THE EUROPEAN COMMISSION AND THE FIGHT AGAINST CYBERCRIME: FROM MARKETIZATION TO SECURITIZATION?

ANA PAULA BRANDÃO (CICP-EEG, UM)
abrandao@eeg.uminho.pt

CONGRESSO DE CIBERCULTURA

PAINEL 'NOVOS DESAFIOS E CIBERCRIME'

CECS-UM, 13 OUTUBRO 2016

AGENDA

SECURITY ACTORNESS AND SECURITY GOVERNANCE

WHY EU/CYBERCRIME?

EUROPEAN COMMISSION APROACH TO CYBERCRIME

SECURITY ACTORNESS… (B&V)

Opportunity

- Security broadening and deepening + security nexus
- Internal market and transnational security threats

Capability

- Institutional
- legal, political, policy, resources

Presence

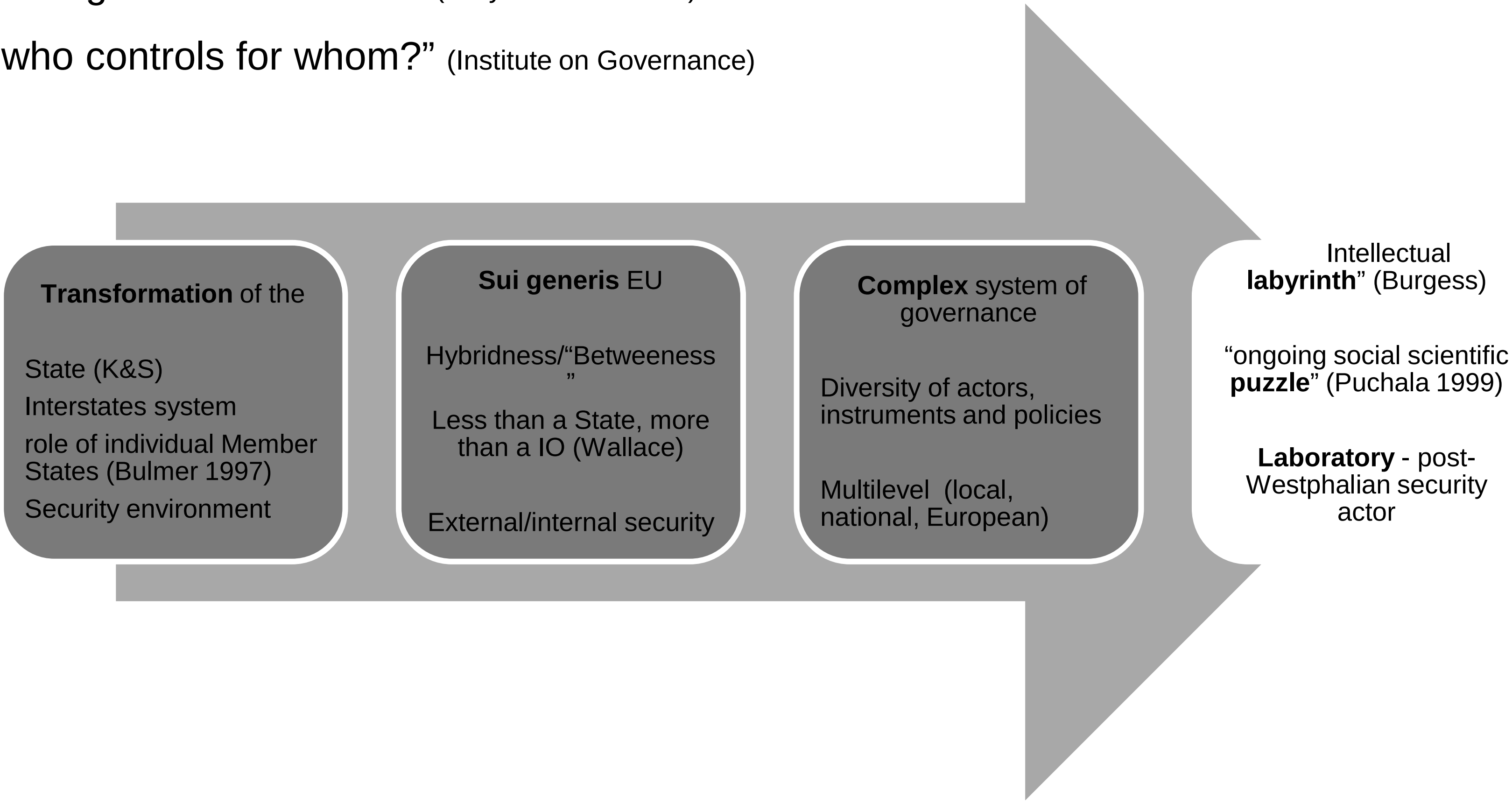
- (collective) Internal security …
- External dimension of internal security ('external governance')

…SECURITY GOVERNANCE

… without a government

“who governs and how?” (Chryssochoou 2001)

“who controls for whom?” (Institute on Governance)



Transformation of the

State (K&S)

Interstates system

role of individual Member States (Bulmer 1997)

Security environment

Sui generis EU

Hybridness/“Betweeness ”

Less than a State, more than a IO (Wallace)

External/internal security

Complex system of governance

Diversity of actors, instruments and policies

Multilevel (local, national, European)

Intellectual **labyrinth**” (Burgess)

“ongoing social scientific **puzzle**” (Puchala 1999)

Laboratory - post-Westphalian security actor

…SECURITY GOVERNANCE (K&S)

TASKS

Prevention	• inter/intra-state conflict prevention through the building of democratic institutions and the consolidation of civil society [e.g. enlargement; conditionality; ENP]
Assurance	• peace-building [e.g. Stability Pact; Stabilization and Association Program]
Compellence	• implementation of the CSDP through peace-making, peace-keeping and peace-enforcement autonomous missions
Protection	• (collective) internal security

WHY EU/CYBERCRIME?

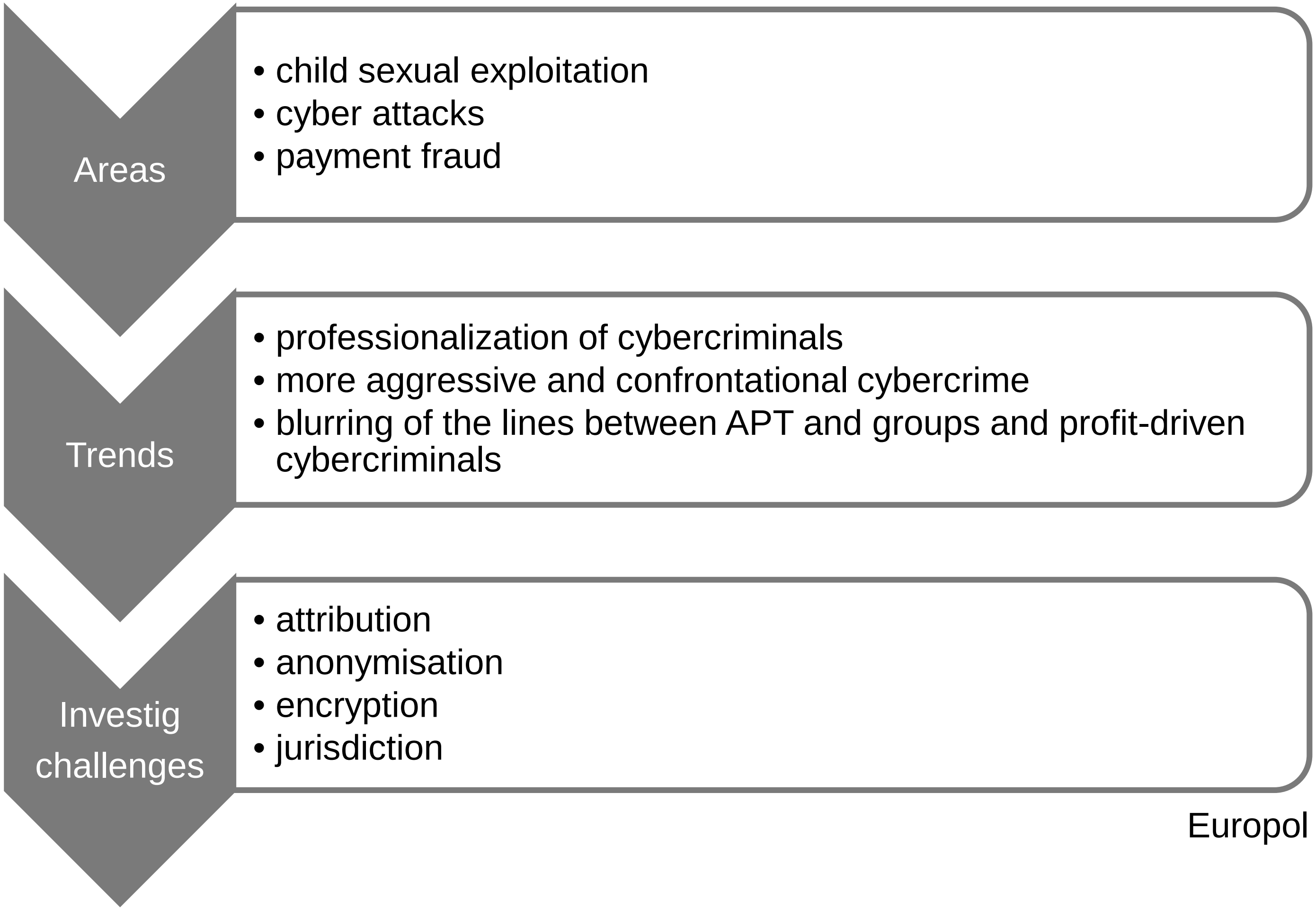
- Transboundary security problem ⬄ “comprehensive approach”

- EU, a key target

- Expansion and sophistication
  - “computer-related fraud and forgery” (Europol 2013)
  - “computer-related production, distribution or possession of child pornography” (UNODC 2013)

- **Public-private nexus**
  - European Commission – internal market and private sector
  - [European Parliament - fundamental rights]

WHY CYBERCRIME?



Areas

- child sexual exploitation
- cyber attacks
- payment fraud

Trends

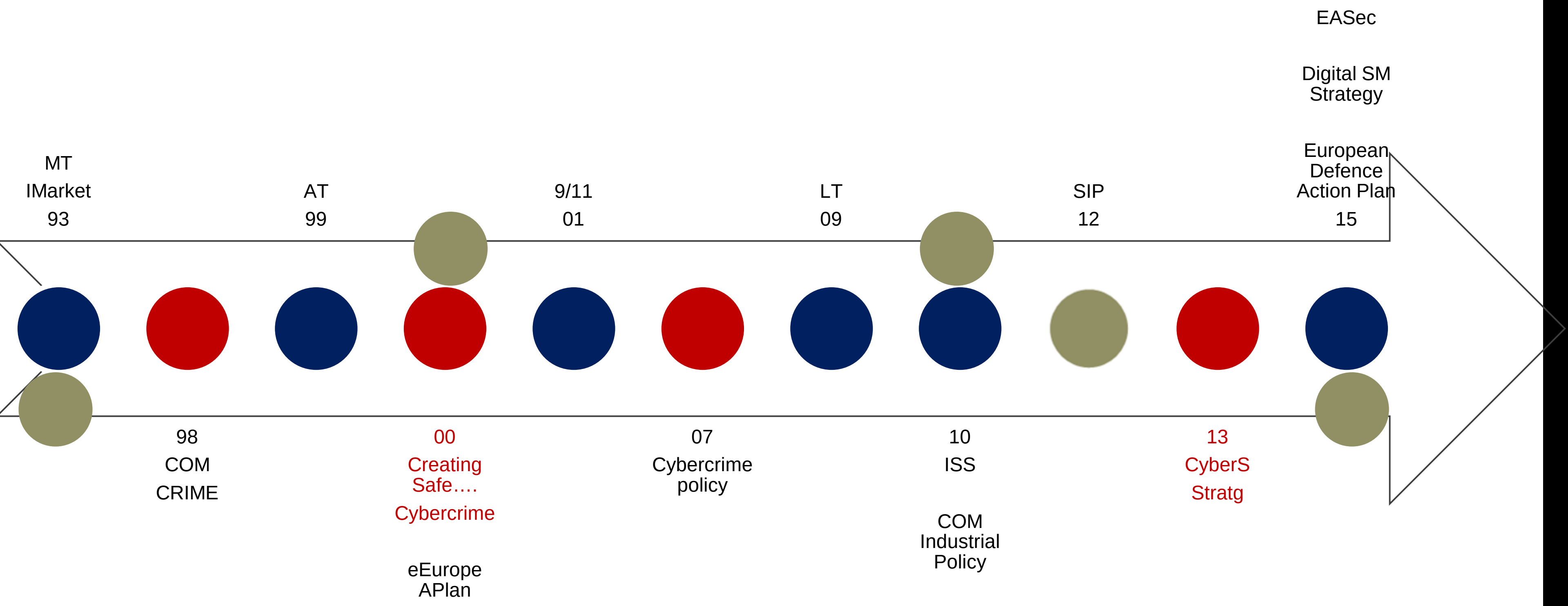
- professionalization of cybercriminals
- more aggressive and confrontational cybercrime
- blurring of the lines between APT and groups and profit-driven cybercriminals

Investig challenges

- attribution
- anonymisation
- encryption
- jurisdiction

Europol 2015

COMMISSION APPROACH



MT
IMarket
93

98
COM
CRIME

AT
99

00
Creating Safe….
Cybercrime

eEurope APlan

9/11
01

07
Cybercrime policy

LT
09

10
ISS

COM Industrial Policy

SIP
12

13
CyberS
Stratg

EASec

Digital SM Strategy

European Defence Action Plan
15

COMMISSION APPROACH

- Securitization

“major security threat”, “a priority”, “an urgent need to take action”

“I don't think I exaggerate when I say that this must be the golden age for cyber criminals” (Malmström 2011)

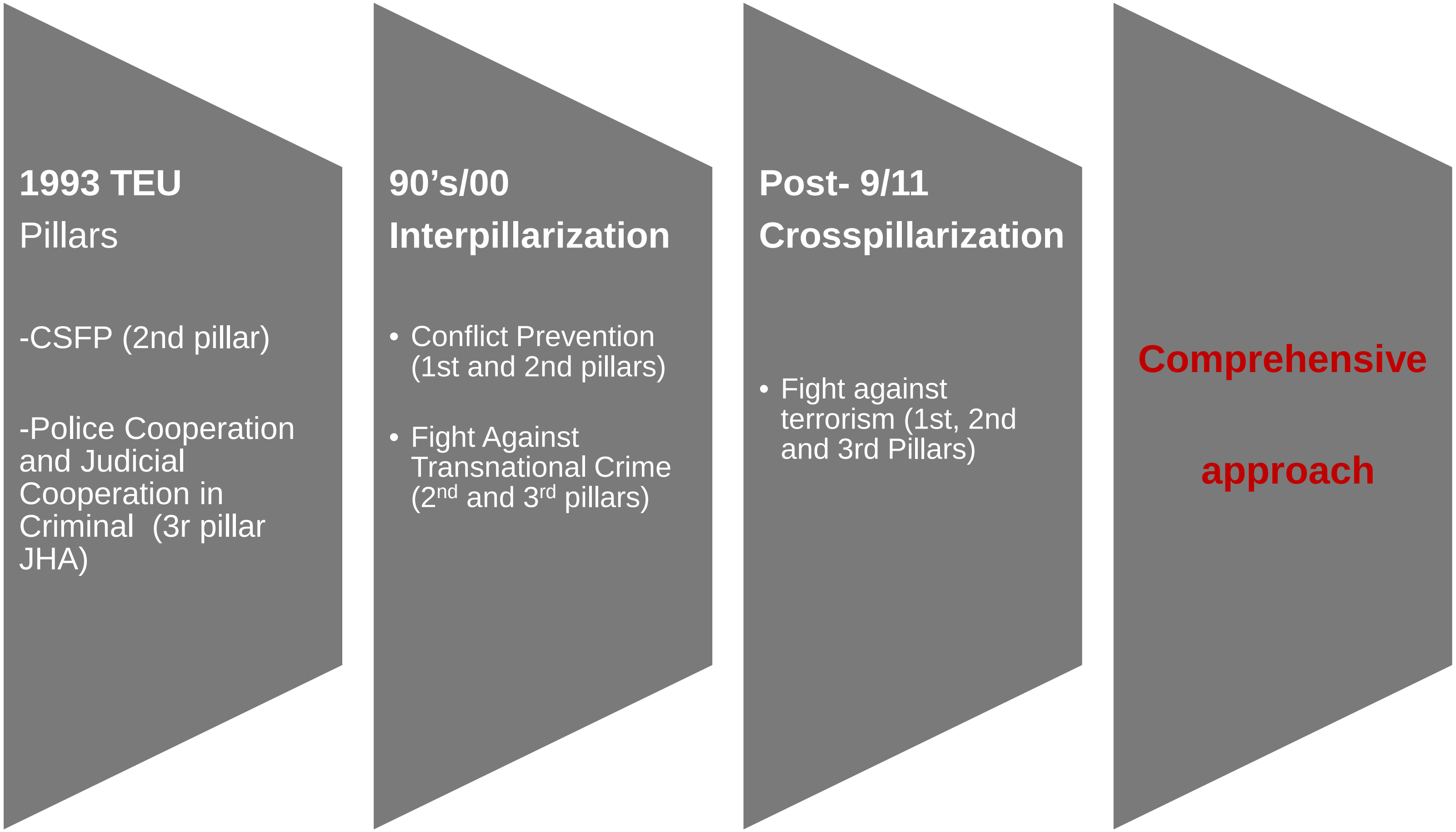
“The surge in Internet users has made cybercrime and terrorist use of the Internet a new frontier of 21st century warfare.” (HR/VP 2016)

COMMISSION APPROACH

- For a common definition of cybercrime
  - “criminal acts committed using electronic communications networks and information systems or against such networks and systems"
  - 3 categories of activities: traditional forms of crime; publication of illegal content over electronic media; crimes unique to electronic network (European Commission 2007)

- **Comprehensive approach**
  - multi-stakeholder cooperation
  - multi-policy areas
  - multi-instruments
  - security nexus (internal-external; public-private)

COMMISSION APPROACH



1993 TEU

Pillars

-CSFP (2nd pillar)

-Police Cooperation and Judicial Cooperation in Criminal (3r pillar JHA)

90’s/00

Interpillarization

- Conflict Prevention (1st and 2nd pillars)
- Fight Against Transnational Crime (2nd and 3rd pillars)

Post- 9/11

Crosspillarization

- Fight against terrorism (1st, 2nd and 3rd Pillars)

Comprehensive

approach

COMMISSION APPROACH

Lisbon Treaty

EU legal personality – end of the dual system

Security area under a IO

Internal security – TFEU + community method

Covered pillar – CSF/CSDP

High Representative – Council Commission

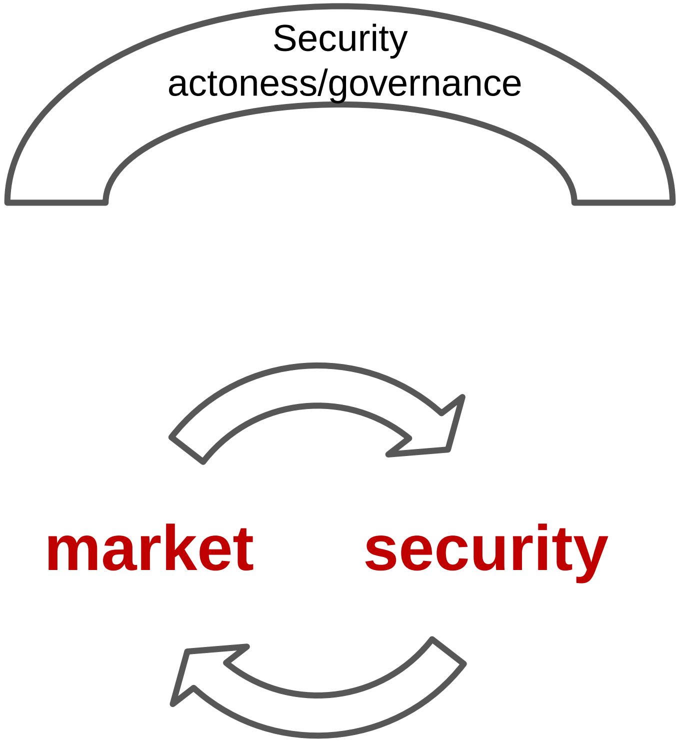
President - European Council

	Economy	Security	External Relations and CSDP
Goals	growth, competitiveness and employment	Security of citizens and businesses, member states, infrastructures	International cooperation Cyberdefense
Policy Domains and Issues	Internal market Liberalization of telecommunications markets Information Society and Digital Europe (IST dissemination, market liberalization, data protection, copyrights) Security Industrial Policy	Internal security (fight against organised crime, fraud, traffic of human beings, child pornography, racism and xenophobia; counterterrorism and fight against radicalization) Criminal Law Cybersecurity (securing network and information systems)	States - US (EU/US working group on cyber-security and cybercrime; 2012 EU-US initiative to launch a Global Alliance against Child Sexual Abuse Online) IOs and International Regimes -Council of Europe (Convention on Cybercrime; OCTPUS) -Interpol - ITU (Global Cybersecurity Agenda) -NATO (Technical Arrangement between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team – European Union (CERT-EU (2016) - IMPACT - International Multilateral Partnership Against Cyber Threats - London Action Plan - Virtual Global Task Force

COMMISSION APPROACH

- **Public-Private cooperation**
  - definition of a “strategy for cooperation between the public sector and private sector operators, including civil society organisations”
- Horizontal Coordination
  - structures for cross-border operational cooperation
- Normative dimension
  - Fundamental rigts (freedom of expression, respect for private and family life, protection of personal data)

FROM MARKET… TO SECURITY…?



Security actoness/governance

market

security

Presence

Single market

Digital Europe

Security industry / SIP

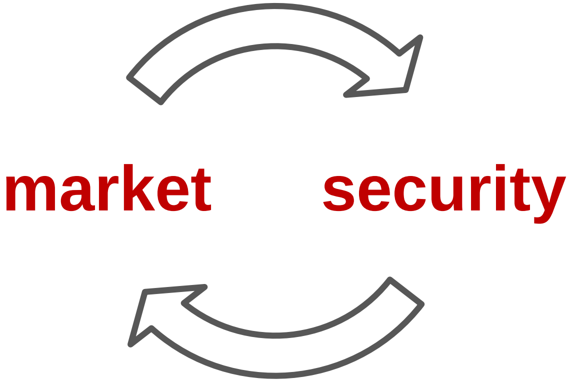
From absence to presence

JHA/AFSJ/’Internal Security

JAIEX

Security Research, S. products

FROM MARKET… TO SECURITY…?



market **security**

“true internal market for security”
a pre-requisite for building the so-called “**EU Security Union**” (COM 2016)

FINAL REMARKS

- Gradual presence of the European Commission in the sensitive security domain

  - Opportunity – transnational threats, EU security actorness/ governance, comprehensive approach, Lisbon Treaty (‘internal security’ – TFEU)

    - European Commission and cybercrime
      - the Commission’s experience in Justice and Home Affairs/Area of Freedom, Security and Justice, including its external dimension; COM knowledge about the private sector (i.e. internal market, competition policy); the ‘window of opportunity’ of the “digital agenda for Europe” and cybersecurity as a part of the Europe 2020 strategy.
      - Upgrated role in internal security (vs external); historical presence, influence and accumulated experience – internal market, private sector
      - securitization actor, entrepreneur, policy-shaper

post-Westphalian (non-statecentric) threat (multi-actor, multi-dimensional, cross-border threat

post-Westphalian system of governance based on “sharing of tasks and responsibilities” and “doing things together instead of doing them alone” (Kooiman 1993)

European Commission

as the promoter of the common interest, with presence in all phases of the policy cycle, is a key actor of the European system that faces the major challenge of complex coordination.

active both in agenda setting and policy formulation, contributing to the move from politicization to securitization of the cyber issue: cybersecurity is one of the priorities of the 2015 Strategic Assessment

“a specific EU policy”

- “improved operational law enforcement cooperation
- better political cooperation and coordination between Member States
- political and legal cooperation with third countries
- awareness raising
- training
- a reinforced dialogue with industry and possible legislative action” (European Commission 2007).

Enhance cybersecurity (EU Internal Security Strategy 2010)

- build capacity in law enforcement and the judiciary (action 1)
- work with industry to empower and protect citizens (action 2)
- improve capability for dealing with cyber-attacks (action 3)