Internet Governance and Cybersecurity

Patrick Curry
MACCSA
patrick.curry@maccsa.net

EU Project MAPPING

MAPPING
Managing Alternatives for Privacy,
Property and Internet Governance

1. Mapping the Internet. 4 years. 13 partners
2. Focus on Internet Governance, privacy and trust
3. Legal and Technical groups

4. For more information: www.mappingtheinternet.eu

5. The goal of MAPPING (Managing Alternatives for Privacy, Property and Internet Governance) is to create an all-round and common understanding of the many and varied economic, social, legal and ethical aspects of the recent developments on the Internet, and their consequences for the individual and society at large.
6. Building on the results of several EU FP7 projects including CONSENT (covering on-line consent and privacy in social networks www.consent.law.muni.cz), SMART (www.smartsurveillance.eu) and RESPECT (http://respectproject.eu).
7. Investigate and debate the existing innovation policies, business models and legal framework related to the implementation of the Digital Agenda for Europe and the changes needed to set up an improved governance structure for the EU innovation ecosystem.

V-P Kroes

- Democracy must talk to technology. We are making a transition to a data driven world

- About simple things, people trusting that their personal data is protected, SMEs understanding cloud protection, citizen understanding eID. <u>Without security there is no privacy</u>.

- Cyber breaches happen for multiple reasons. Over 3/4 of SMEs and 93% businesses suffered at least one breach, each costing up to 50M euros.

- Merkel call for secure EU network.   Central to our competitiveness, single digital market, strengthen security of services, <u>no to data protectionism </u>and <u>yes to data protection</u>. We want to use big data.

- <u>Trust is key</u>. Weak link is the whole network, weak directive will let us down.

- Cyber security strategy is providing the right building blocks. Strong cyber security domain is important to Europe. Without it, democracy would fail to manage technology. <u>Make EU the safest place for digital</u>.

MAPPING
Managing Alternatives for Privacy,
Property and Internet Governance

EUROPOL Public Information

EUROPOL

THREAT ASSESSMENT
(ABRIDGED)

INTERNET FACILITATED
ORGANISED CRIME

iOCTA

O2 – Analysis & Knowledge
The Hague, 07/01/11
FILE NO.: 2530-264

ID Fraud = a top EU crime enabler
McAfee: $1 trillion/year cybercrime (rising $2 trl)

UK fraud > £73bn
EU fraud > €500bn

If we are not winning, we must be losing

MAPPING

Managing Alternatives for Privacy,
Property and Internet Governance

- More users
- More devices – internet of things…
- More mobile
- More cloud(s?)
- More BYO Disaster
- More sensitivity – my info, health
- More critical systems – smart metering, big data
- Weak cyber borders >> internet governance under strain
- Increasing expectations and temptations → unwise decisions

- UK – 50M smart meters by 2020 in 30M buildings (HMG)
- 76% of financially active organisations in UK are <u>not registered</u> in UK or at all (& can't tell the difference). (HMG)
- 65% of IP theft is by insiders (SANS)
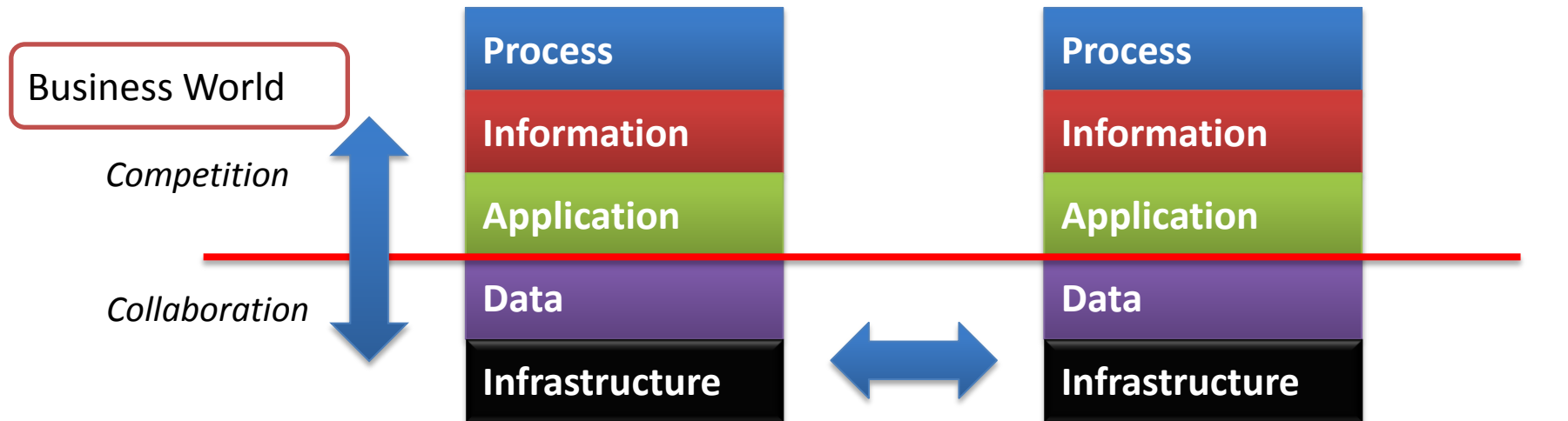- Organised crime expanding online - UK Operation FALCON

Just **Surface Web**
….add
Deep web
Dark Web

Reactions

- **More regulations and directives**
  - EU eID Authentication (digital) Signature (eIDAS) (now)
  - EU Cybersecurity Framework <> NATO CDAP
    - EU Network Information Security Directive (mid 2015)
      - banks, energy, transport, health (telco)
      - Information sharing, incident notification, collaborative risk management
    - EU Network Information Security Platform
  - US Exec Order 13636 – Cybersecurity Framework
  - US Pres Policy Directive 21 – Information Sharing
  - UK Cyber Essentials mandated for HMG suppliers
- **More surveillance concerns**
- **More privacy pressures**
- **More disruption – cryptocurrencies, hawala**
- **More pressures on Internet governance**
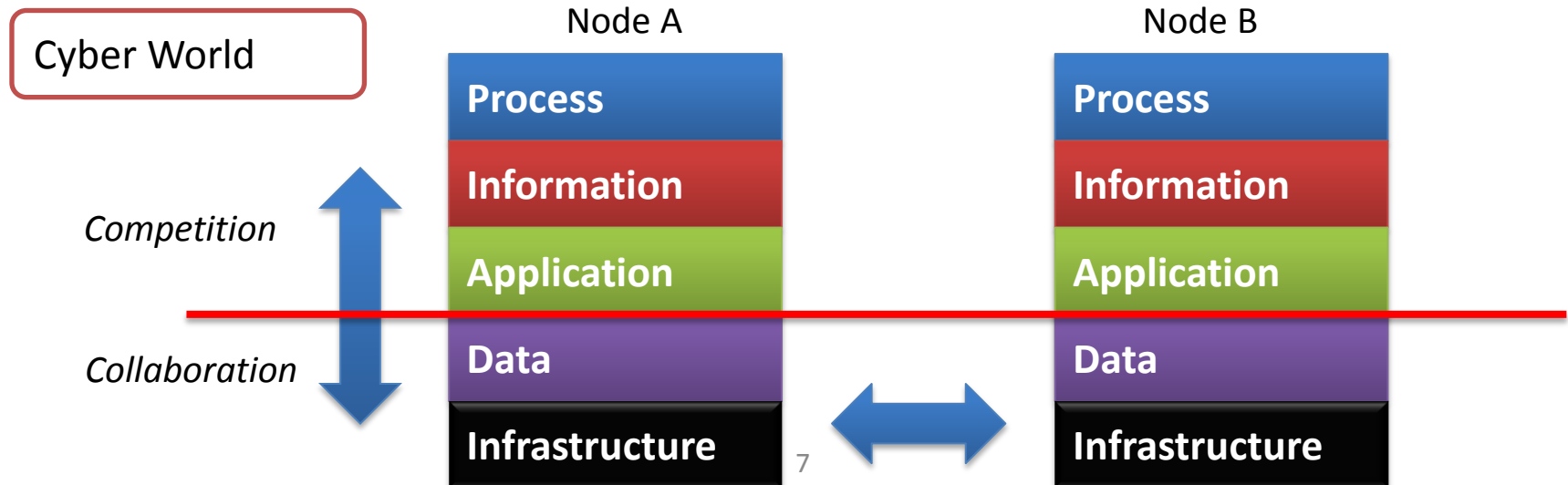- **More demand for collaborative trust <u>between parties</u>**

Highlights - Big Picture "Building the Wall"

Collaborative Crisis Management

Incident management

Counter-fraud

Collaborative Cyber SA

EU NISD NIS Platform

Incident Notification

Risk Transfer

Cyber insurance models

Managed risk

Risk Assessment

Risk Treatment

Risk Mitigation

International Standards – ISO, EU

Assessment tools

Approved assessors

Cyber controls frameworks

Assurance Schemes

Federated ID & Access management

Red team/ serious games

MACCSA is enabling in every area plus development of:
- New capabilities
- New data sources and registers

CCSA & Incident Management

Highlights - Big Picture
"Building the Wall"
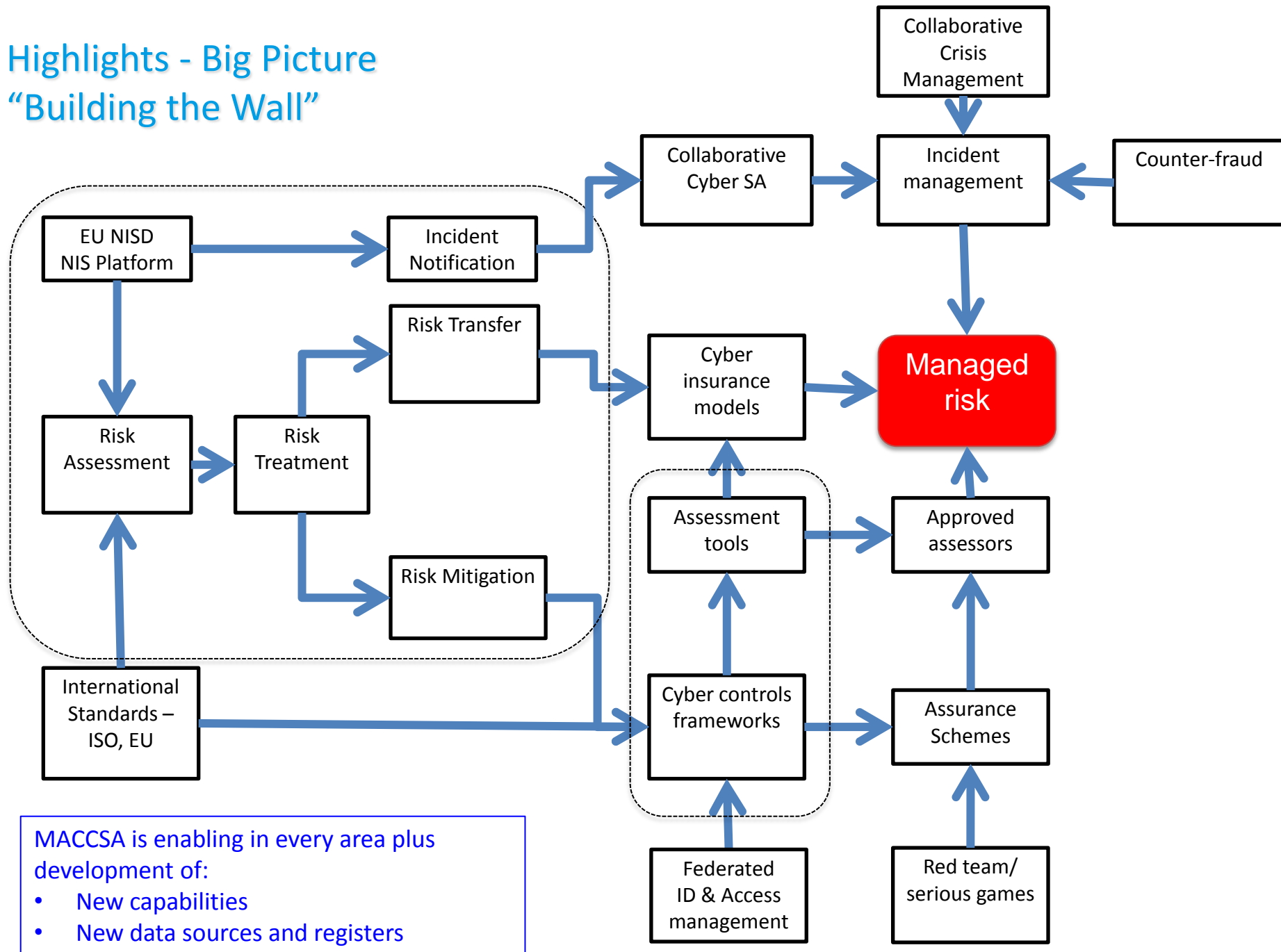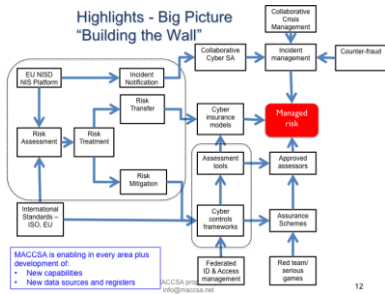
1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Intel led
Layered proactive defence
Rumsfeld-based

Collaborative Crisis Management

Collaborative Cyber SA Hubs & Nodes → Incident management ← Counter-fraud

Federated ID & access management

Cyber controls frameworks

Taxonomies & Automation

Triage & Analysis Processes

Priority Info Requirements

Red team/ serious games

ROLO OrgID registers

PANCRAS Defeat fake docs and products

Others