BKA Autumn Conference 2014

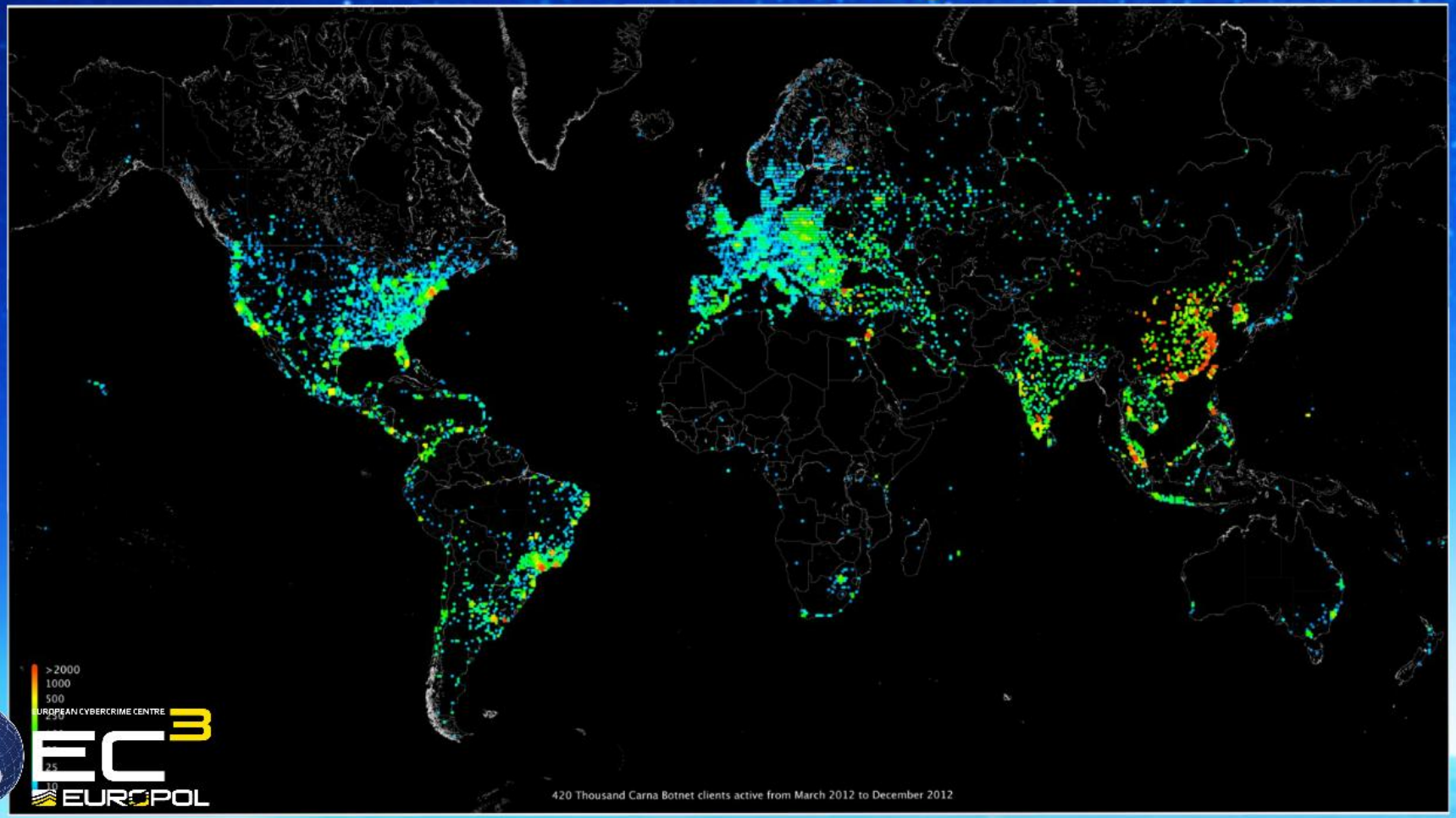
Technical Challenges and Required Response

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

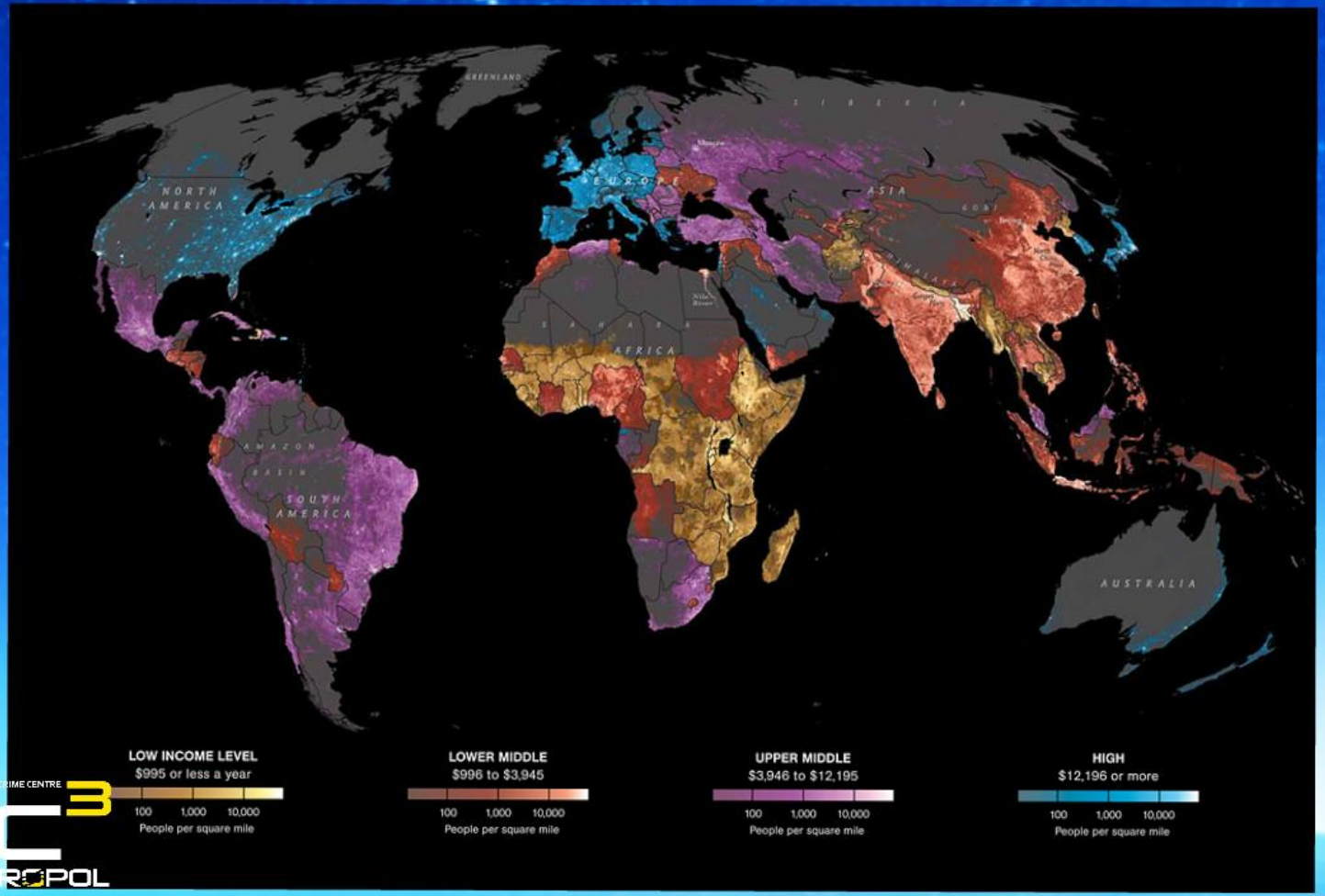
20 November
Mainz, Germany

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Live Internet Usage



Income Distribution Worldwide



EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

NORSE

ATTACK ORIGINS

#	Country
1311	China
1020	United States
368	Mil/Gov
111	Netherlands
111	Russia
80	Canada
78	Japan
76	Hong Kong
51	Italy
45	South Korea

ATTACK TARGETS

#	Country
3148	United States
97	Hong Kong
55	Portugal
49	Singapore
42	Turkey
39	Canada
37	Austria
32	Spain
27	Australia
26	Liechtenstein

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-20 02:44:07.47	MJS Marketing LLC	Kansas City, United States	173.208.222.82	New York, United States	unknown	49152
2014-06-20 02:44:09.20	Kazan Broad-band access	Kazan, Russia	78.138.164.167	Seattle, United States	unknown	53377
2014-06-20 02:44:10.17	SunnyVision Limited	unknown, Hong Kong	124.248.211.81	unknown, Hong Kong	CrazzyNet	17500
2014-06-20 02:44:10.77	Softbank BB Corp	Tsu, Japan	219.54.103.5	unknown, United States	unknown	26203
[illegible]	[illegible]	Shanghai, China	101.85.185.110	Saint Louis, United States	unknown	52454
[illegible]	[illegible]	Shanghai, China	180.174.164.126	San Rafael, United States	ipcserver, Sadmind	600
[illegible]	[illegible] Unicom Shanxi	Changzhi, China	60.220.197.249	Saint Louis, United States	unknown	26577
[illegible]	[illegible] AS	unknown, Slovakia	195.146.145.100	San Rafael, United States	telnet	23

ATTACK TYPES

#	Service	Port
654	ssh	22
356	smtp	25
326	ms-sql-s	1433
232	unknown	49152
160	CrazzyNet	17500
135	http-alt	8080
116	domain	53
95	microsoft-ds	445

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Visible Web

Publicly accessible, searchable Internet

4 % indexed

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

96% unindexed

Deep Web

Deep web with limited access

Dark Net

Environment accessible only through specialised software providing users with anonymity and encryption

Challenges

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Cyber-Crime (traditional)

Cyber-Facilitated Crime

Cyber-Facilitated Crime

Cyber-Crime (traditional

Extremist Activity (left-right)

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Terrorism Related Activity

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

State Sponsored Activity

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Organised Crime
Individual/Network Crime

Hacking

Trojans

Malware

Spyware

DDoS

Bots

Darknet

Encryption

Virtual Currency

Crime as a Service

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Malware sent

Tested Malware

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Deep Web

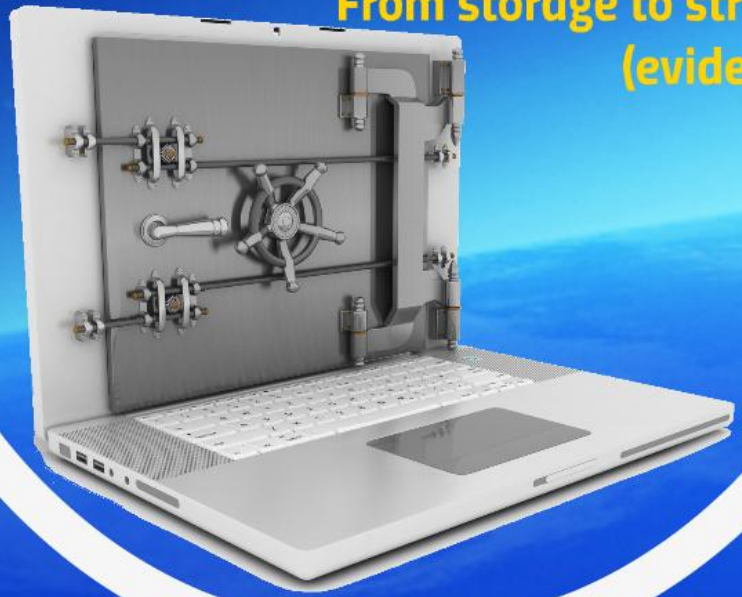
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Dark Marketplaces

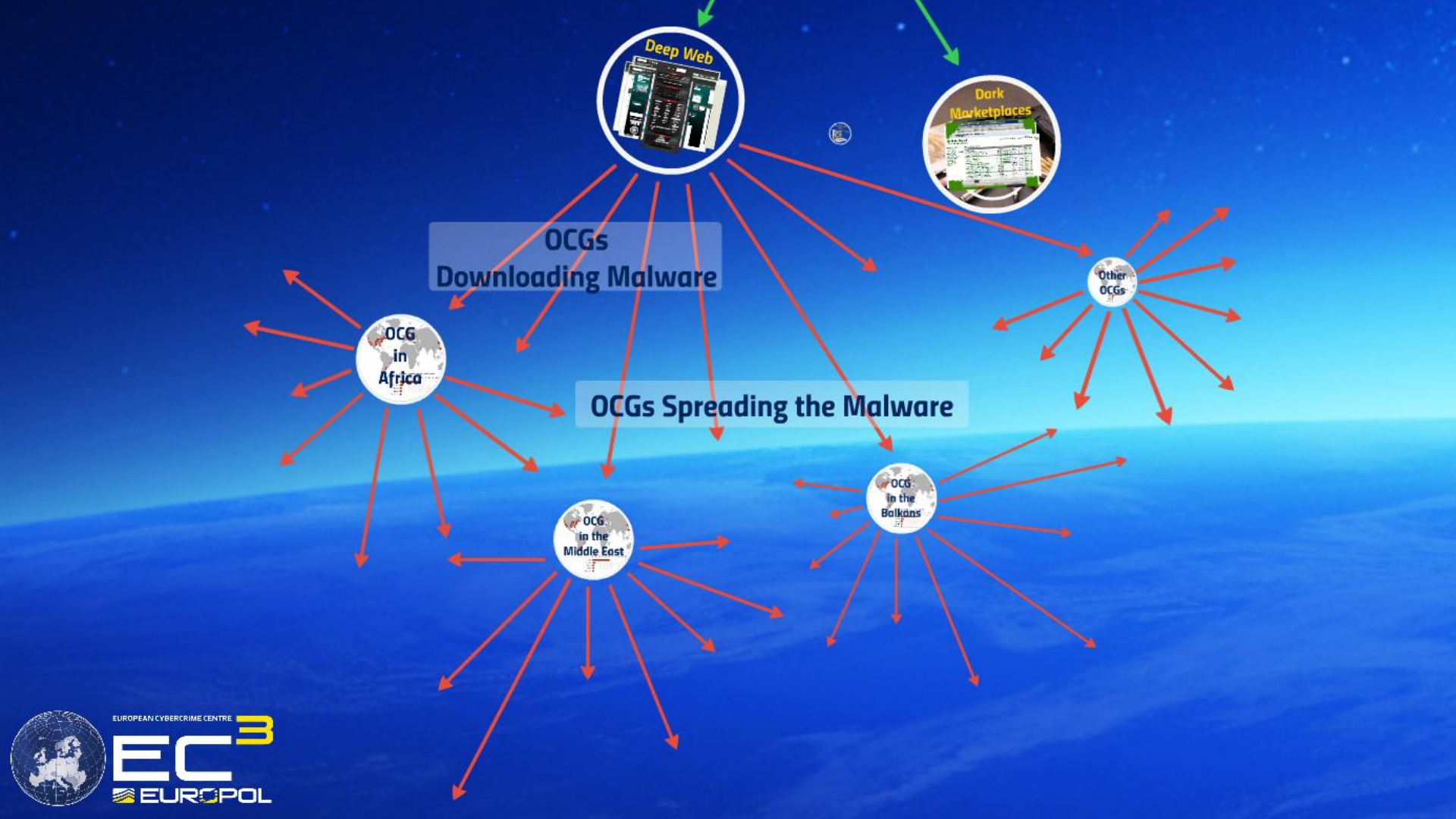
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Bullet Proof Cloud Hosters

From storage to stream (evidence)



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL


Deep Web
Dark Marketplaces
OCGs Downloading Malware
OCG in Africa
Other OCGs
OCGs Spreading the Malware
OCG in the Middle East
OCG in the Balkans
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Coders

Organised Criminals (OC)

Mainstream Criminals

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Physical vs Online Crime: Core Challenges

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Offline	Online
Geographical proximity between criminal and crime scene	No geographical proximity between criminal and crime
Jurisdictional clarity	No clear jurisdiction
Adequate resource allocation of police force depending on crime levels	

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Scale

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Offline	Online
Criminal ties & resources	Anybody can be a cybercriminal

Impact

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Offline

One criminal robbing one bank at a time

Online

One criminal attacking 1 mln computers in 20 countries in 20 sec

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Traceability

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Offline

Limited ability to hide: CCTVs, DNA, biometrics

Online

Tools facilitating anonymity: proxies, onion routers, P2P, encryption

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Offline	Online
Forensics	Traceability Difficult attribution

Present

Server-based electronic evidence gathering

Future

Streaming and cloud services, communication traffic across borders and jurisdictions

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

EC3's Response

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Prevention

Capacity building of first responders

Regional & National

Prosecutors & Judges

Outreach Program

Protection

Virtual Police Stations/Police Officers

Online Patrol

National systems for ensuring security by design

National standards for securing business and cities' sensitive information

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Prosecution

The obstacles between the jurisdiction of nation states vs. the global nature of cyber crime

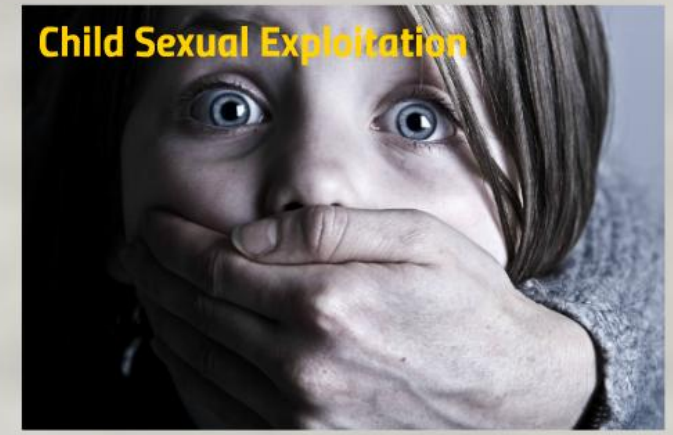
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Governance

Who owns the Internet?

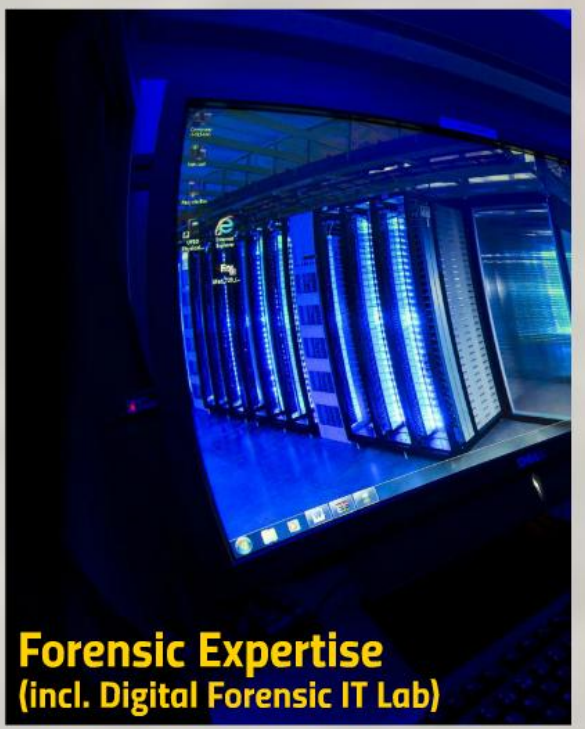
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Operations



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Strategy



EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

J-CAT

Joint Cybercrime Action Taskforce

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Taskforce Approach in Addressing Cyber Threats

Identification of priorities → INVESTIGATION ← Investigative opportunities

Areas of Competence

Intrusion

Crime-facilitation

Online fraud

Child sexual exploitation online

24/7 Permanent Taskforce operating from EC3

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL


Retail
Public Sector
Private Sector
Academia
J-CAT
Joint Cybercrime Action Taskforce
Security Companies
Cyber Units
Financial Sector
Member States
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

EC3 Programme Board

Direct interaction of EC3 in relevant areas

assisted by

2 Advisory Groups

Ongoing set up of Working Groups on:

Industrial Cross-Sector Developments

Cyber Psychology

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

EC3 Programme Board

Direct interaction of EC3 in relevant areas

assisted by

2 Advisory Groups

Programme Board

Advisory Board created to help the strategic decision-making process of EC3

European Commission

enisa European Network and Information Security Agency

CEPOL European Police College

EUROJUST

EC3 EUROPOL

computer emergency response team CERT-EU

INTERPOL

EUCTF European Union Cybercrime Taskforce

CONSILIUM

Internet Security

BlackBerry

McAfee

CISCO

FOX IT

DIGITAL CRIMES UNIT

IRISS

KASPERSKY lab

TREND MICRO

verizon

Infineon

Financial Services/EUFCC

CB

citigroup

VISA

WESTERN UNION WU

CSIS

RBS

ibf IRISH BANKING FEDERATION

EUROPEAN CYBERCRIME CENTRE

EC3 EUROPOL

EUCTF
European Union
Cybercrime Taskforce

European Union Cybercrime Task Force

European Cybercrime Training and Education Group (ECTEG)

European Cybercrime Prevention Framework

European Forensics Framework

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Ongoing set up of Working Groups on:

Industrial Cross-Sector Developments

Cyber Psychology

Roadmap for Next Steps

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Combating Crime in a Digital Age

Thank you

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL