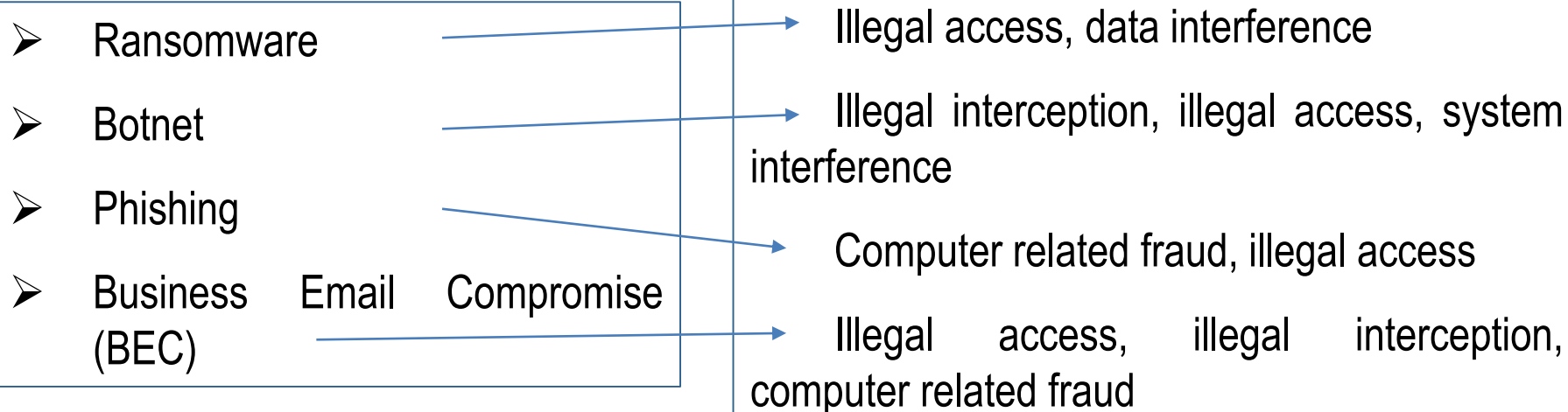
## Resources

- National and international legislation
- **Local**: internal regulations, procedures, training course, best practices
- **International**: guidance, standards, training materials, etc
- Academia
- Private sectors

**Adapted to** the national needs and international standards

# Cybercrime Programme Office (C-PROC)

## Modi operandi vs offences



## To consider

- Cybercrime threats and crime techniques
- Legislation to apply
- Complexity of the case and multidisciplinary approach of the investigation
- Transborder elements



# Cybercrime Programme Office (C-PROC)

## Investigative techniques vs IT developments

- Production order
- Preservation
- Interception (Internet and phone)
- Undercover

- Software applications to support investigations
- OSINT

## To consider

- How to check IPs, Web sites, Domains, etc
- How to read log data, traffic data, etc
- Undercover profile, how to act, etc



[Virgil.spiridon@coe.int](mailto:Virgil.spiridon@coe.int)

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)