EUROPOL
EC3 | European Cybercrime Centre

@EC3Europol

ENISA CTI-EU

Cyber Intel within European Cybercrime Center Ops

Álvaro Azofra
EC3 Operations
Rome, 30 Oct 2017.

SUMMARY

1. Europol
2. European Cybercrime Center (EC3)
3. EC3 Operations
4. EC3 strategic products

Europol Headquarters

EUROPOL EC3 European Cybercrime Centre

The Hague, Netherlands

Europol creation and objective

EUROPOL EC3 European Cybercrime Centre

- European Police Office (Europol)
- Established in 1999
- The EU's law enforcement agency
- Make Europe safer by assisting EU law enforcement authorities

Europol staff

EUROPOL EC3 European Cybercrime Centre

OPERATIONAL STAFF

- Different kinds of law enforcement agencies (LEAs)
- NO direct power of arrest
- Analytical capabilities + Expertise + Resources = tackle criminal networks

EU Liaison Bureau Network

EUROPOL EC3 European Cybercrime Centre

Europol Liaison Officers in:

- Interpol IGCI
- Interpol IPSG
- Washington DC

Cooperation Agreements Third Parties

EUROPOL EC3 European Cybercrime Centre

28 EU Member States

Operational Agreements: Albania, Australia, Bosnia and Herzegovina, Canada, Colombia, Denmark, Eurojust, former Yugoslav Republic of Macedonia, Frontex, Georgia, Iceland, Interpol, Liechtenstein, Moldova, Monaco, Montenegro, Norway, Serbia, Switzerland, Ukraine, United States

Strategic Agreements: CEPOL, ECB, ECDC, EMCDDA, ENISA, FRONTEX, OHIM, OLAF, Russia, UNODC, World Custom Organisation

Europol Legal Framework

- **MANDATE:** Europol Council Decision (upd. Jun´16)
- Support and strengthen member states
- Prevention and combat:
  - Organised crime
  - Terrorism
  - Other serious crime
  - Affecting 2+ member states

Europol activity

EUROPOL EC3 European Cybercrime Centre

- 46 000 cases initiated in 2016 (+16%)
- 870 000 operational messages
- 7 000+ users from the 28 Member States

European Cybercrime Centre (EC3)

- **Established in January 2013**
- **Strengthen the law enforcement response to cybercrime.**

EC3 Structure

EUROPOL EC3 European Cybercrime Centre

Head of EC3

Strategy

- OUTREACH & SUPPORT
  - STRATEGY & DEVELOPMENT
- OUTREACH & COOPERATION
- PUBLIC AWARENESS & PREVENTION
- STRATEGIC ANALYSIS
- TRAINING & CAP. BUILDING

Forensic Expertise

- DIGITAL FORENSICS
- DOCUMENT FORENSICS

Operations

- CYBER INTELLIGENCE
- HIGH-TECH CRIMES
- PAYMENT FRAUD
- CHILD SEXUAL ABUSE
- AP CYBORG
- AP TERMINAL
- AP TWINS
- JOINT CYBERCRIME ACTION TASKFORCE (J-CAT)

EC3 Cybercrime Operations

EUROPOL EC3 European Cybercrime Centre

Critical infrastructures and information systems

Cyber Attacks

AP CYBORG

Cyber Intelligence Team

Organized groups generating large criminal profits

Serious harm to the victims

Payment Card Frauds

AP TERMINAL

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Child Sexual Exploitation

AP TWINS

EC3 Cyber Intelligence Team

EUROPOL EC3 European Cybercrime Centre

- Analytical hub: collection + process + analysis.
- Disparate intel feeds: public, private and open sources
- Identify emerging threats and patterns
- Support other EC3 teams
- NO surveillance
- NO infiltration

EC3 Joint Cybercrime Action Taskforce

EUROPOL
EC3 | European Cybercrime Centre

JOINT CYBERCRIME
J-CAT
ACTION TASKFORCE

High-Tech Crimes

Online Child Sexual Exploitation

Payment Fraud

Cybercrime facilitators

EC3 Advisory Groups

EUROPOL EC3 European Cybercrime Centre

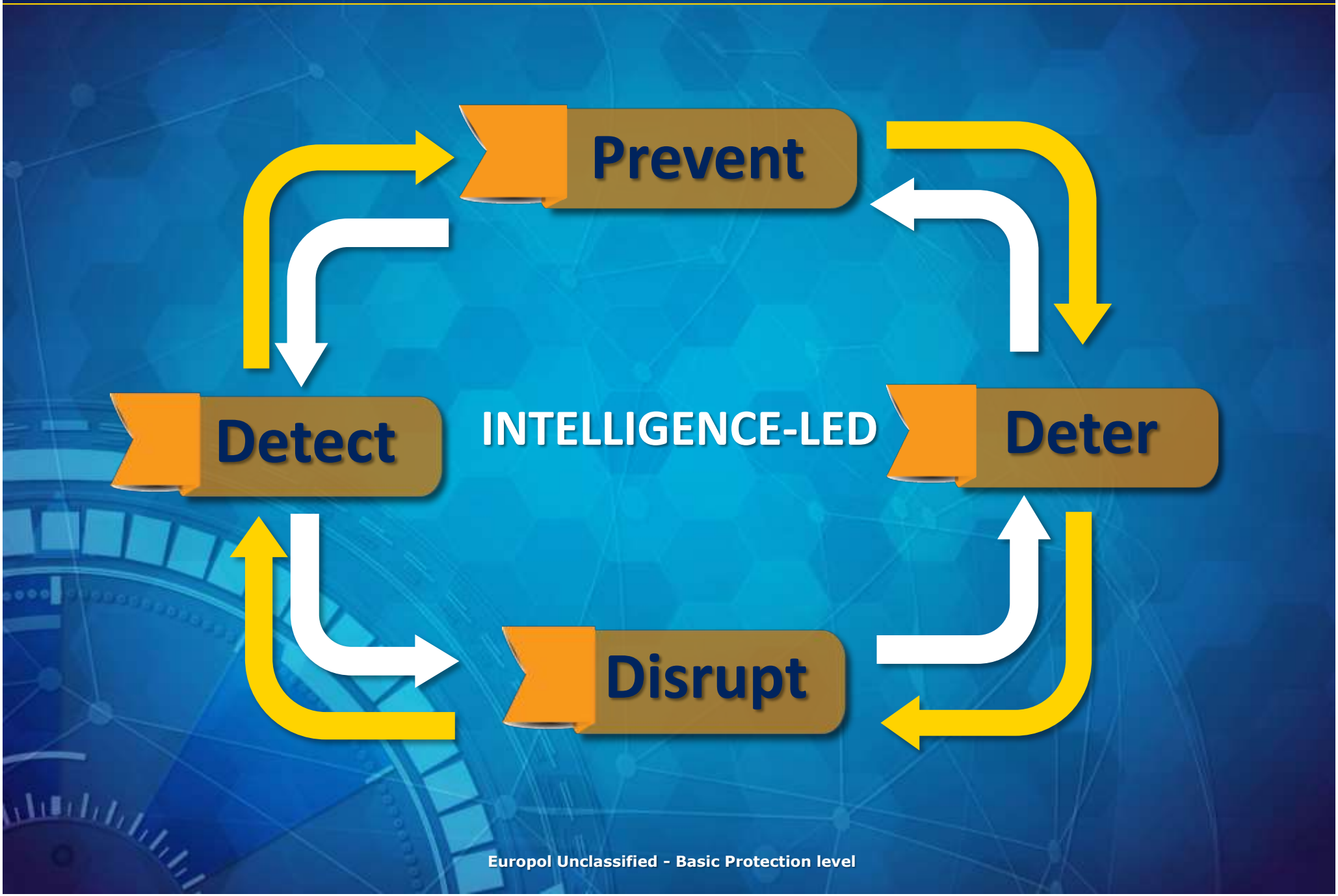
Communication Providers

Financial Services

Internet Security

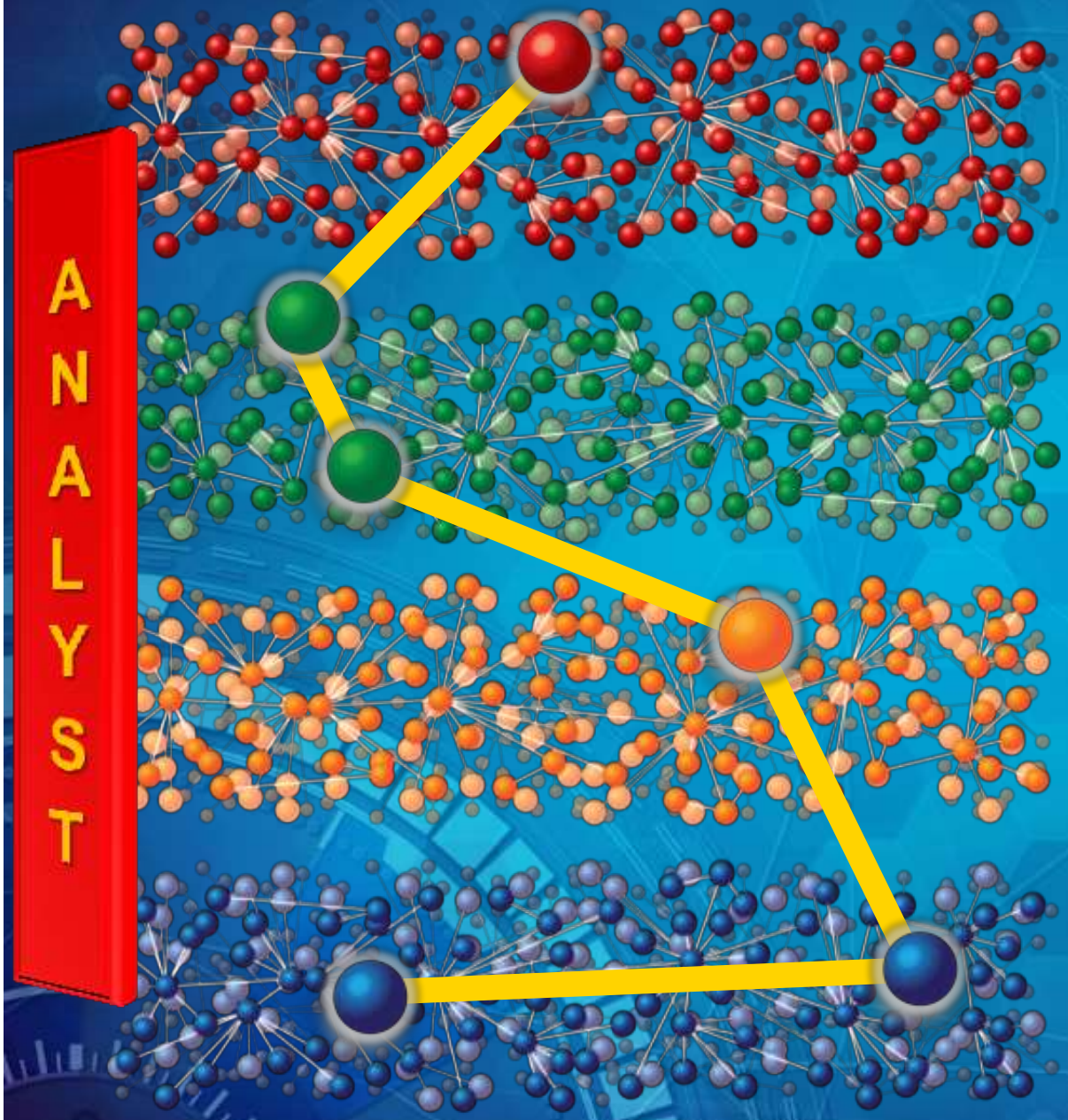
EC3 Cybercrime Fighting Model

EUROPOL EC3 European Cybercrime Centre



From Collect to Connect

EUROPOL EC3 European Cybercrime Centre



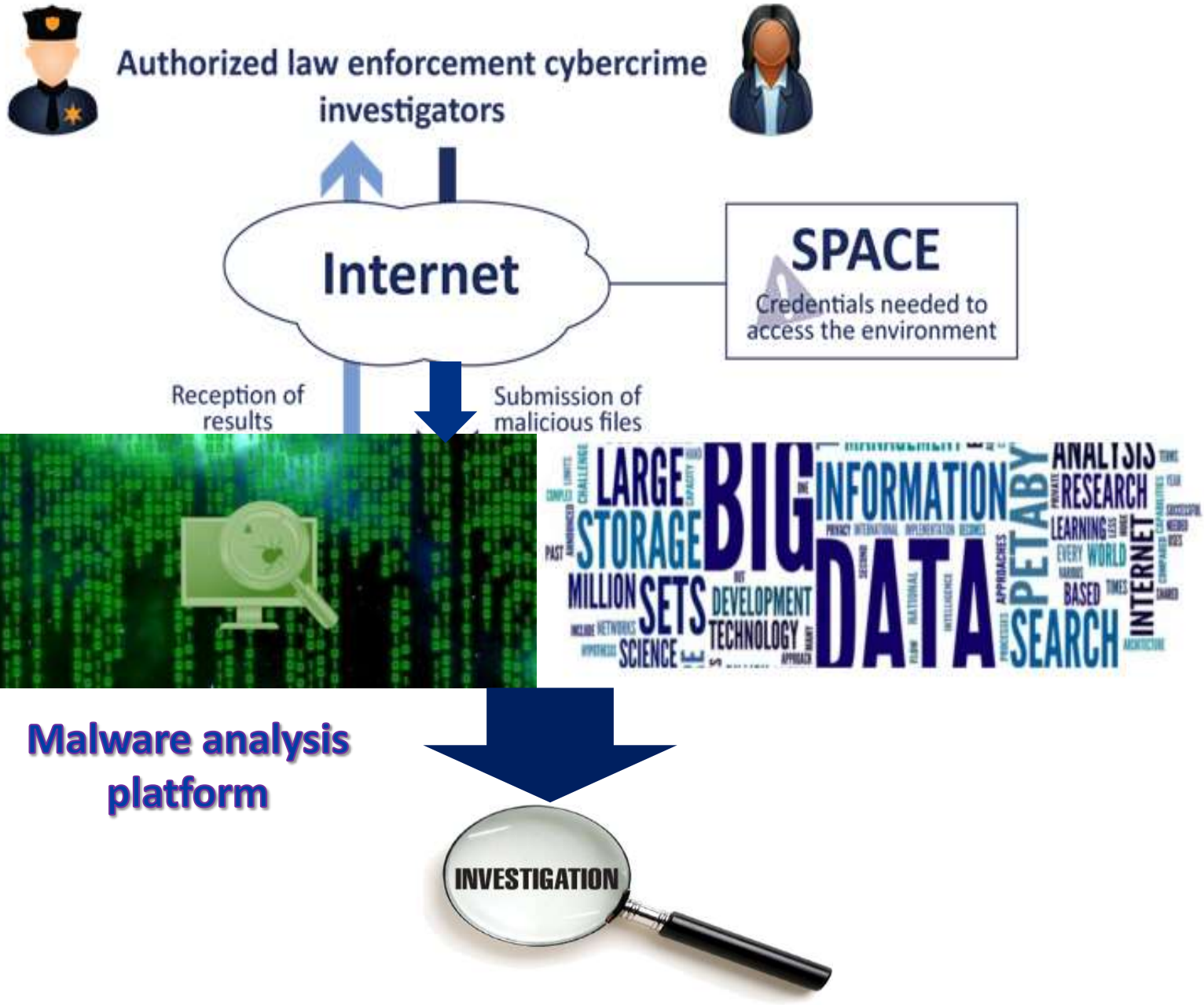
Law Enforcement, Private Sector and Academia's contributions

Intel from current and past investigations

Forensics indicators

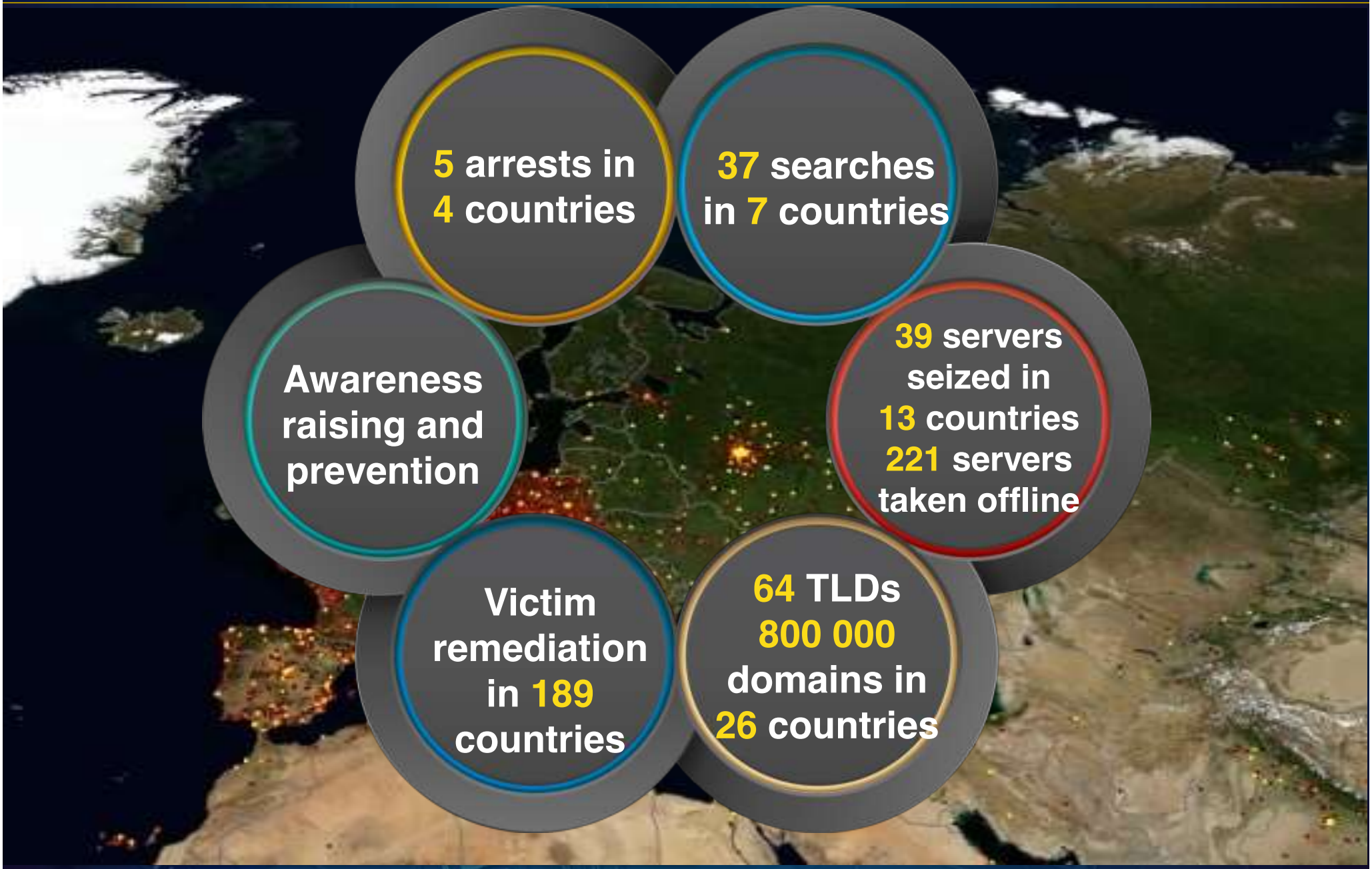
Appropriate tools

EC3 Operations flow



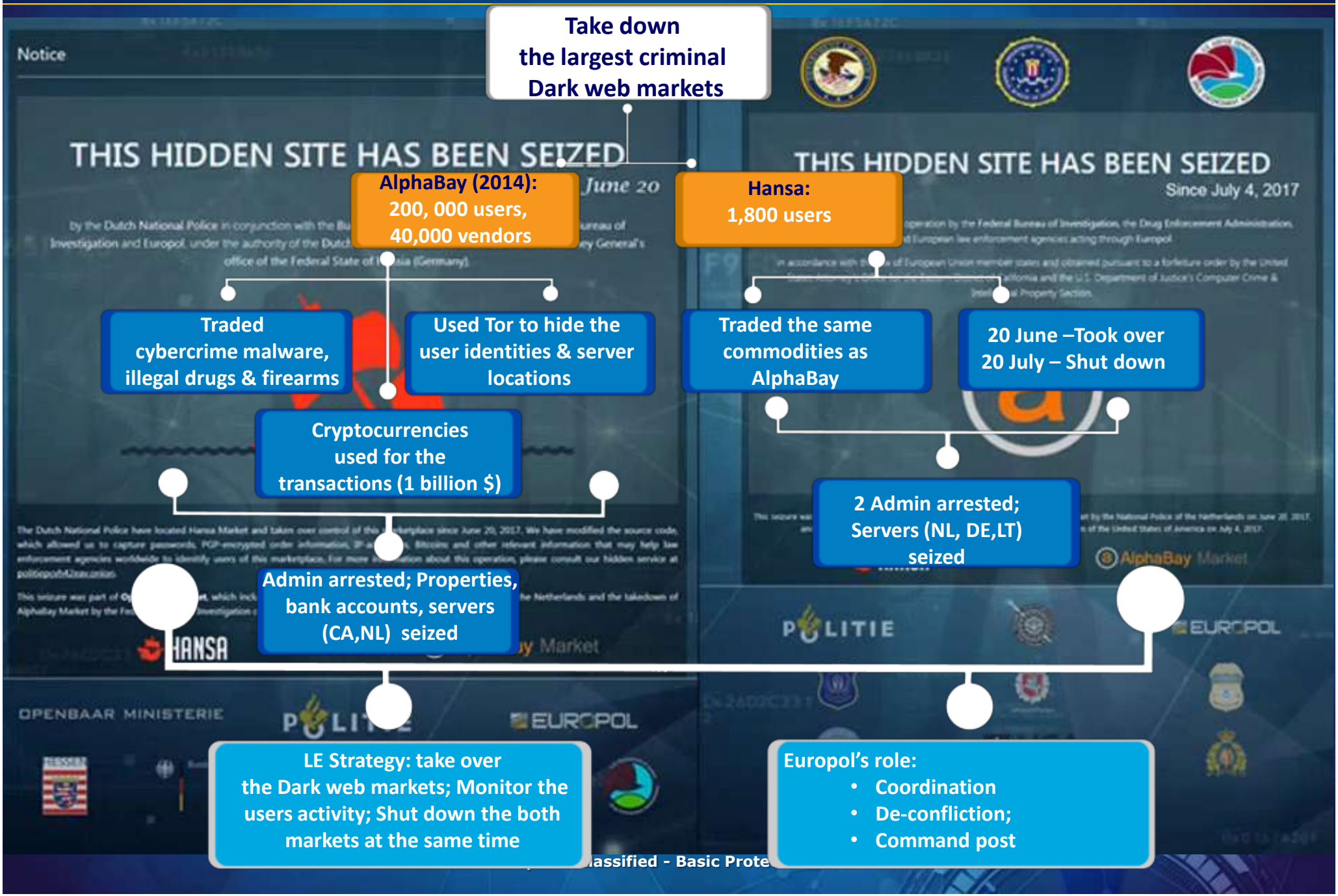
Operation Avalanche - Nov 2016

EUROPOL EC3 European Cybercrime Centre



Operation Bayonet & GraveSac

EUROPOL EC3 European Cybercrime Centre



Take down the largest criminal Dark web markets

AlphaBay (2014): 200, 000 users, 40,000 vendors

- Traded cybercrime malware, illegal drugs & firearms
- Used Tor to hide the user identities & server locations

Hansa: 1,800 users

- Traded the same commodities as AlphaBay
- 20 June –Took over 20 July – Shut down

Cryptocurrencies used for the transactions (1 billion $)

- Admin arrested; Properties, bank accounts, servers (CA,NL) seized
- 2 Admin arrested; Servers (NL, DE,LT) seized

LE Strategy: take over the Dark web markets; Monitor the users activity; Shut down the both markets at the same time

Europol's role:

- Coordination
- De-confliction;
- Command post

EC3 approach to Cyber Intel

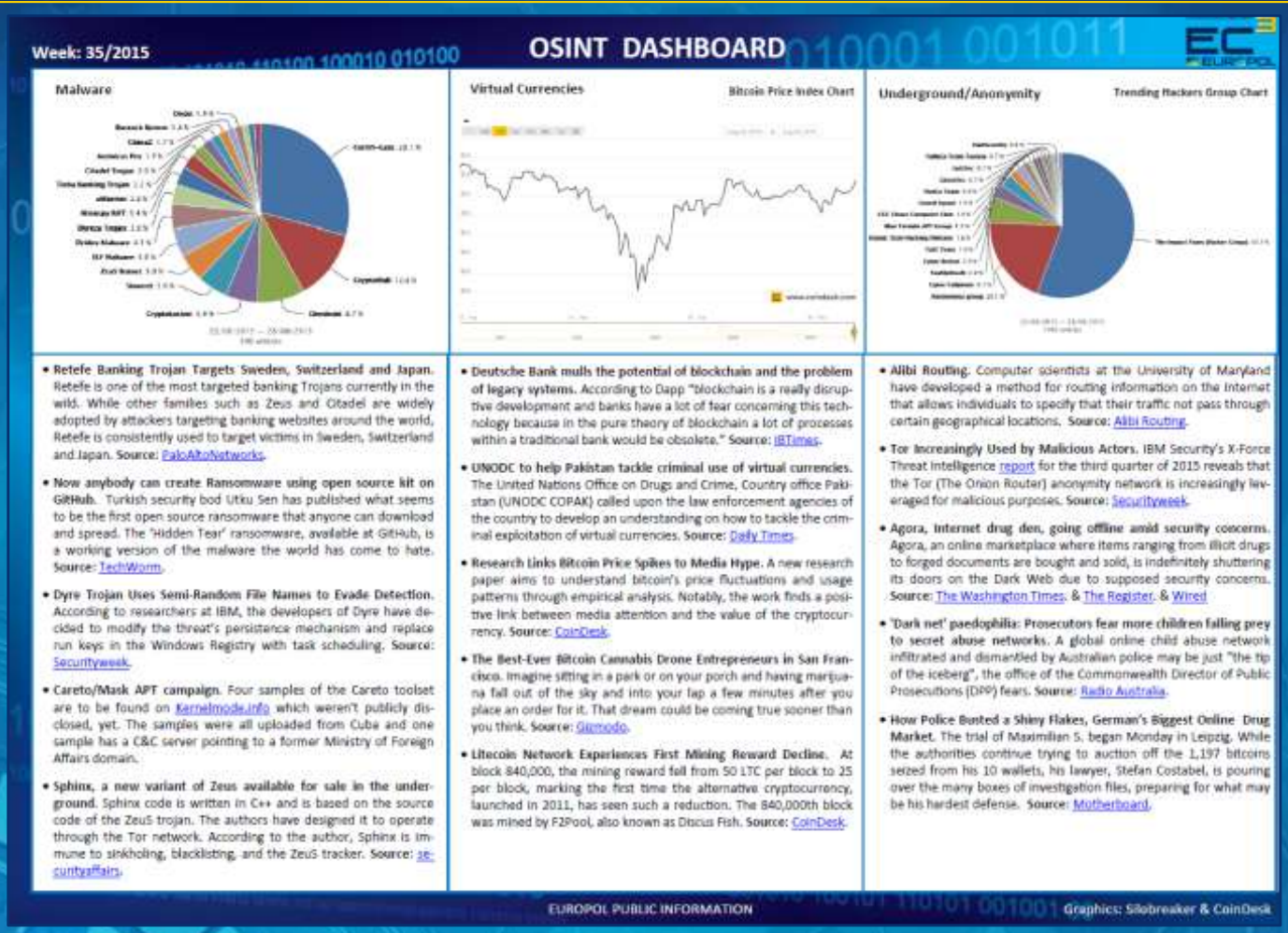
- Operational and Tactical phases
- Threat Identification in the contributions (IoCs , TTPs) + Dissemination of the tactical intel to the MS/ TC
- Strategic intel based in the tactical intel gathered-generated by specialist and analysts
- Strategic intel to tackle international cybercrime by the MS
- Strategic intel to assess Europol and its constituency in better decision-making and risk identifying

EC3 strategic product: Cyber Bits

- Short intelligence notifications
- Objective: raise awareness, trigger discussions, ask for further actions.
- Distributed to LEAs and relevant partners.
- Public ones posted on the Secure Platform for Accredited Cybercrime Experts (SPACE), Europol's Platform for Experts (EPE) on cybercrime.

EC3 strategic product: Dashboard

EUROPOL EC3 European Cybercrime Centre



Weekly most important cyber events related with the EC3 ecosystem

EC3 strategic product: IOCTA

EUROPOL EC3 European Cybercrime Centre

Takeaways

EUROPOL EC3 European Cybercrime Centre

Gather the best manpower

Use the best tools

Build your trust ecosystem

"I have been impressed with the urgency of doing. Knowing is not enough; we must apply. Being willing is not enough; we must do."
Leonardo da Vinci (1452-1519)

Consume better not more

Chess approach

EUROPOL

EC3 | European Cybercrime Centre

Let's make Europe safer

Follow us: **@EC3Europol**

alvaro.azofra@europol.europa.eu