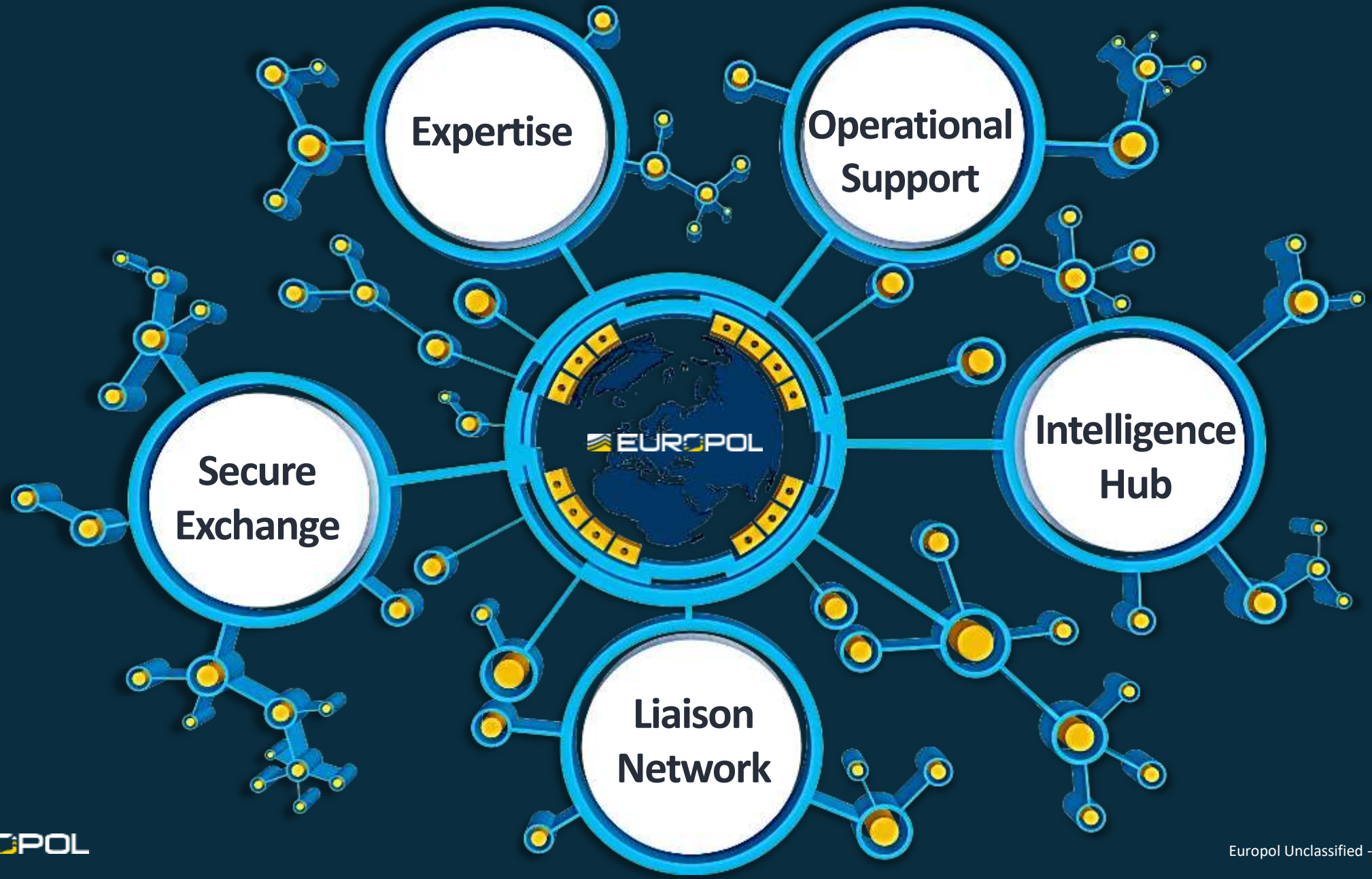
Virtual Currencies and Ransomware: Combating Criminal Use – The Law Enforcement Response

Dr Philipp Amann, MSc
Head of Strategy
European Cybercrime Centre
Europol

“Law Enforcement as a Service”



Networks of networks…

Communication Providers

Financial Services

Internet Security

Europol Unclassified - Basic Protection Level

J-CAT – operational coordination at EU level and beyond

Chair-Country: Poland

Vice-Chair-Country: Switzerland

21 Law Enforcement Agencies from
18 Countries (11 EU Member States, 7 Third Parties)

+

Europol's European Cybercrime Centre (EC3)

Europol Unclassified - Basic Protection Level

Key threats and trends

- Crime-as-a-service remains prominent
- Ransomware groups adapting their ‘business model’
- Increase in mobile malware, online scams and CEO fraud
- Increase in abuse of decentralized finance models (NFT thefts, attacks against smart contracts, etc.)

Successful operational response

Operation Emlog

- Dismantled InfinityBlack, a hacking group for distributing stolen user credentials, creating and distributing malware and hacking tools
- Two platforms with databases containing over 170 million entries closed down

Operation Invoke

- Two suspects arrested for running the CyberSeal and Cyberscan crypting services to evade antivirus software detection
- Services purchased by more than 1500 criminals
- Services used for crypting different types of malware

Operation Nova

- Takedown of VPN service
- used by cybercriminals globally
- Seizure of infrastructure in DE, NL, CH, FR, US
- 250 companies worldwide spied on by the criminals using this VPN

Operation Ladybird

- Disruption and takedown of EMOTET
- LEAs gained control of the infrastructure and took it down from the inside and the infected machines of victims were redirected
- Administrator detained in UA

Operation Secreto

- Dismantled an OCG involved in fraud and money laundering
- More than 40 house searches
- 105 arrests & 88 house searches
- Over €12 million in damages

Successful operational response – continued

Operation Talpa

- Arrests of two ransomware operators with victims in Europe and North America
- Seizure of assets

Operation Trojan Shield

- FBI-led + 16 countries
- 800 arrests
- Seizure of USD 48 Million, 30 tons of drugs, ..
- Intelligence from 27 million messages during 18 months

Operation 26Palm Beach

- Takedown of DoubleVPN service used by ransomware operators & phishing fraudsters
- Servers seized worldwide

Ongoing Operations Ransomware Actors

- Operation in 8 countries
- 50 investigators deployed to Ukraine
- 12 arrests with 1800 victims in 71 countries
- Seizure of assets

Operation Dark hunTor

- Arrest of 150 Darkweb suspects (sellers/buyers) in Europe, Australia, North America.
- Seizure of USD 26 million, 234 kg drugs, 45 firearms …

Effective public-private partnership at work

170
Partners

120
Decryption Tools

6
Million victims helped

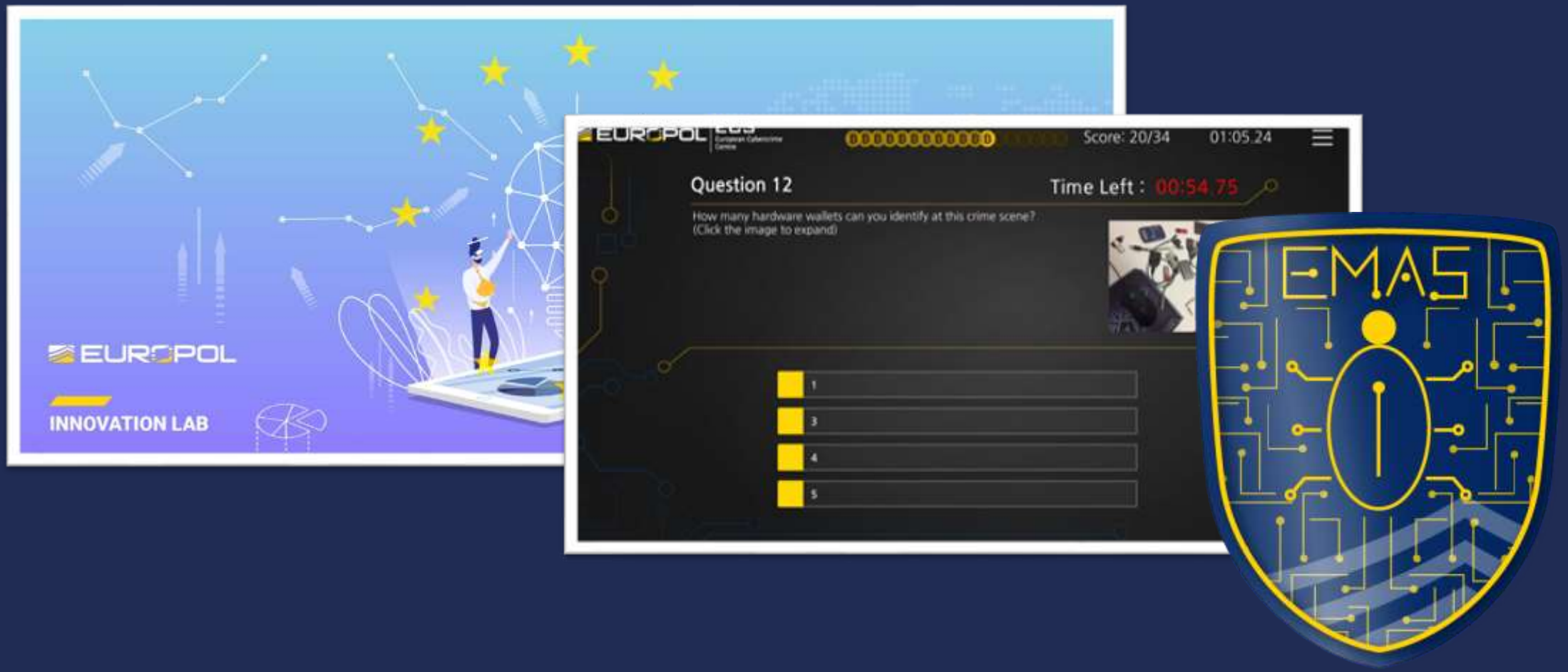
37
Languages

Most visited languages

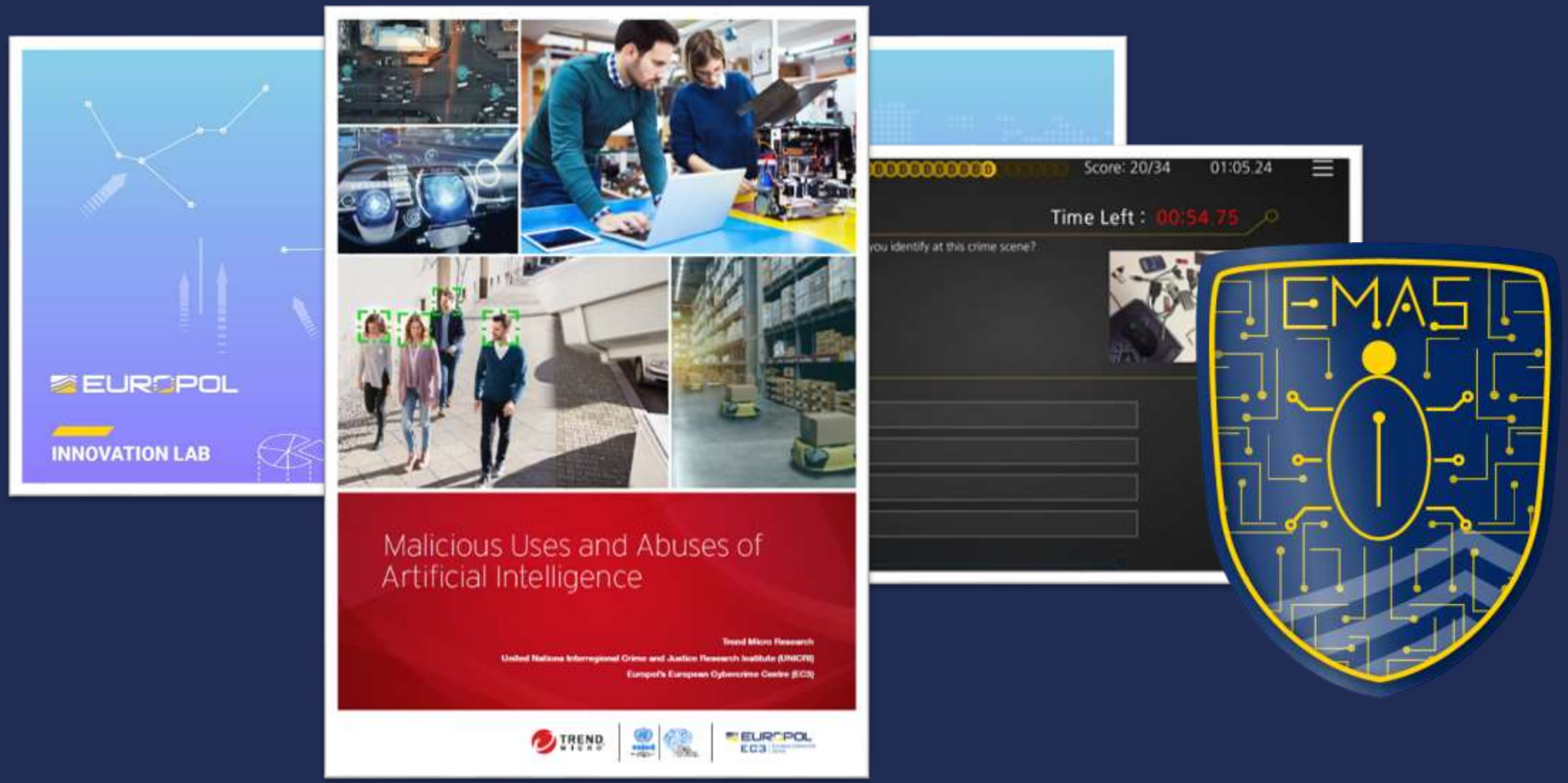
▶ **https://nomoreransom.org/**

EUROPOL

Innovate or perish…



Innovate or perish…



Innovate or perish…

Other Key Activities

- Structured collaboration (EPE, LE, industry)
- Bitcoin and Ethereum Guides for Investigators
- International Ransomware Response Model (IRRM)
- Anti-money Laundring and Countering of Terrorism Package

Cooperation is key