European legal frameworks for online investigations into dark web criminality

30 September 2019, The Hague

Background

- **Joint Europol-Eurojust questionnaire on *'investigations of Darknet criminality'***
  - *Overview of approaches and investigative possibilities, challenges and best practices in relation to Dark Web investigations*
- **For more detailed information**
  - 3rd issue of the Cybercrime Judicial Monitor

National legal frameworks

- Most countries have **no specific legislation** concerning online investigations
  - ➡ apply general provisions on wiretapping, undercover operations, infiltration, etc.

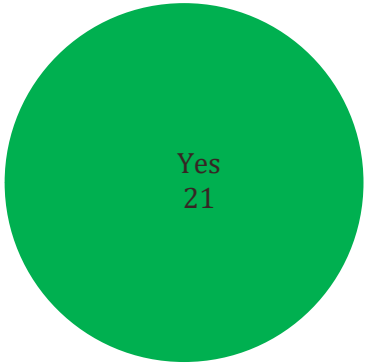
- Passive vs. active presence of LEA online
  - interaction with subjects online
  - differences in possibilities and limitations

Online investigations

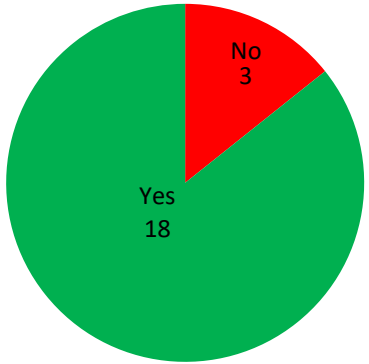
Passive presence online - requirements

- General competence of LEA
- Publicly accessible places
- Observation/surveillance
- *Limitations:* open investigation, special investigative measures requiring further conditions/restrictions

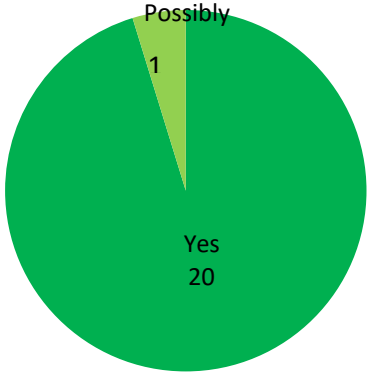
Monitoring of user activity



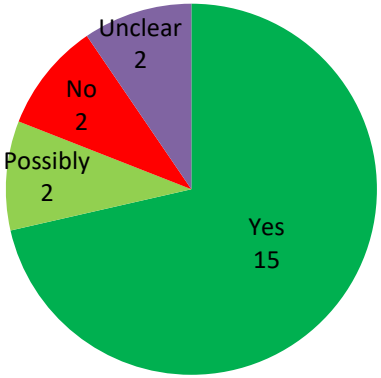
Lurking



Logging of user activity



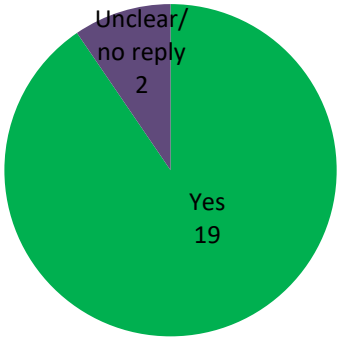
Scraping



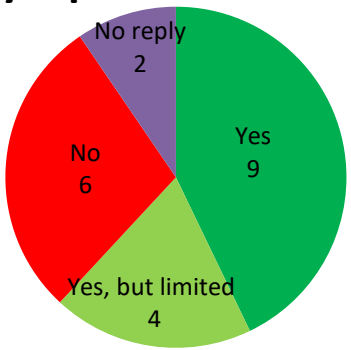
Active presence online

- Undercover investigation/infiltration/surveillance
- **Requirements and limitations:**
  - Offence: listed, serious, sentencing level
  - Initial suspicion/sufficient evidence of crime
  - Suspects identified
  - Open investigation
  - Cannot be achieved through other measures
  - Authorization court/judge/prosecutor
  - Limited in time
  - No provocation
  - LEA not committing crime

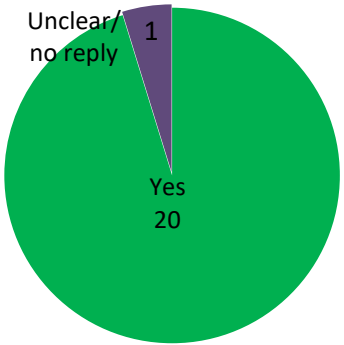
Engaging in conversations



Participation in criminal activity by a police officer



Pseudo buys/deliveries/servicing



Involvement in running a Darknet environment (as an administrator or moderator)

Taking over Darknet and vendor accounts

- Undercover operation, infiltration, covert surveillance, interception, seizure of data
- **Requirements**
  - Court order/authorisation judge or prosecutor
  - LEA not to commit crime
  - No provocation
- **Continuation of crime**
  - Interfere as soon as possible/proportionality
  - Assess on case-by-case basis
  - Not when threat to life, health of person or serious harm
  - Prior authorisation to commit offences

Online presence - challenges

- **Legal challenges:**
  - Application of general legal provisions/lack of specific legislation
  - Jurisdiction
  - (Suspicion of) crime committed/identity persons known
  - LEA not allowed to commit crime/no provocation
  - Coordination between MS to avoid overlapping/hindering other investigations
  - Consider how long crime can continue

- **Practical challenges:**
  - Setting up/take over account which does not raise suspicion
  - Encryption and anonymization hinder access to darknet and identification of users
  - Locating users/tracing virtual currencies
  - Technicalities of operations
  - Lack of resources/capacity/training
  - Protecting agent's identity
  - Efficient evidence collection
  - Measure limited in time

Joint Investigation Teams

- **JIT is a useful tool to investigate Darknet** because of cross-border nature of the crime and need to coordinate investigations across countries with different legal jurisdictions

JIT - Challenges

- **Legal challenges:**
  - Integrate different jurisdictions in JIT; different rules on confidentiality
- **Practical challenges:**
  - Decision making in case of many JIT participants
  - Information sharing between JIT participants
  - Investigations in countries at different stages
  - Preparation of the JIT agreement

Thank you for your attention

Mieke De Vlaminck

Judicial Cooperation Advisor

www.eurojust.europa.eu

Follow Eurojust on Twitter and LinkedIn @ *Eurojust*