PICASSO Project

Towards new avenues in EU-US ICT collaboration

Policy Briefing on ICT Security issues affecting EU-US ICT development collaboration

Second Webinar of the PICASSO Policy Expert group

16 May 2017, 15:00 UTC

ICT Policy, Research and Innovation for a Smart Society

www.picasso-project.eu

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

Cybersecurity and its impact on EU-US ICT collaboration

Agenda – Tuesday, May 16, 2016 – 15:00 a.m. – 16:30 p.m. (UTC)

- **PICASSO Welcome and purpose of the call**
  Maarten Botterman, PICASSO Policy Expert Group Chairman
- **Introduction to EU-US Cybersecurity technology issues relating to ICT development**
  Dr. David Farber, Carnegie Mellon University, IEEE fellow, ACM fellow
- **Introduction to EU-US Cybersecurity policy issues relating to ICT development**
  Dr. Jonathan Cave, GNKS Consult and University of Warwick

  Participatory discussion: current status and expected development in EU and US

- **Three domains focus - 5G, Big Data, IoT/CPS**
  Yaning Zou, Project Manager of PICASSO 5G Networks Expert Group
  Dr. Nikos Sarris, Chairman of the PICASSO Big Data Expert Group
  Christian Sonntag, Project Manager of PICASSO IoT/CPS Expert Group Manager

  Introduction and Participatory discussion: Focus per domain on cybersecurity issues and its affections to EU-US collaboration

- **Preliminary conclusions (Briefing Document validation)**

Project in brief

> **Coordination and Support Action**, funded by the European Commission/DG CONNECT

> **Duration:** January 1, 2016 - June 30, 2018

> **Target groups:** industry, government and civil society actors involved with ICT research and innovation development and policy

> **Target regions:** European Union, United States of America

> **Key Message:** ICT research and innovation (R&I) collaboration between the EU and the US can help it to reflect socioeconomic and technological realities and to improve the contributions of ICT development and policy to enhancing economic growth and reconciling industrial needs with societal objectives.

PICASSO
EU-US ICT collaboration

PICASSO priorities at the heart of EU policy orientations

"On its Strategy to create a Digital Single Market and digitise European industry, the European Commission focuses on accelerate standard setting and related enabling technologies, such as 5G, cloud computing, internet of things, data technologies and cybersecurity."

Andrus Ansip , Vice-President EC for Digital Single Market
Günther Oettinger, Commissioner for Digital Economy and Society

PICASSO focusses on synergies between ICT *policies* and ICT *technologies* to:

> reinforce EU-US collaboration in pre-competitive ICT R&I in key enabling technologies with the greatest promise in meeting societal challenges: **5G Networks, Big Data and Internet of Things (focus on Cyber Physical Systems)**

> support EU-US ICT policy dialogue by creating a forum for discussion and contributing to policy debate regarding **privacy, security, internet governance, interoperability and ethics**.

PICASSO EU-US ICT collaboration

Expert Groups

Synergies between policy and technology groups

3 Technology Groups
Strategic ICT Technology areas linked to Societal Challenges

5G Networks

Big Data

IoT/CPS

1 Horizontal Group
On ICT Policy linked to key ICT technology areas

Policy issues:
Privacy and data protection | Security | Standards and Interoperability | Ethics …

+25 Experts in total across all groups

PICASSO EU-US ICT collaboration

EU – US Cybersecurity and its impact on EU-US ICT collaboration: fundamental approaches and developments

Scoping the issue

Maarten Botterman
Chairman of PICASSO ICT Policy Expert Group

ICT Policy, Research and Innovation for a Smart Society

www.picasso-project.eu

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

2017 (today!) WannaCry

2016 Dyn Cyberattack

PICASSO
EU-US ICT collaboration

2016 Data breach Yahoo

ICT Security is high on the agenda

- Growing incidence of adverse and highly-publicised events
  - Massive distributed denial of service attacks on the Internet,
  - Malware, hacking, and unauthorized penetration of critical services and sensitive data
  - Ransomware, phising, etc.
- No magic cure – and every “cure” sets the stage for next sset of issues
- Challenges are global
- Require acting in every step of the value chain, by all stakeholders:
  - ICT designers and developers
  - Businesses
  - Governments
  - End users

Agenda webinar

- PICASSO Welcome and purpose of the call
  - Maarten Botterman, PICASSO Policy Expert Group Chairman
- Introduction to EU-US Cybersecurity technology issues relating to ICT development
  - Dr. David Farber, Carnegie Mellon University, IEEE & ACM fellow
- Introduction to EU-US Cybersecurity policy issues relating to ICT development
  - Dr. Jonathan Cave, GNKS Consult and University of Warwick
- Three domains focus - 5G, Big Data, IoT/CPS
  - Dr. Gerhard Fettweis, PICASSO 5G Networks Expert Group
  - Dr. Nikos Sarris, PICASSO Big Data Expert
  - Dr. Christian Sonntag, PICASSO IoT/CPS Expert Group

PICASSO EU-US ICT collaboration

Introduction to EU-US Cybersecurity technology issues relating to ICT development

Dr David Farber

ICT Policy, Research and Innovation for a Smart Society

www.picasso-project.eu

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

Technical situation today

- Enormous increase in power and distribution of computing environment
- Vulnerable environment:
  - Operating system monoculture and consequent application ecosystems are so large that targeting became attractive;
  - Interdependency and complexity of internet components. (Bad) code remains in use for a long time.
  - Over-the-net software maintenance and patching, and new ways of offering products and services have created an global environment that is vulnerable;
  - Massive distribution of IoT devices often based on old and sometimes defective software, sometimes remaining in use beyond due date

Technical situation today

- Improved technology and softaware capability, introduction of Software Defined Networking and Information Ce3ntric Networking;
- Largely same communication infrastructures;
- Many old devices and software remaining

- *New measures and improved ways are available, and it is not clear yet who is willing to pay for this*

Introduction to EU-US Cybersecurity policy issues relating to ICT development

Dr. Jonathan Cave

ICT Policy, Research and Innovation for a Smart Society

www.picasso-project.eu

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

Starting points

- Policy-makers bear responsibility for cybersecurity risks, which they struggle to understand, let alone anticipate or control;
- CS risk cannot be minimized and trust cannot be maximised
- Trust and security are both real and imagined
- Some illustrative examples
  - Definitional issues
  - Identification vs. authentication
  - Data and data processing integrity and quality
  - Cybercrime vs. cyber-enhanced crime (what is a crime?)
  - Encryption
  - Balancing CS: CNIs, innovation, growth, national security, etc.
  - International perspectives – conflict of interests, jurisdictions.

PICASSO EU-US ICT collaboration

Some policy developments

- Definitions –
  - ICT security rests on data and processing;
  - Obvious insecurity of underpinning elements (fake news and compromised algorithms, resp.) produces much more widespread and consequential insecurities.
  - Policy and rules can only do so much in the face of human behaviour
  - Relation between laws etc. and the Internet are still skewed
  - Traditional, resilient 'security' powers and thinking may be unhelpful
- Identification vs. authentication
  - Verification makes it possible to hold people responsible, but it may not be useful
  - Liability-shifting; 'too strong' ID, displacement
  - Security sensitivity based on people, technology, information, service/purpose, context
  - No general agreement on universal ID – why not? (*Quis custodiet…*)
  - No obvious quick fix:
    - Individuals are identified online by IP, MAC IMEI numbers, etc. not by anything personal;
    - Biometrics are ambiguous;
    - Other forms of personal identity (esp. passwords) are unwieldy and increasingly insecure; and
    - •Multiple enrolment is a classic, and simple, way to defeat even strong identification systems.

More examples

- Data and processing integrity and quality
  - Audit and data ownership (authentic sources) vs. distributed ledgers
  - Crypto currencies; Japanese, etc. laws; US/UK national alternatives
- Cybercrime
  - EU: Framework, ePrivacy, Child exploitation, national measures, Data Retention, IP (UK), GDPR, NIS Directive - European Cybercrime Centre
  - US: various 'computer crime' enhancements, much litigation. Cybersecurity Executive Order
  - Mainly focussed on legislating to prevent new, specifically cyber, crimes (including new categories linked to specific technological domains)
  - Will have to adapt to how new technologies change law enforcement:
    - ★ facilitating existing crimes (e.g. fraud, theft, tax evasion, money laundering, perverting the course of justice),
    - ★ making it harder or easier to collect and analyse evidence
    - ★ providing payment and transaction services to criminal enterprises.

ICT Security and 5G; Big Data; and IoT/CPS?

What can we do, as stakeholders, to make collaboration easier and more attractive?

ICT Policy, Research and Innovation for a Smart Society

www.picasso-project.eu

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

5G: key developments and relation with Cybersecurity

Yaning Zou
Manager of PICASSO 5G Networks Expert Group

ICT Policy, Research and Innovation for a Smart Society

www.picasso-project.eu

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

What is 5G?

- A key enabler for the networked society 2020
- More than just a radio access network
  - Integration of cross-domain networks
- KPIs
  - Throughput
  - Coverage
  - Number of connections
  - Latency
  - Reliability
  - Mobility

- Vertical industries
  - Automotive and transportation
  - Industry automation
  - eHealth
  - Energy

- Intensive R&I activities
  - Technology components
  - Testbeds and trials
  - Spectrum allocations
  - Standardizations

PICASSO EU-US ICT collaboration

Security related challenges in 5G: past and future

- From 2G to 4G, the mobile network is relatively safe.
  - The main function is for data/voice transmission.
  - Each user/device is identified with a SIM card
  - Basic connectivity service: one user and two operators (one home and one roaming)
- 5G security challenge: device-level
  - An unprecedented number of devices will be connected.
  - A very wide range of devices will be connected.
    - ★Smart phone, IoT node, sensor,…..
    - ★Low-cost device might endanger network as a whole
  - More than basic connectivity service
    - ★E.g., machine control, car-to-car communications
    - ★Different connectivity/KPI requirements
    - ★Different security solutions

PICASSO EU-US ICT collaboration

Security related challenges in 5G

- 5G security challenge: network-level
  - A wide range of vertical industries implies diverse security requirements.
    - ★ Different connectivity and application requirements
    - ★ Different security solutions
    - ★ Multiple operators from different domains
    - ★ Critical infrastructures, e.g., power grid, require very high protection.
  - The trend of software and hardware isolation requires special attention on security issues
    - ★ E.g., network function virtualization (NFV)
    - ★ Multiple operators work on the same entities.
    - ★ Security across multiple virtualized domains.

Security related challenges in 5G

- 5G security challenge: general privacy and data management
  - New identity management approaches are required.
    - ★ Different users: human, machines, cars…
  - New data management approaches are required.
    - ★ Who will own the data?
    - ★ Who can see the data?
- 5G security challenge: cost and energy
  - The cost and energy consumption should be taken into account in the design for building viable 5G business.
- Potential 5G security threat
  - The highly connected 5G vision could rise much higher interests of cyber attack as higher gain can be obtained.

What solutions 5G can offer?

- Network slicing
  - It allows multiple logical networks to be created on top of a common shared physical infrastructure.
  - It enables differentiated and flexible security services .
    - ★ Each logical networks can be associated with different security requirements/characteristics.
    - ★ Each vertical industry can be associated with one or multiple logical networks.
    - ★ Security can be built as value-added services.
  - It provides isolations between different logical networks.
    - ★ The interactions of different logical networks can be designed based on the required security levels.
    - ★ E.g., critical infrastructures must be isolated from others.

Perspectives on 5G security

- To ensure the success of 5G network and the envisioned network society
  - intensive R&I activities should be done in both
    - ★ Policy domain
    - ★ Technology domain.
  - It might be more sensible to apply a top-down approach.
  - It invites innovations on new security architectures and concepts.
  - EU-US collaboration is essential for the 5G global success.

Cybersecurity: Policy Challenges for the Big Data

Dr. Nikos Sarris

Chairman of PICASSO Big Data Expert Group

ICT Policy, Research and Innovation for a Smart Society

www.picasso-project.eu

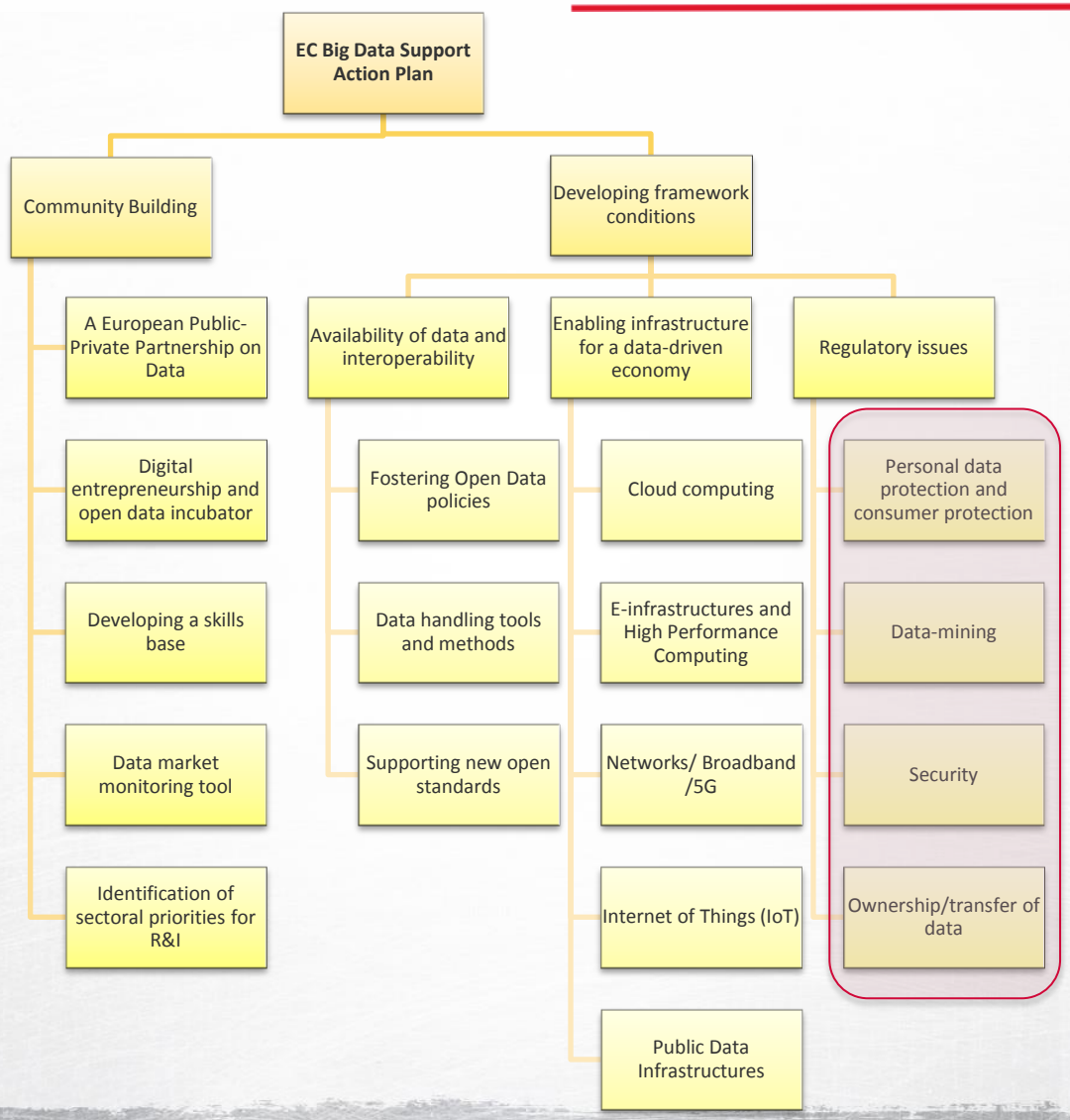
PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

Cybersecurity is critical in many aspects to Big Data

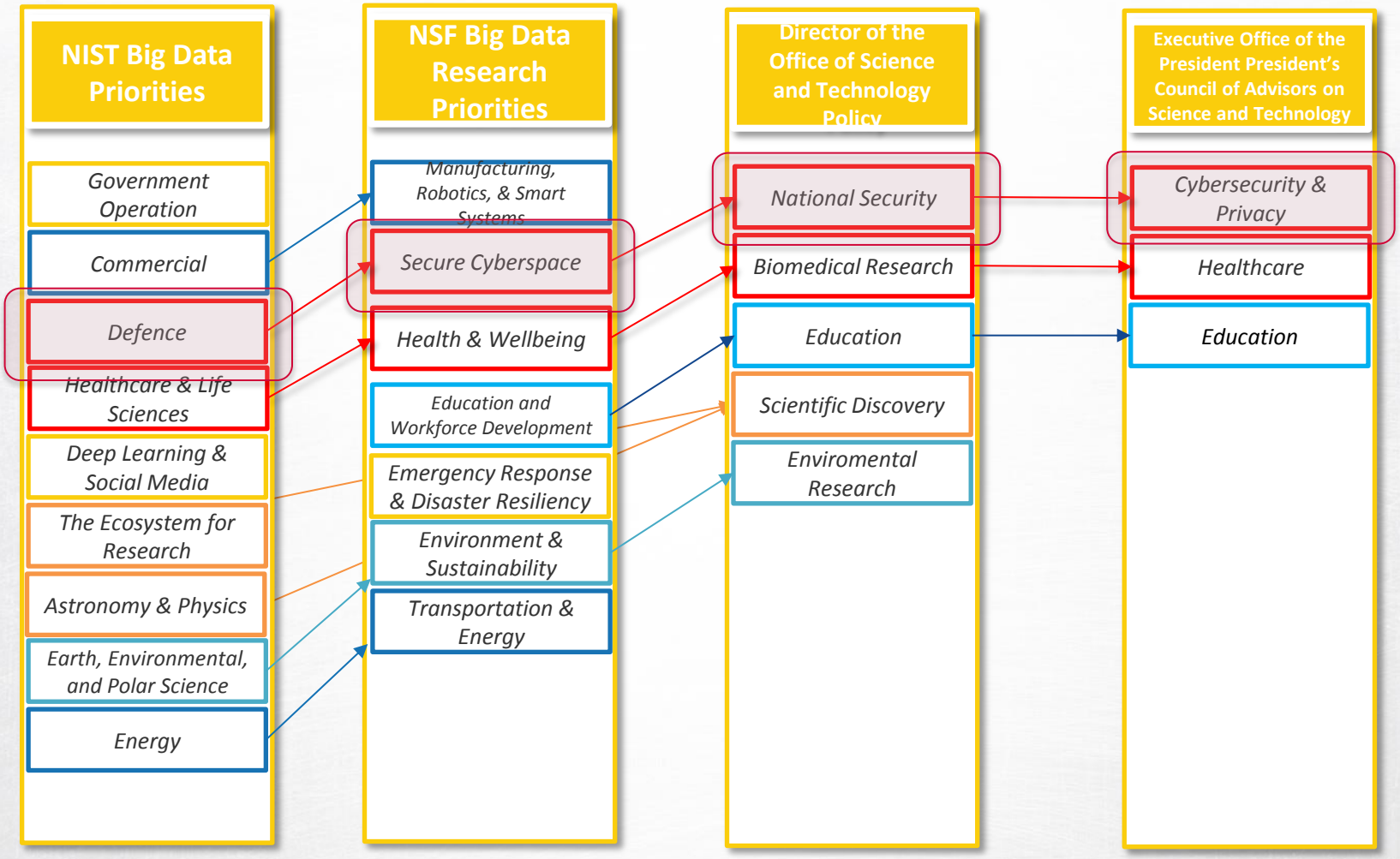
- **'Data is the new oil'**: As 'Data' is the main element of systems and applications if data security is not ensured the integrity of the entire Big Data industry is jeopardised.
- **Big data : large responsibility : huge security problems**
- **Secure data** means that
  - ***Data born in the applications*** should be protected by unauthorised access
    - ★ Should be visible only to authorised users and processes
    - ★ Should be editable only by authorised users and processes
  - ***External data used by applications*** should be trustworthy
    - ★ Data sources must ensure the integrity of provided data
    - ★ Data transfer must ensure no manipulation, eavesdropping or other interception
- The importance of the problem is acknowledged both in the EU and US [PICASSO opportunity report]

PICASSO EU-US ICT collaboration

EU Big Data Strategy

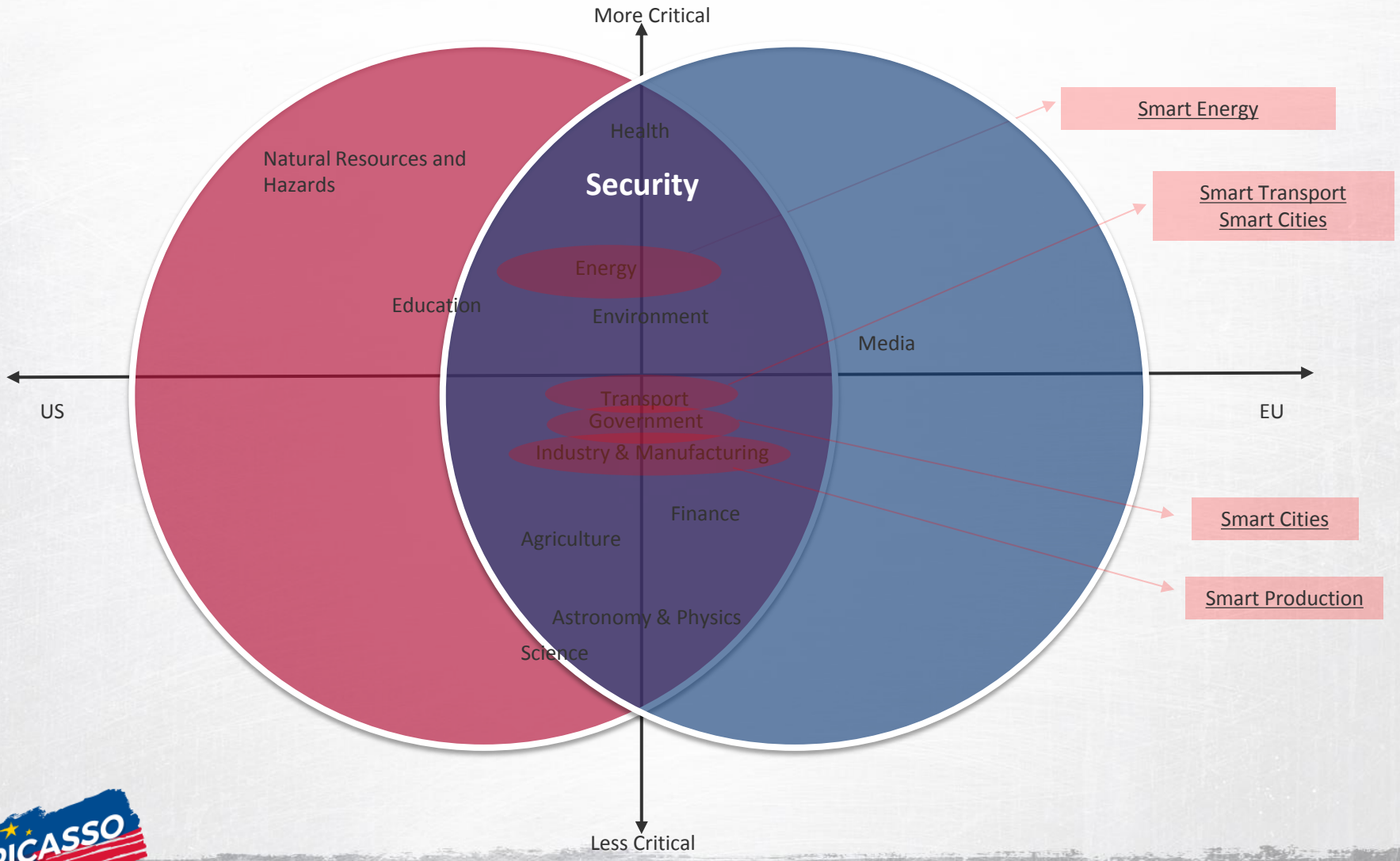


US Big Data Priorities



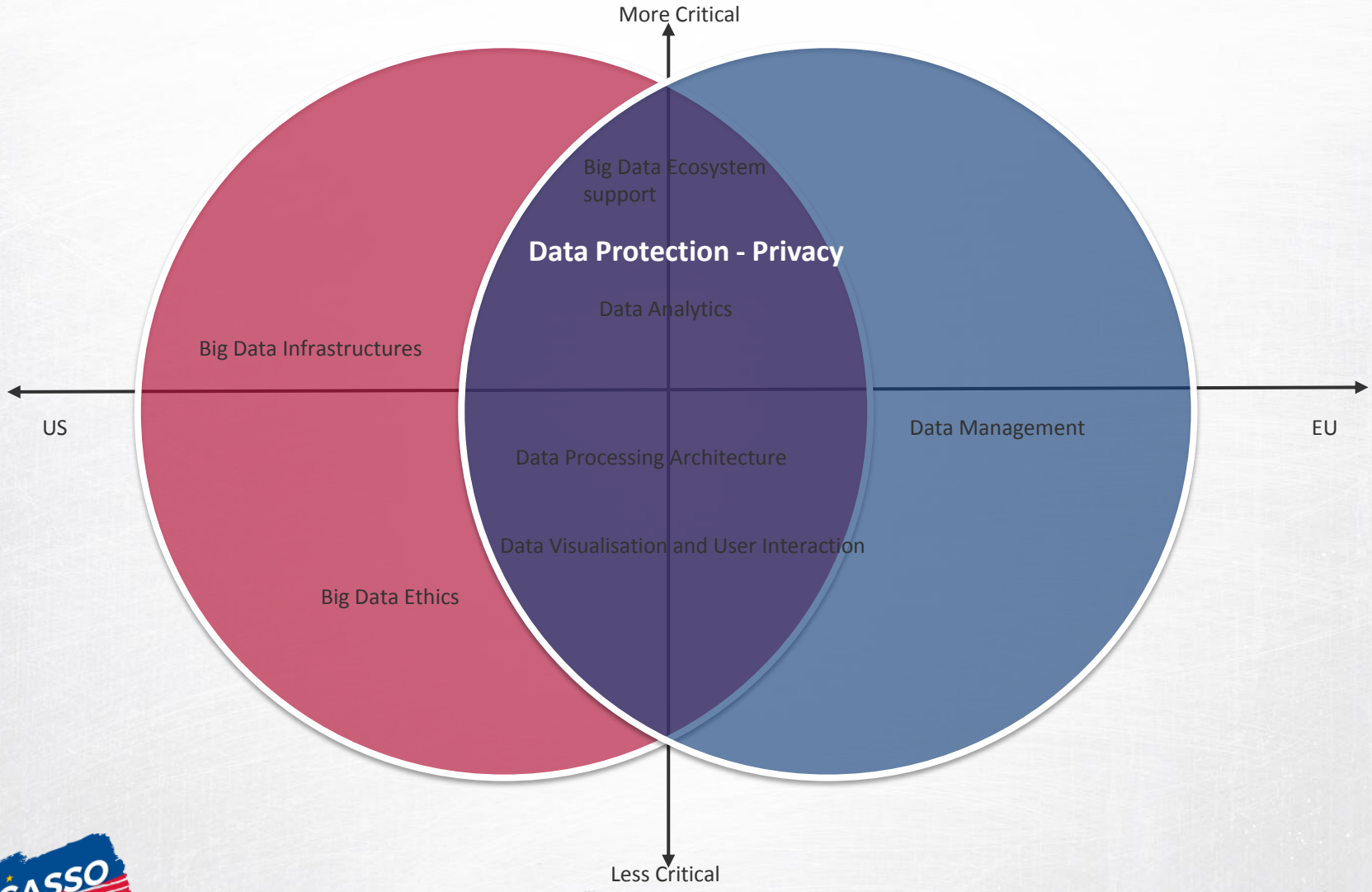
PICASSO
EU-US ICT collaboration

EU-US Common Big Data Priorities



PICASSO
EU-US ICT collaboration

EU-US Common Big Data Application Sectors



PICASSO
EU-US ICT collaboration

Cybersecurity: Policy Challenges for the Internet of Things (IoT) and Cyber-physical Systems (CPS)

Christian Sonntag

Manager of PICASSO IoT/CPS Expert Group

ICT Policy, Research and Innovation for a Smart Society

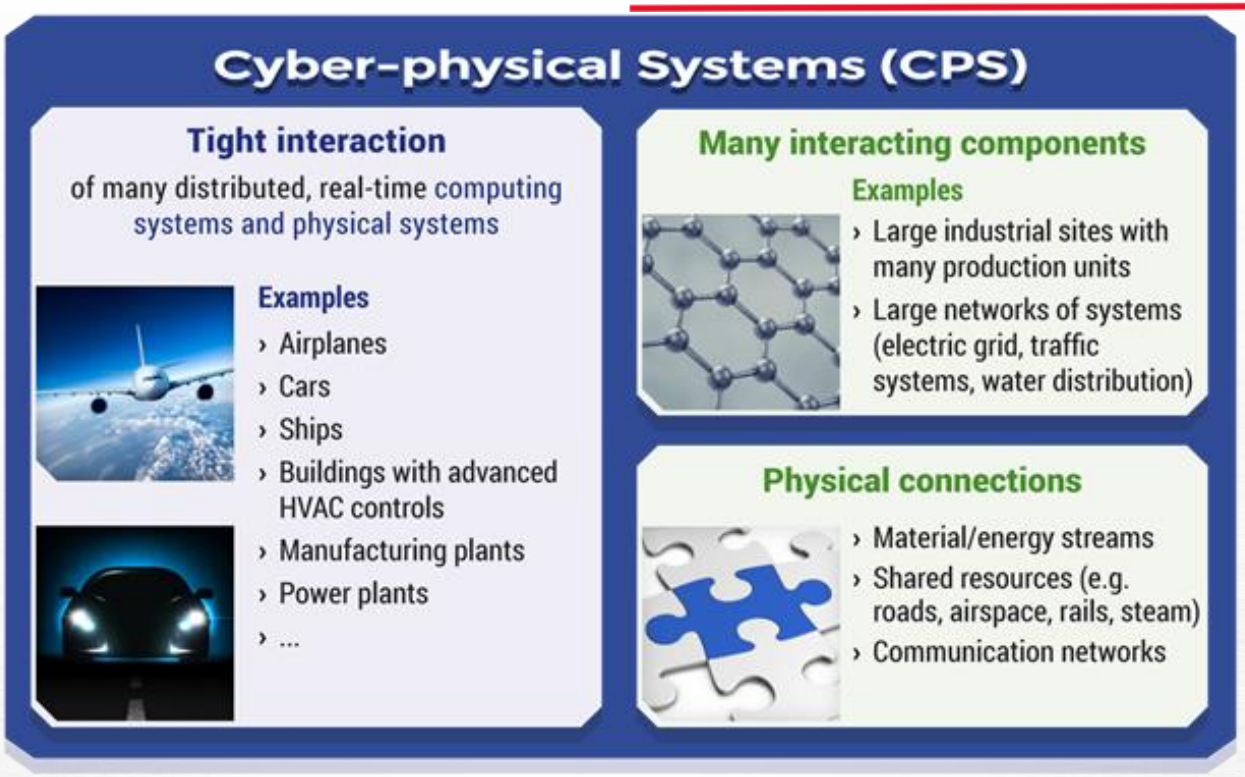
www.picasso-project.eu

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

The Internet of Things (IoT)

- **The Internet of Things (IoT)** – A paradigm based on the convergence of:
  - Low-cost sensing and computation
  - Ubiquitous connectivity and mobile apps
  - Cloud analytics and big data
- IoT annual global economic potential: Between **$1.4 trillion** to **$14.4 trillion** by 2020
- IoT initiatives, alliances, and clusters
  - **US:** Several alliances with international membership (e.g. **Industrial Internet Consortium**)
  - **European IoT Research and Innovation Cluster** with over 40 European projects
  - **Alliance for Internet of Things Innovation (AIOTI**)

Cyber-physical Systems (CPS)



- **An area of European strength**
  - € 410 billion market
  - 4 million jobs worldwide, of which one quarter are in Europe

PICASSO EU-US ICT collaboration

Convergence of IoT and CPS: IoT-enabled CPS

- **Focus of current research and development in IoT**
  - Low-cost sensors / computing, connectivity, middleware → **enormous amounts of data can be collected**
- **How to make use of the data is often not clear**
  - What benefits can be gained from the data
  - **Challenge: From sensing to actuation, closing the loop**

→ **IoT is an enabling technology for CPS**

- **Cyber-physical systems are often embedded in large systems consisting of many coupled components with partial autonomy**
  → **Cyber-physical Systems of Systems (CPSoS)**

See also www.cpsos.eu

  - E.g. power grids, oil and gas pipelines, commercial buildings, transportation systems, production sites, and other complex, critical infrastructures

Importance of Cybersecurity in IoT-enabled CPS

- **Physical connections: Security breaches may have drastic physical, financial, and human consequences**
  - Large-scale power outages; chemical spills; road, air, and rail traffic congestion and accidents; malfunctioning medical devices; suppression of emergency responses; …
  - Cyber attacks can mask/exacerbate physical attacks and vice versa
- **Large-scale systems → Numerous points of vulnerability**
  - Sensors, communication networks, data repositories, analytics engines, actuation devices, human-in-the-loop interfaces, …
  - Overall security depends on the “weakest link”, badly secured systems may have adverse effects on public cyber infrastructure (e.g. DDoS attacks)

→ Cybersecurity & trust/trustworthiness of technical systems are dominant topics for IoT and CPS in the US and the EU

★ Importance is expected to grow over the next years

Some Policy Challenges in IoT-enabled CPS

- **Many IoT-enabled CPS cross national boundaries**
  - Policy, legal, and jurisdiction issues, need for policy alignments regarding data access, cybersecurity regulations, and privacy
- **IoT-enabled CPS are multi-stakeholder systems (companies, suppliers, operators, …)**
  - Separation of data, data ownership, liability in case of attacks, tracing and combatting attacks across multi-stakeholder systems and networks
- **Innovation pressure and legacy system integration**
  - Systems connected as an “afterthought”
  - Time-to-market of new devices more important than reliability / security
  - Frameworks for security certification (e.g. “trusted IoT”)
- **Cybersecurity and privacy are sensitive topics, collaboration may be difficult to set up**

Preliminary conclusions

- Confirming the importance of ICT security

  Security of ICT devices, data and services are broadly seen as a top priority and a concern that needs to be addressed. Without appropriate security in ICT, trust in use of the products and services that are based on ICT erodes and this reduces the opportunities to reap the benefits.

- Two roads ahead:
  1. Make the most out of we have today and increase security by improvements in technologies and services, and in awareness and training;
  2. System-wide redesign of the ICT and communications infrastructure.

PICASSO EU-US ICT collaboration

Operational conclusions

- Need for a security taxonomy for development of ICT based technologies and services;
- Cloud and mesh networking are here to stay and put new requirements for security functions to be along the chain;
- Outdated security models need to adapt to become automated, distributed, context aware and real time. Focus needs to move towards:
  - Secure access management;
  - Self-protection;
  - Privacy controls;
  - Embedded security.
- Move towards biologically inspired security
- Move towards proactive protection

PICASSO EU-US ICT collaboration

PICASSO News

Trans-Atlantic Symposium on ICT Technology and Policy
5G Networks, Big Data, Internet of Things and Cyber Physical Systems for a smart society

Date: June 19-20, 2017
Venue: Minneapolis, Minnesota, USA
Host: Technological Leadership Institute

For more information and registration:
www.picasso-project.eu

PICASSO EU-US ICT collaboration

PICASSO EU-US ICT collaboration
CROSSROADS
Your EU-US ICT info-hub

Download on the App Store
GET IT ON Google Play

PICASSO CROSSROADS

Free of charge and continuously updated, CROSSROADS will provide :

- Access the EU-US ICT projects and networks databases
- Find out more about EU and US programmes facilitating ICT collaboration
- Discover information on existing collaborative initiatives
- Learn about ICT open calls in the EU and the US
- And much more ...

Don't wait any longer and try CROSSROADS - your information hub on EU-US ICT collaboration.

Consortium

Coordinator
inno TSD, France

Technische Universitat Dortmind (TUDO), Germany

THHINK Wireless Technologies Limited (THHINK), United Kingdom

Athens Technology Center (ATC), Greece

Agency for the Promotion of the European Research (APRE), Italy

Honeywell International INC (HON), United States

GNKS Consult BV, (GNKS), The Netherlands

Technische Universitaet Dresden (TUD), Germany

Florida International University, (FIU), United States

Regents of Univeresity of Minnesota, (TLI), United States

Contacts

Policy Expert Group Chairman: **Maarten Botterman,** GNKS Consult BV
maarten@gnksconsult.com

Project Coordinator: **Svetlana Klessova,** inno TSD, France
s.klessova@inno-group.com

More on Picasso

www.picasso-project.eu

@picasso_ICT

PICASSO – EU/US ICT research, innovation and policy collaboration