EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Successful Botnet Takedowns: The-good-cooperation part

Margarita Louca

FP Cyborg – EC3

EUROPOL

EUROPOL

European Union's law enforcement agency

Europol is an information and criminal intelligence hub

Acts as a coordination platform for joint operations

Facilitates cooperative actions and the secure exchange of information between Member States, but also LEA and private sector

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

European Cybercrime Centre

EUROPEAN CYBER CRIME CENTRE

Cybercrimes committed by Organised Groups, particularly those generating large criminal profits such as online fraud

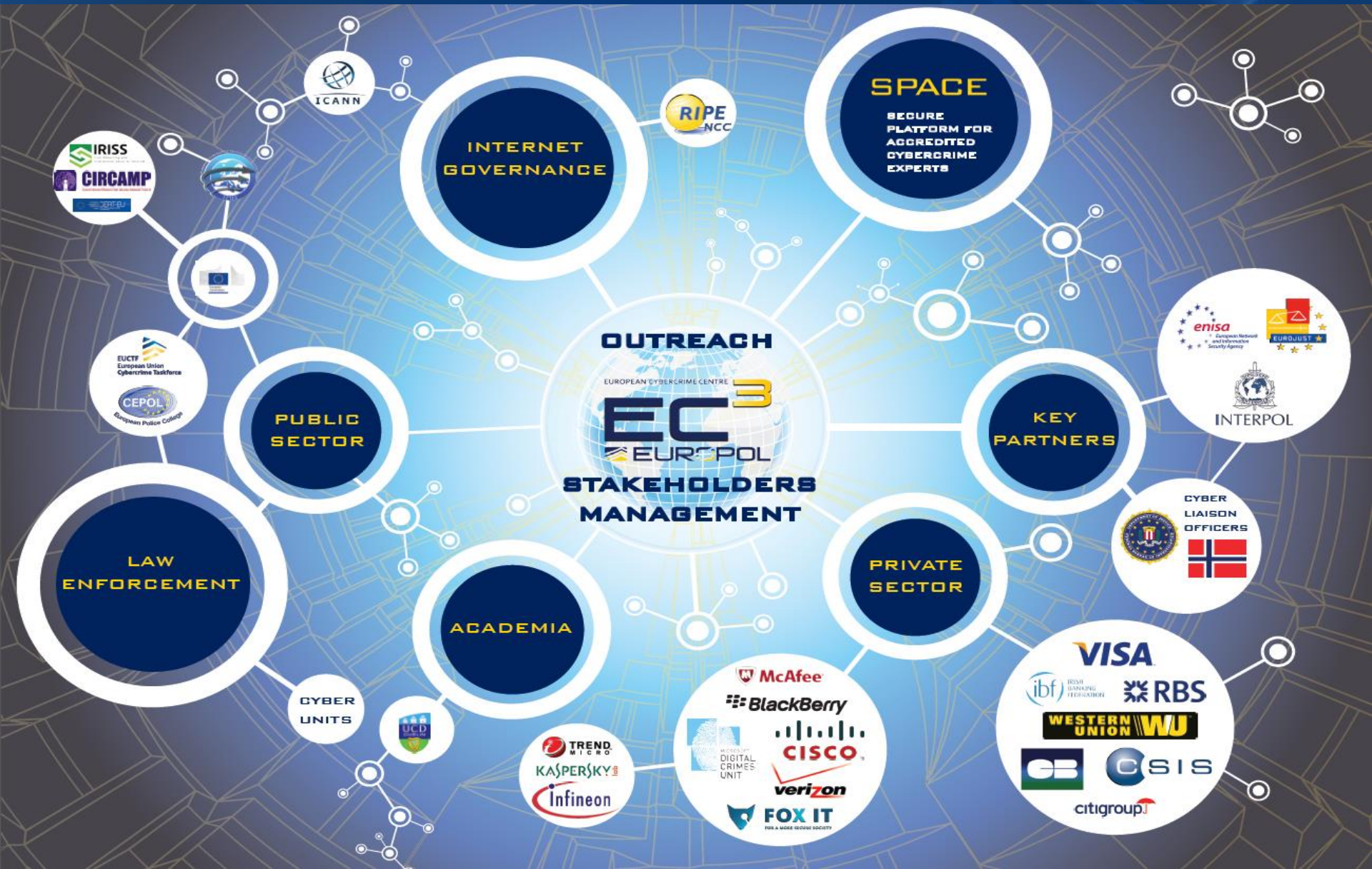
Cybercrimes which cause serious harm to their victims, such as online child sexual exploitation

Cybercrimes (including cyber attacks) affecting critical infrastructure and information systems in the Union

EUROPEAN CYBERCRIME CENTRE

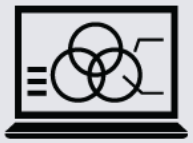
EC3 EUROPOL

Multi-Stakeholder



EC3 Operations

FP Cyborg



Cyborg

Building a cross-border information on active criminal groups, group structures, roles, modus operandi, routes for/or money, sequences of events, etc.

Primary Goal

Coordinating and supporting the cross-border criminal investigations into cyber incidents or to initiate new cross-border cases.

Focus on cybercrime

Focus on Internet/ICT driven organized crime aiming at financial gain.
Crimes defined in the cyber crime convention (art. 2 - 8) including, but not limited to ID theft, e-banking scams, e-commerce fraud and e-laundering

Botnet Takedowns

Europol-Coordinated Botnets Takedowns

Game Over Zeus

May 2014

Feb 2015

Ramnit

Shylock

July 2014

Beebone

April 2015

Operation Shylock – July 2014

Shylock Trojan – attacks online banking systems

Action day: **July 2014**

LEA partners: **EUROPOL, FBI, UK's NCA**

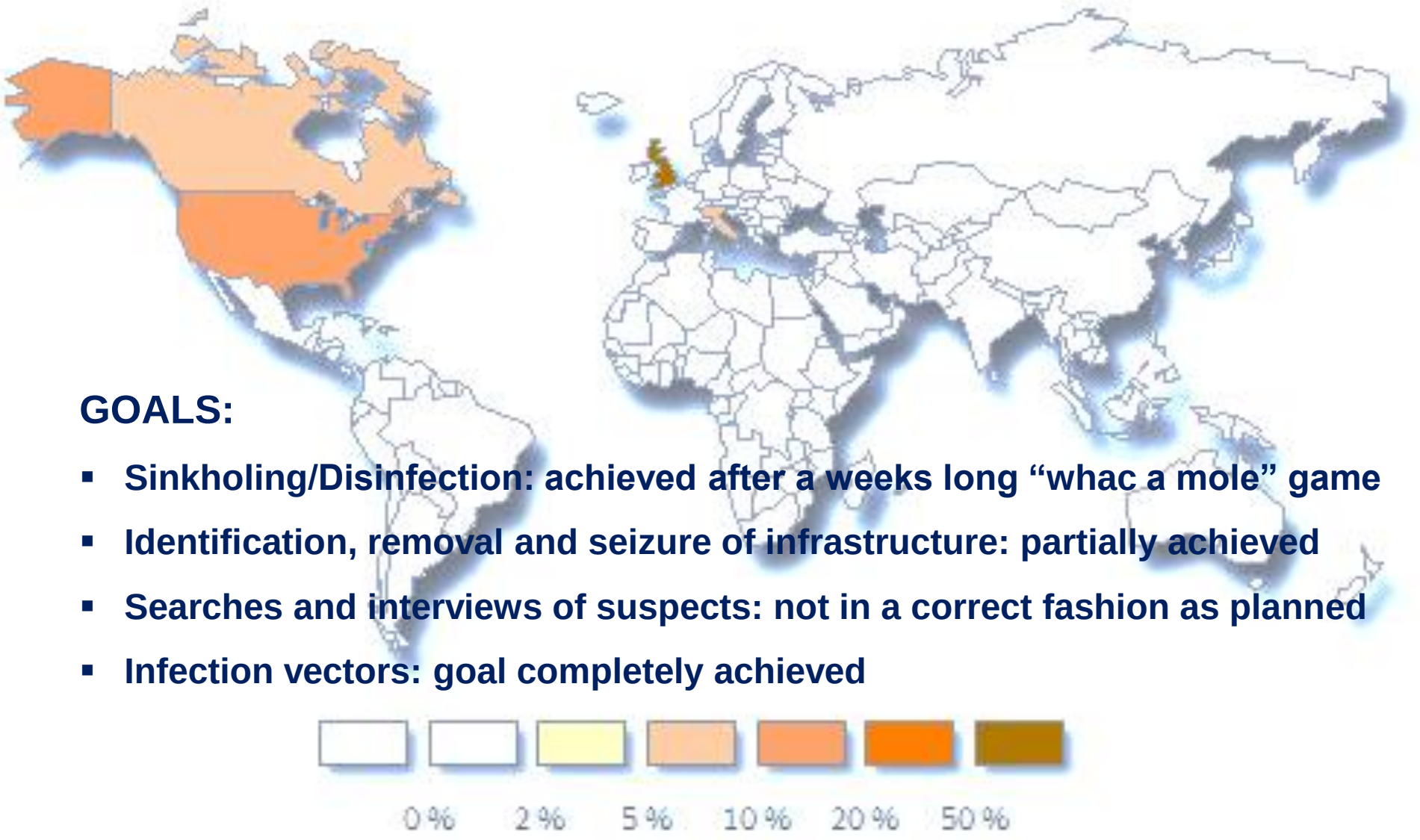
Private sector: **BAE Systems Applied Intelligence, Dell SecureWorks, Kaspersky Lab, UK's GCHQ**

CERT-EU participated in the takedown and distributed information on the malicious domains to the peers

EUROPEAN CYBERCRIME CENTRE

EC3 EUROPOL

Operation Goals



GOALS:

- **Sinkholing/Disinfection: achieved after a weeks long “whac a mole” game**
- **Identification, removal and seizure of infrastructure: partially achieved**
- **Searches and interviews of suspects: not in a correct fashion as planned**
- **Infection vectors: goal completely achieved**

Learning Points

Industry's task to align sinkholing wasn't completely efficient:

- Not all the parties could act
- The court order couldn't be changed to include new domains
- Troubles with blocking the .SU domains
- Industry busy with the MSRT, not the sinkholing itself

Mainly Tier 1 and partly Tier 2 servers were taken down:

- Not completely mapped out
- The plan was not communicated in detail
- Information received late

Searches and seizures planned:

- Not concerted

Ramnit – February 2015

Ramnit Trojan – hijacking online banking sessions etc

Action day: **February 2015**

Command post hosted at Europol HQ

Participants: **EC3, UK's NCA, FBI, DE, NL, IT, J-CAT***

Private sector: **Microsoft, Symantec, AnubisNetworks**

Operational Outcome

- Command & control server identified and successfully taken down
- 7 servers were seized
- Entire infrastructure of the botnet was taken down
- 300 domains used by botnet's operators were seized and botnet was sink-holed
- Removal tool released by Microsoft & Symantec
- For mitigation purposes, information was channeled to CERT-EU for dissemination to National CERT's

So… successful piece of action, smoothly executed and the perfect example that LEA can undertake action in cooperation with industry

But… there are some open ends!

Botnet Down.. Botnet UP!

Unfortunately..

Botnets don't simply die after the takedown!

Because…

- **Incident handling in organizations varies a lot**
- **No common/baseline operating procedures for responding to and recovery from attacks/incidents**
- **Different directories are used for information sharing and mutual response**
- **Persistence of the botnets itself**
- **Legal issues**

The Challenge

- Build trust among participants
- Reporting & journalism
- Prevent new infections
- Information sharing among expert groups
- Minimize profitability of botnets and cybercrime
- Align our activities and map-out criminal activity


~~Law Enforcement~~ Joint Action!

Obviously what we need is multi-actor eco system in which the relevant stakeholders have and can take up their role without competition or redundant overlapping with others.

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Thank you