CYBER ROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

European Commission
Seventh Framework Programme

Hitting the CyberROAD: what to expect in cyber crime by 2020

http://cyberroad-project.eu

Davide Ariu
University of Cagliari, Italy

EECTF Plenary Meeting – March 31, 2015

An Open, Safe and Secure Cyberspace

- **EU Strategic Priorities and Actions***
  - **Achieving Cyber Resilience**
  - **Drastically Reducing Cybercrime**
  - Develop cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
  - Develop the industrial and technological resources for cybersecurity
  - Establish a coherent international cyberspace for the EU and promote core EU values

*Cybersecurity Strategy of the European Union - 2013

FP7 SEC-2013.2.5-1

- **Developing a Cyber crime and cyber terrorism research agenda – Coordination and Support Action (Coordinating Action)**

- **Development of a research agenda which provides concrete answers to the following issues:**
  - In what **categories** can we subdivide **Cyber Crime** and **Cyber Terrorism**?
  - What are the **major research gaps**?
  - What are the **challenges** that must be addressed?
  - What **approaches** might be desirable?
  - What **needs** to be in place for **test** and **evaluation**?
  - To what extent can we **test real solutions**?

The CyberROAD Project

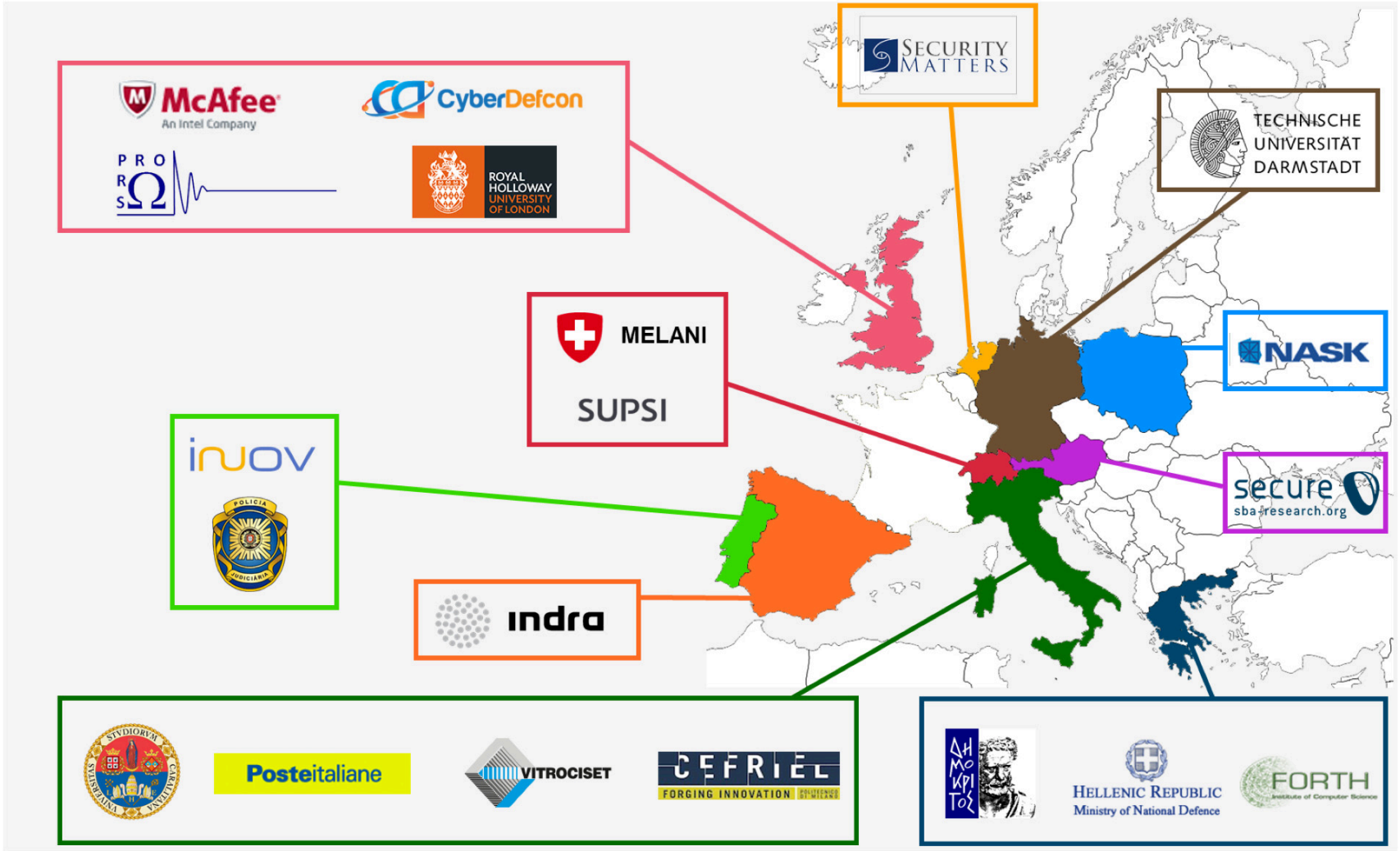
Development of the **Cyber** Crime and **Cyber** Terrorism Research **ROAD**map

- **CyberROAD has started in June 1st 2014 and will end May 31st, 2016**

COURAGE CYBERCRIME AND CYBERTERRORISM EUROPEAN RESEARCH AGENDA

CAMINO

The CyberROAD Consortium



Why to Roadmap?

- **Roadmapping techniques can be used to support strategic & long-range planning***
  - Technology roadmapping is widely used especially by the companies for exploring and communicating the relationships between evolving and developing markets, products, and technologies over time.
  - Can be also used by governments to plan the achievement of mid and long term goals
    - After World War II, the US Department of Defense was faced with the task of deciding what projects should be funded for the development of new weapons systems.
  - It can in general help making challenging decisions in turbulent environments

- **Data sources:**
  - Experts in the domain of interest
    - Generally provide their views on the future in terms of "Future Scenarios"
  - Stakeholders
    - Usually express their needs
  - Empirical Data
    - Provide concrete evidence regarding the problem at hand
  - Scientific Literature

*Robert Phaal et. Al., *Technology roadmapping – A planning framework for evolution and revolution*, 2003

Why to Roadmap?

- **Was in 2007-2008 (when Apple marketed the iPhone and Google released Android) possible to foresee the current scenario of Mobile (in)Security?**

Technical facts

- **(relatively) High Computational Power**
  - Moore's Law known since '60s
- **Always-on connectivity**
  - 1st generation iPhone soon replaced (in 2008) by the 3G version

Economical facts

- **Huge size of the Mobile market, even before the Smartphone era**
  - E.g. Since 2004 in Italy we have more mobile devices than citizens
  - Quickly enlarging markets

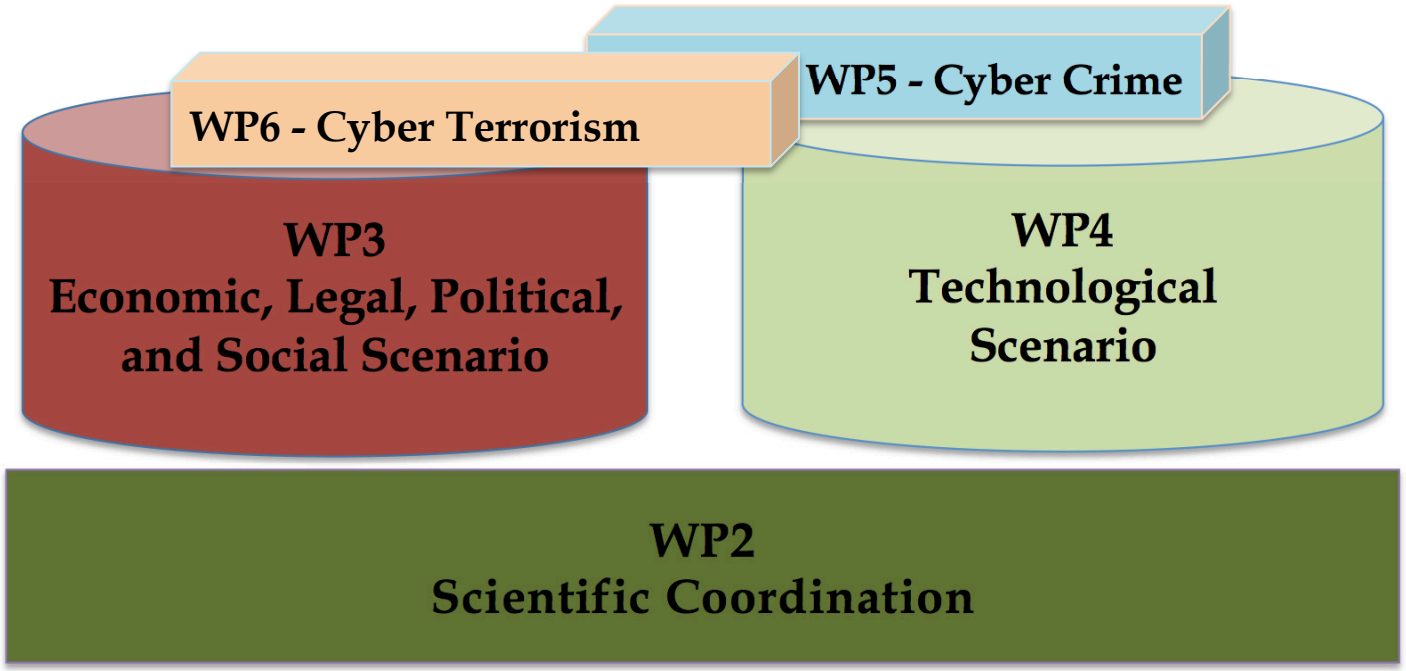
- **Pressure from the Internet Providers**

amazon Google ebay

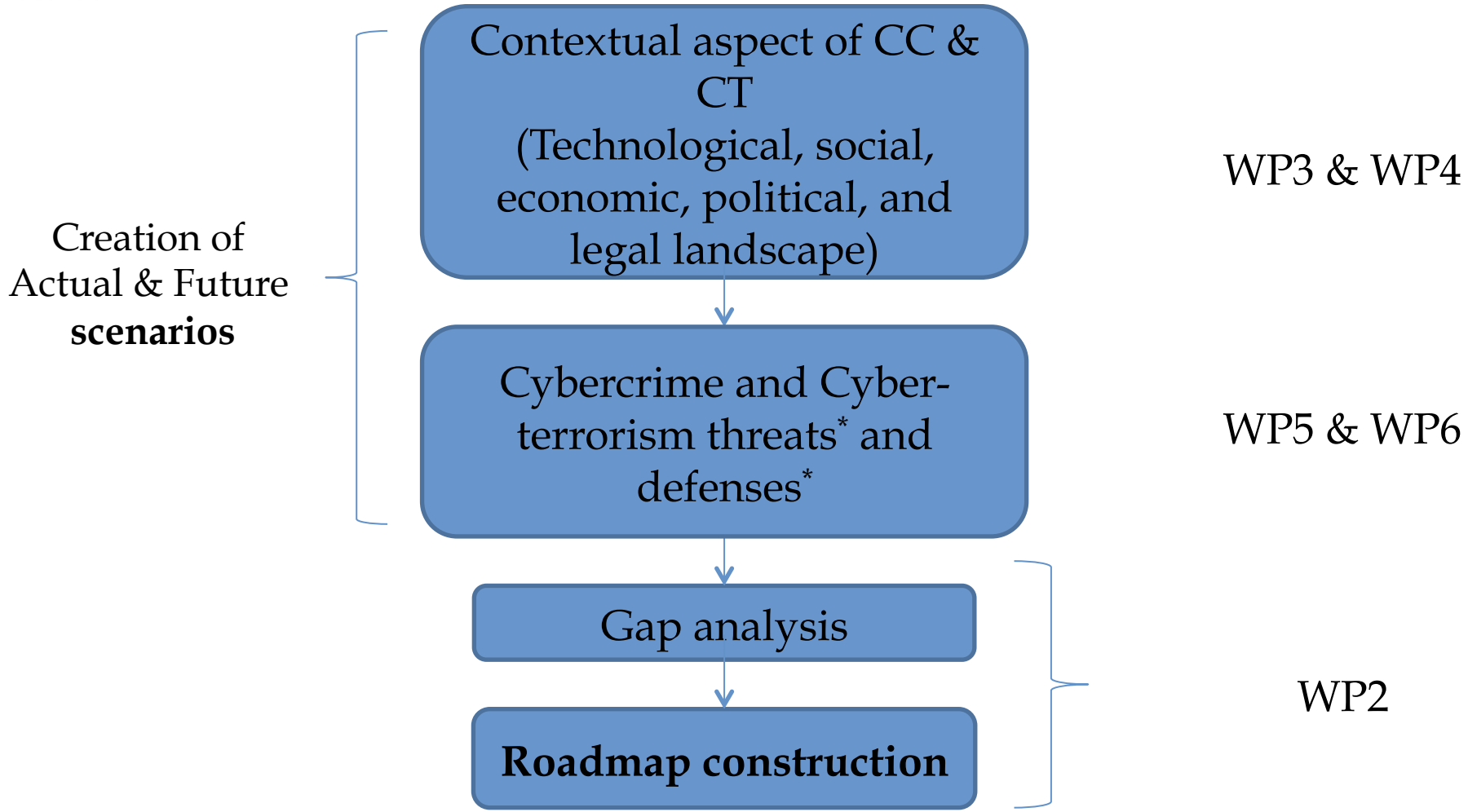
Experience from past cyber-attacks

- **Platforms with many users are strongly appealing**
- **Always connected devices are more exposed**

The CyberROAD Approach



Main steps of CyberROAD roadmapping



*In the context of the CyberROAD roadmapping methodology, the words "threat" & "defense" are used with a meaning different from the one they typically have in Computer Security

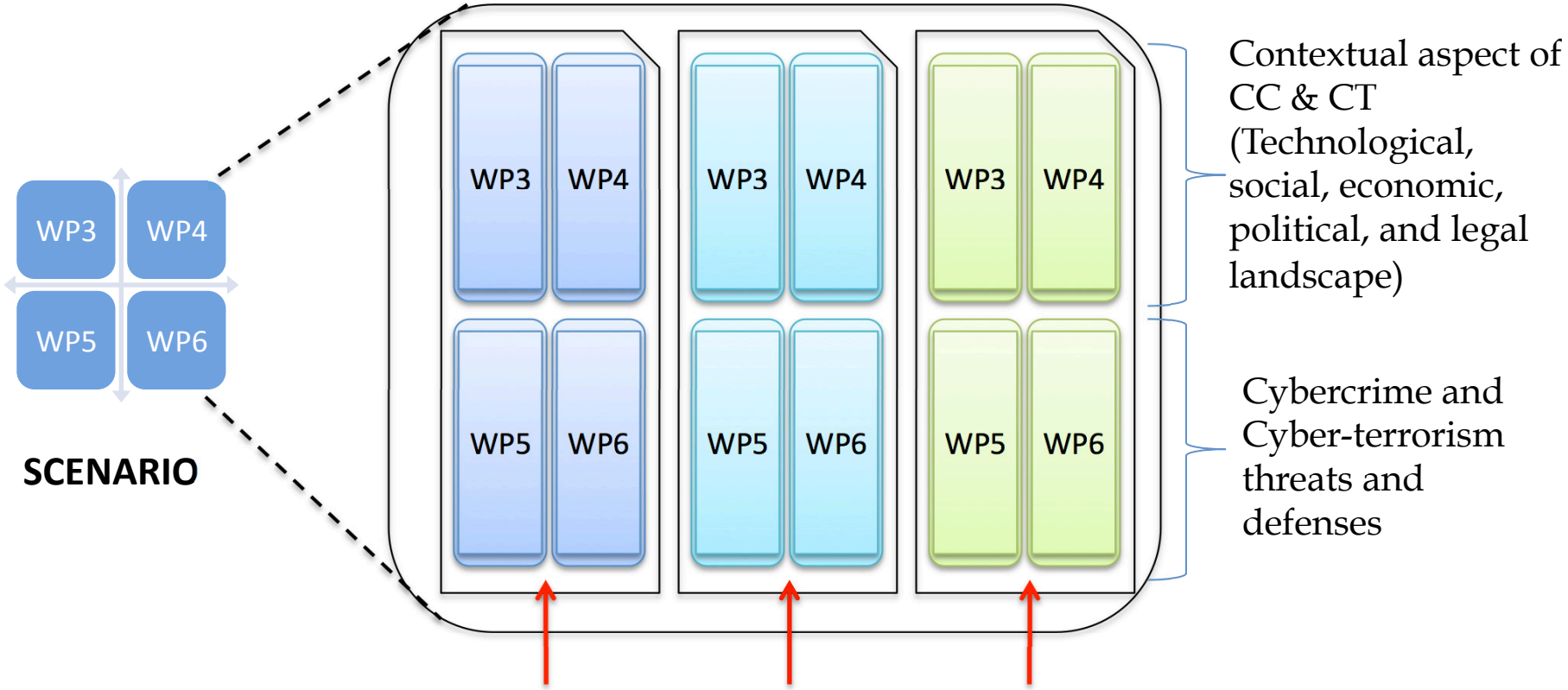
CyberROAD Threats & Defences

- **THREATH**
  - any circumstance or event, not necessarily related to technology, with the potential to adversely impact either an Information System or the society or group of people which makes use of and benefits from the services offered by that system.
  - It is also considered a threat whatever circumstance or condition makes it difficult to properly defend a system or to carry out the forensic activities aimed to investigate the event, to identify responsibles, and/or eventually to prosecute them.
    - **E.g.** A gap in the legal framework or the absence of a sovra-national authority for the prosecution of Cyber Crime

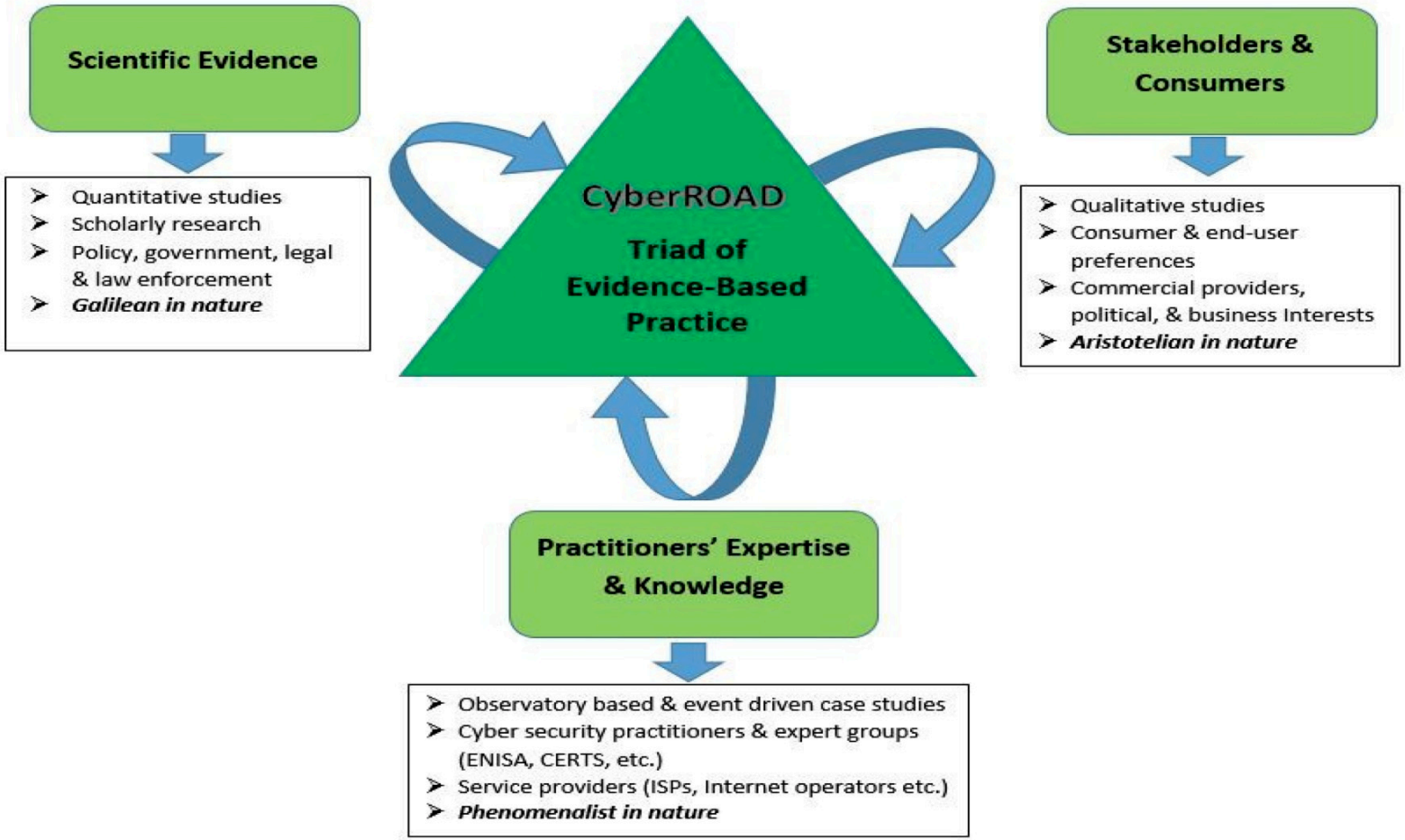
- **DEFENSE**
  - any mechanism, not necessarily technological (i.e. a policy, a legislative framework, and so on), with the potential to either stop or mitigate a threat, or to make its prosecution easier.
    - **E.g.** A legal framework or an authority which allows an effective prosecution of Cyber Crime or Cyber Terrorism is considered a defense

Scenario

A concise description of the current or future state aimed at identifying *"threats"* and *"defenses"*



The CyberROAD Triad

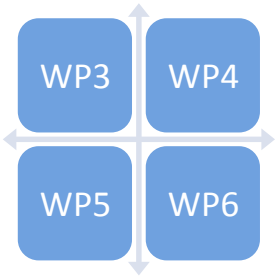


Roadmap creation based on scenario analysis

Actual state (WP3-6)

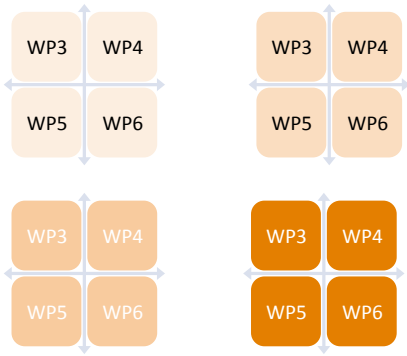
1

several views that compose the **actual state scenario**



2

construction of a set of **future views**



3

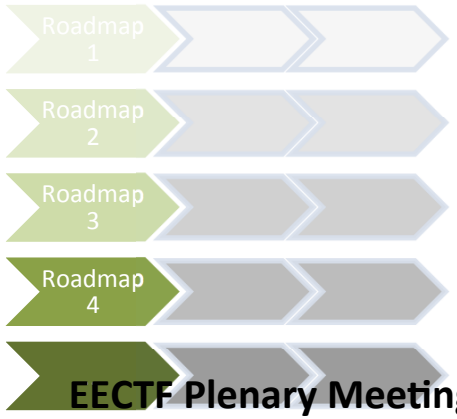
gap analysis: comparison of actual and future desired defenses

4a

identification of **research topics**, as coherent clusters of research gaps

4b

construction of a **roadmap** for every research topic, using PROPRS risk assessing methodology to rank the research activities

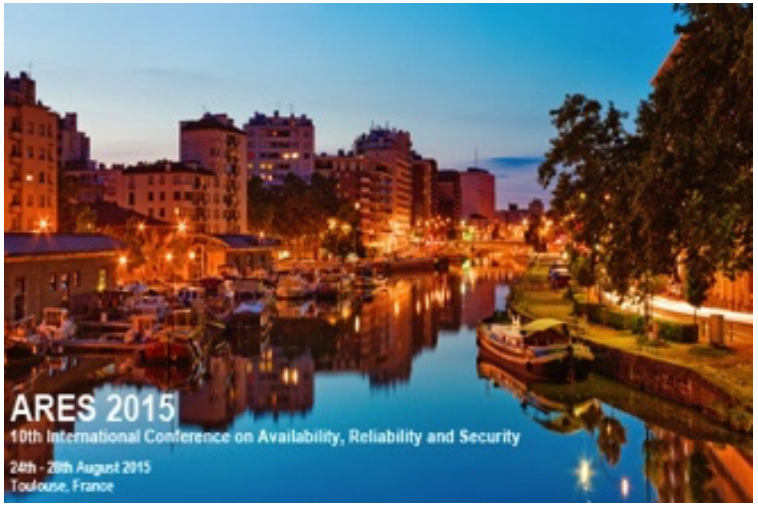


Status of the project and Challenges

- **The project is still in its first year**
  - Spent **<u>to consolidate the roadmapping methodology</u>**…
  - … and **<u>to define</u>** the **<u>Actual State</u>** of Cyber Crime and Cyber Terrorism
    - Deliverables that will depict the Actual State are due by May 2015
- **Challenges emerged during the first year:**
  - **<u>Cyber Crime</u>**
    - To understand exactly how Cyber Crime will evolve in the forthcoming years
      - Many examples of Cyber Crime, unfortunately, already exists
  - **<u>Cyber Terrorism</u>**
    - The definition of Cyber Terrorism is controversial
      - Propaganda, Financing, Training, and Planning are definitely easier over the Internet than elsewhere, but are they actually **Cyber** Terrorism?
      - Is Internet just a channel which facilitates traditional Terrorism?
    - Terrorists want to generate fear:
      - Does a cyber attack against a critical infrastructure really generate fear? Unfortunately, the Charlie Hebdo and the Bardo Museum shootings did…
      - Is it perhaps an attacks against a critical infrastructure Cyber War?
    - Do we have evidence of Cyber Terrorism?
      - E.g. No mention of Cyber attacks in the 2014 EUROPOL EU report on Terrorism

First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism

- **August 24-28, Toulouse, France**
  - Co-located with the ARES Conference - http://www.ares-conference.eu



- **Aimed to:**
  - Disseminate CyberROAD results
  - Obtaining perspectives on the future of Cyber Crime and Cyber Terrorism from **outside** the CyberROAD consortium

- **Important Dates:**
  - **Submission Deadline** **April 10, 2015**
  - Author Notification May 10, 2015
  - Proceedings Version June 8, 2015

- Workshop Website:
  - http://www.ares-conference.eu/conference/ares-eu-symposium/fcct-2015

Contacts

- **Project website**
  http://cyberroad-project.eu

- **PRA Lab Website**
  http://pralab.diee.unica.it

- **Davide Ariu**
  davide.ariu@diee.unica.it