



CYBER ROAD

DEVELOPMENT OF THE CYBERCRIME AND
CYBER-TERRORISM RESEARCH ROADMAP



European Commission
Seventh Framework Programme

CyberRoad Final Workshop

Fabio Roli

Cagliari, May 25th, 2016



Aims of my speech



- Quick overview of project organization and goals
- Providing the context for the next speeches



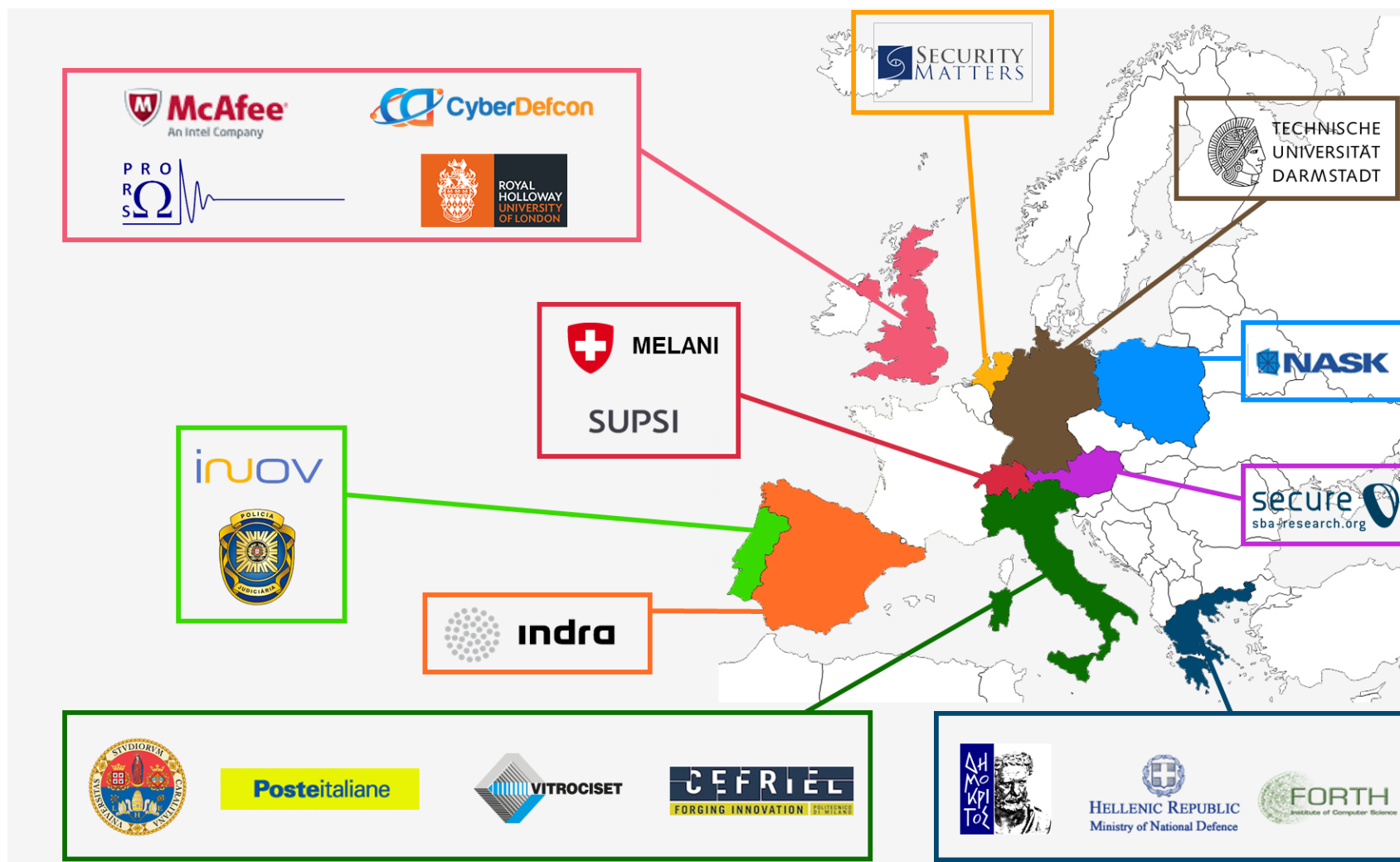
CyberRoad people



«We few, we happy few, we band of brothers»
W. Shakespeare - Henry V



The CyberRoad team





Why CyberRoad?



- The project call: Topic SEC-2013.2.5-1 Developing a **cyber crime** and **cyber terrorism research agenda**
 -
 - What are the major research gaps?
 - What are the major research topics that must be addressed to fill the gaps?
 -
- **Research agenda:** we have been committed to do a **roadmap**
- Based on a solid **roadmapping methodology**



How we did the roadmap



- We built on state-of-the-art methodologies and available guidelines of **S&TRM (science and technology roadmapping)**, including past EU projects
 - Geschka, H., Hahnenwald, H., "Scenario-Based Exploratory Technology Roadmaps - A Method for the Exploration of Technical Trends", 2013
 - EC-funded project eGovRTD2020 www.egovrtd2020.org
- We developed a methodology that takes into account the specific features of the fight against cyber crime and cyber terrorism
- As well as its contextual environment, which encompasses societal, political and economic issues beside technological ones.

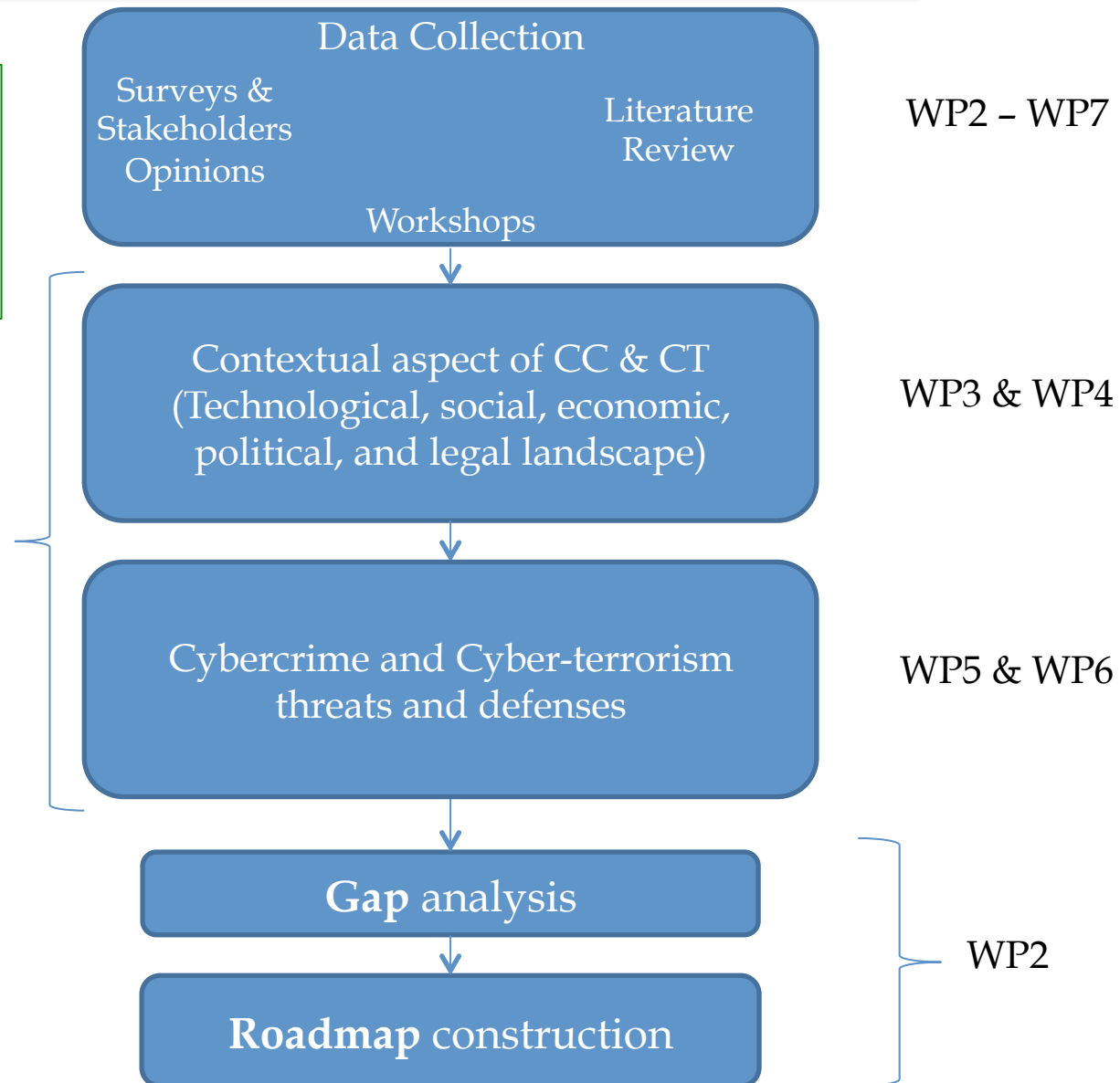


How we did the roadmap



**Exploratory
roadmap using
scenario building
and gap analysis**

Creation of
actual & future
scenarios





Project organization



**Ensures the
management of the
Project**

**WP1
Management**



WP organization



WP2
Scientific
Coordination

Provides the
roadmapping
methodology

WP1
Management



WP organization



WP2
Scientific
Coordination

Identify the S.E.P.L.
scenario behind
Cybercrime and
Cyberterrorism

WP3
Social, Economic,
Political, and Legal
Scenario

WP1
Management



WP organization



WP2
Scientific
Coordination

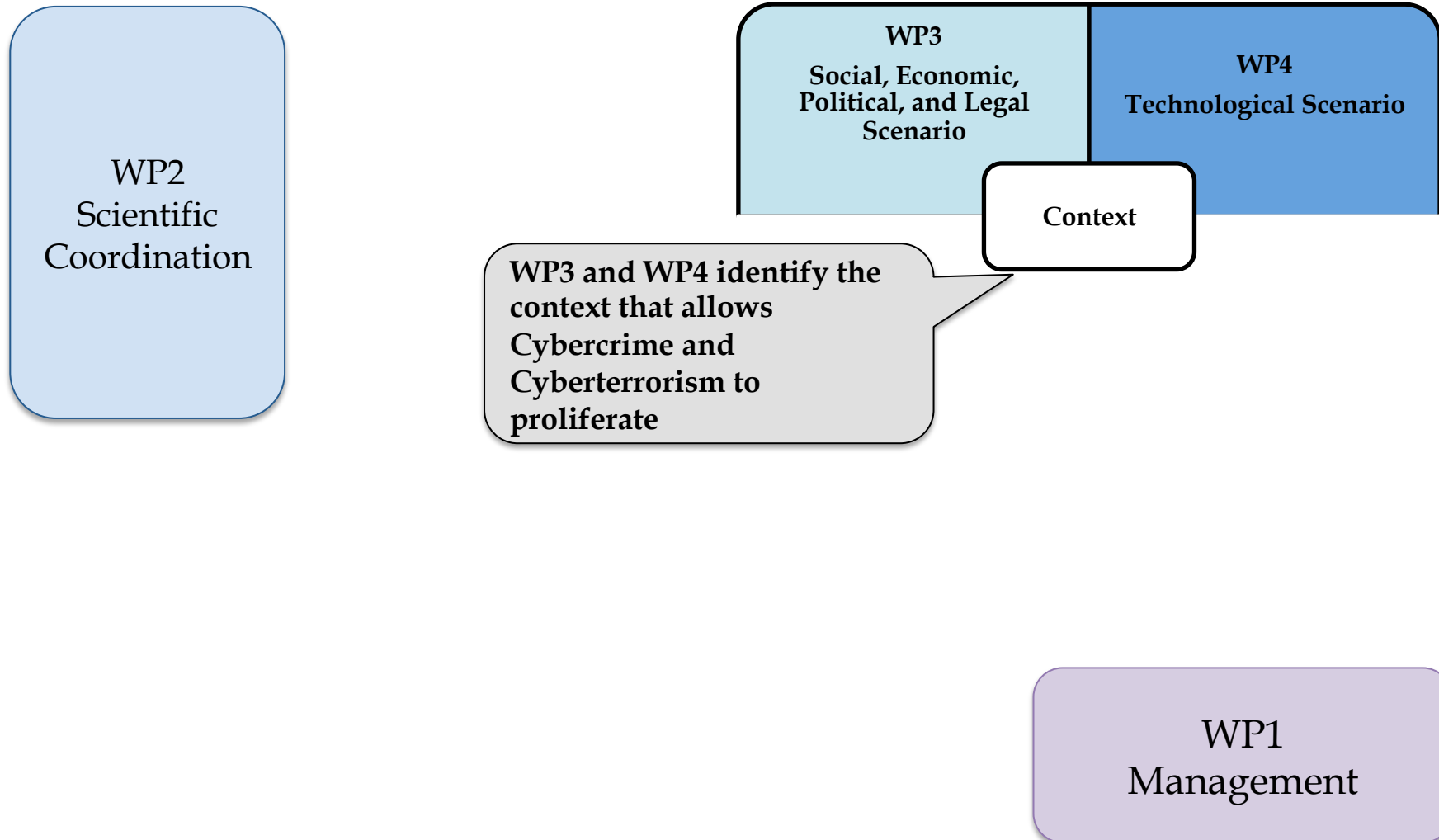
Provides a
comprehensive
view on
technologies

WP4
Technological Scenario

WP1
Management

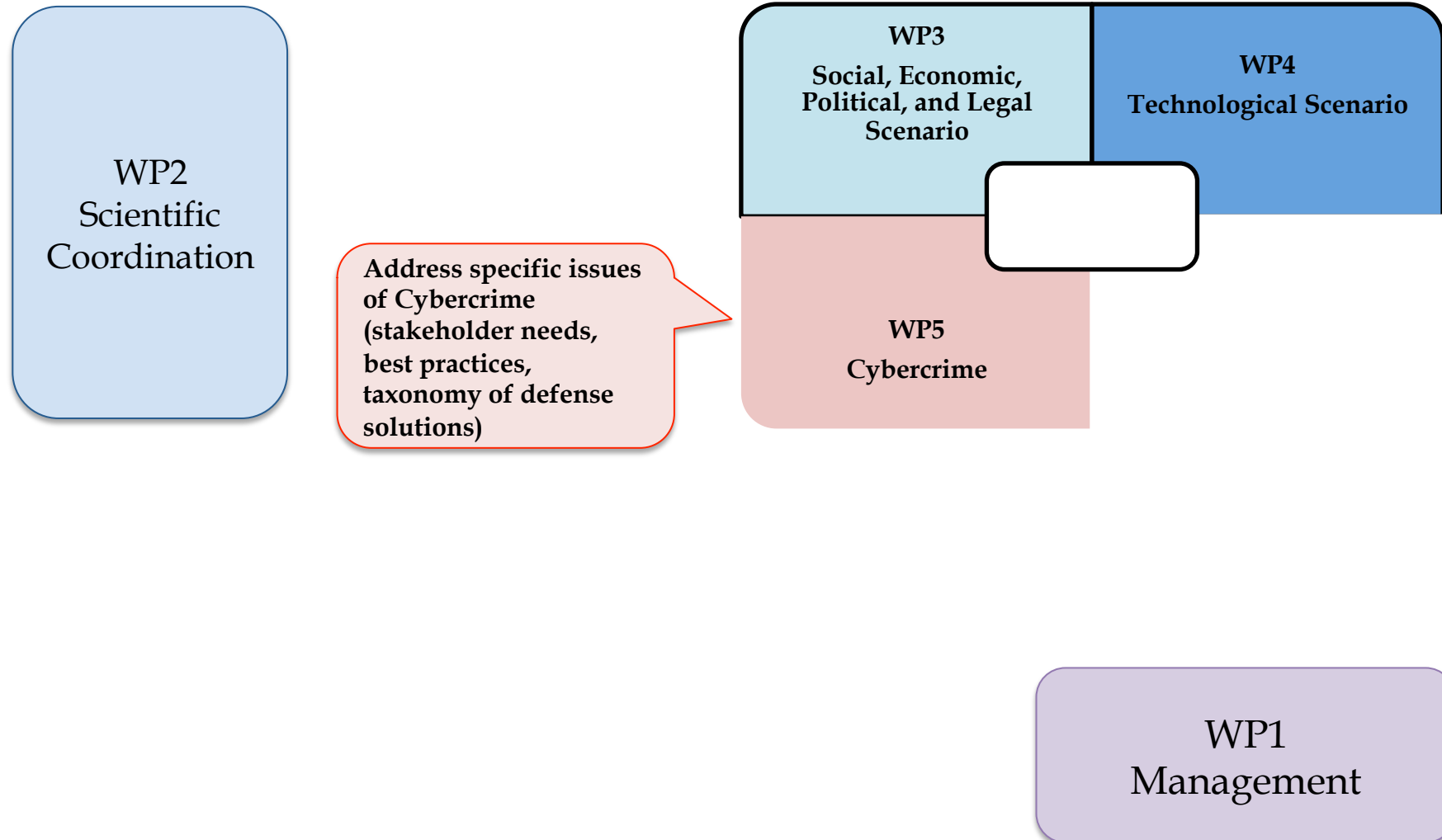


WP organization



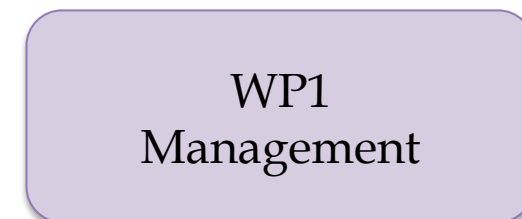
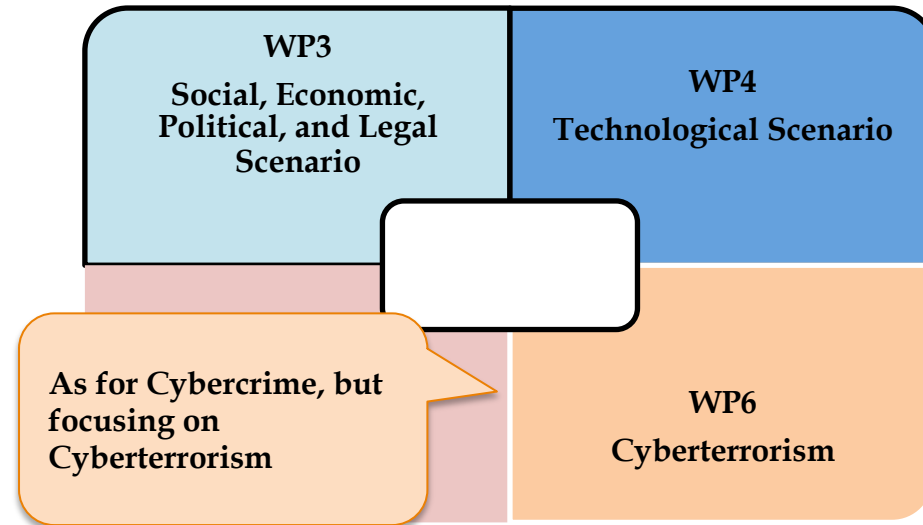
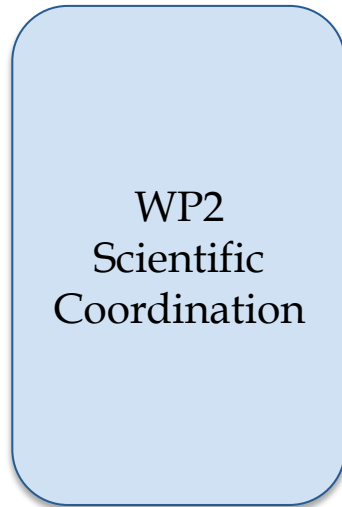


WP organization



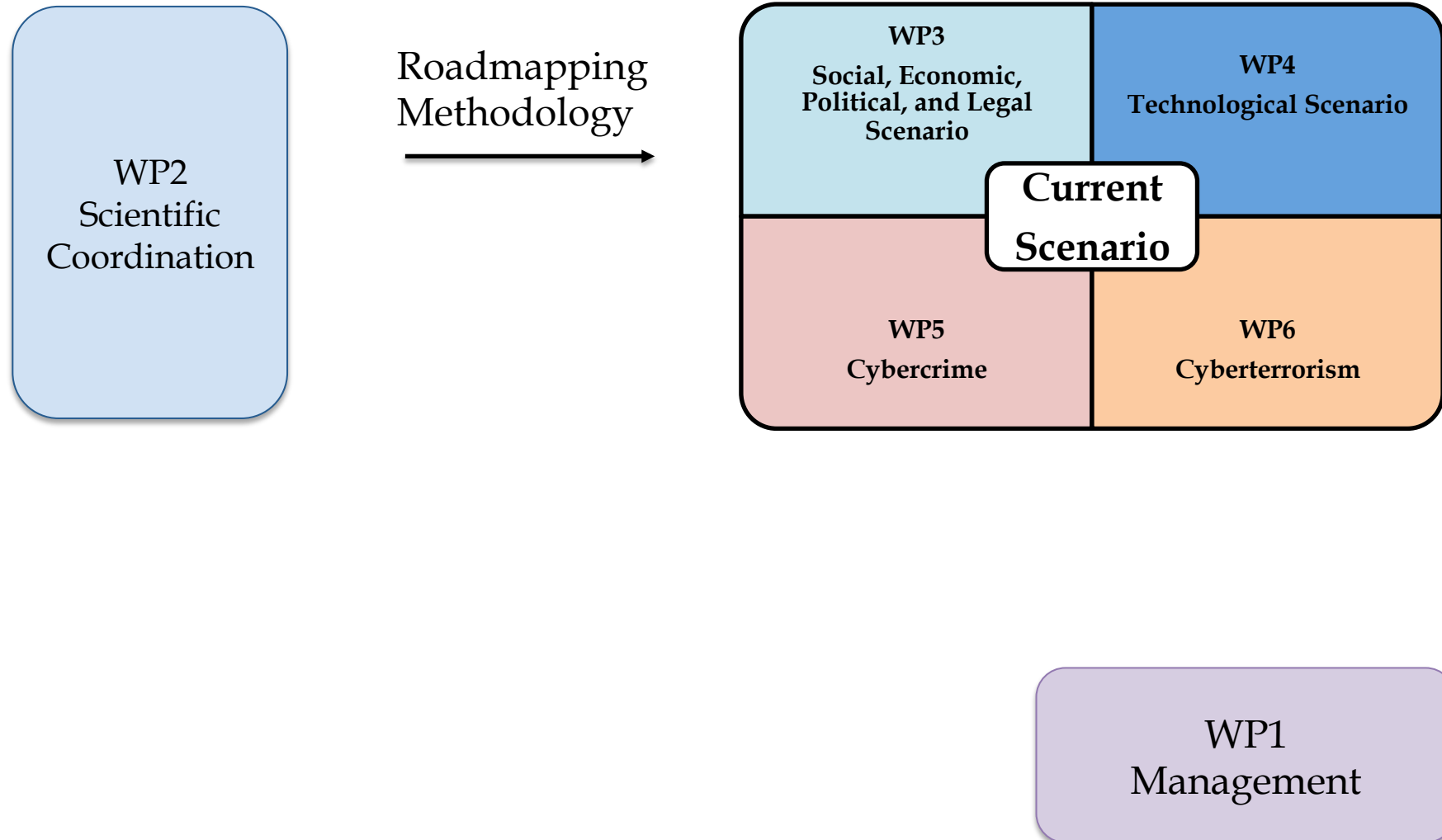


WP organization





WP organization





Scenario Template



Title

Summary

Threats

Threat 1:

- description
- targeted assets
- threat likelihood
- consequences

Threat 2:

...

Defenses

Key drivers

← a **one-page** narrative description

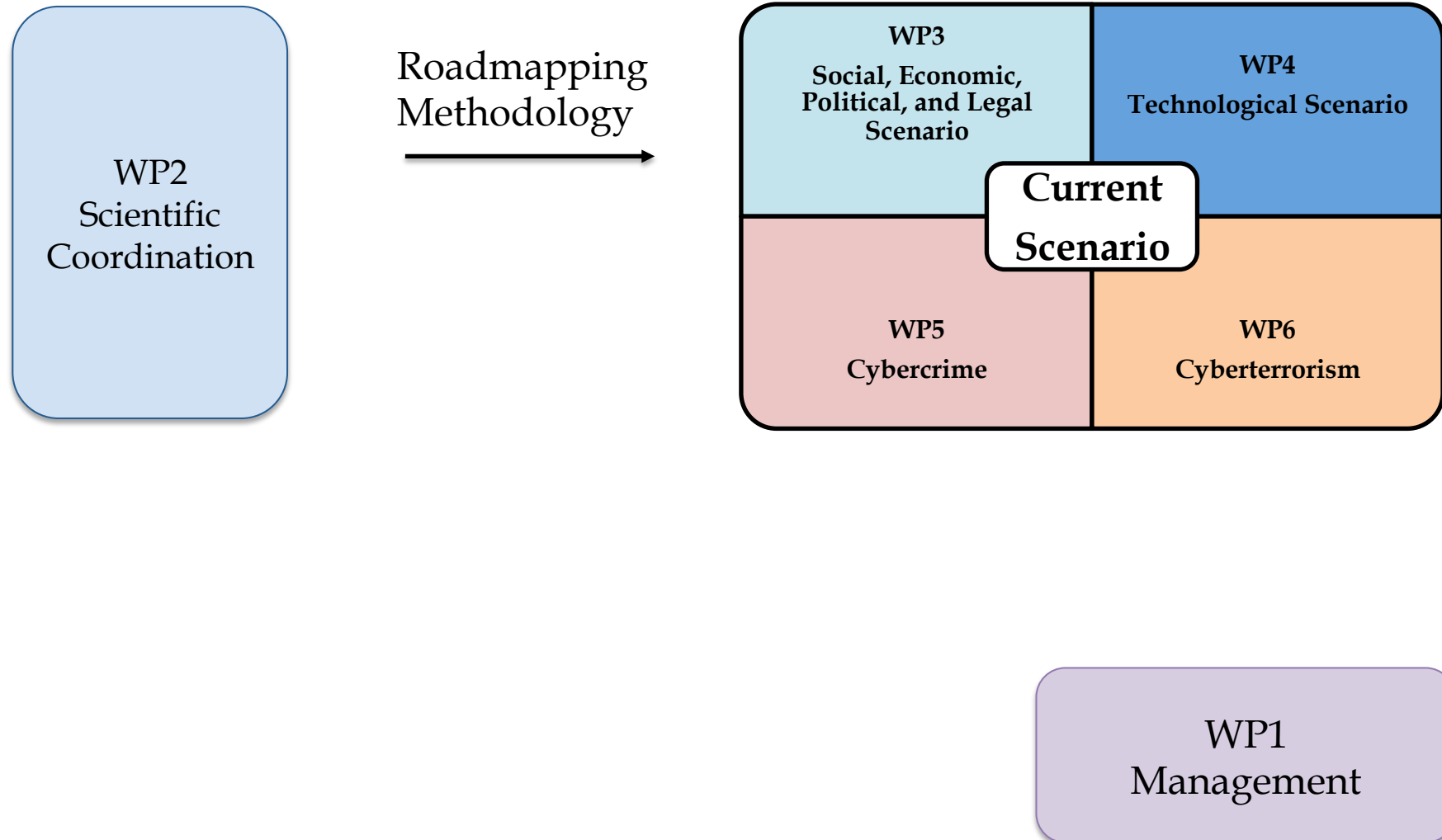
← a list of the threats that emerge from the scenario

← a list of the desired defenses

← a list of the key driving factors

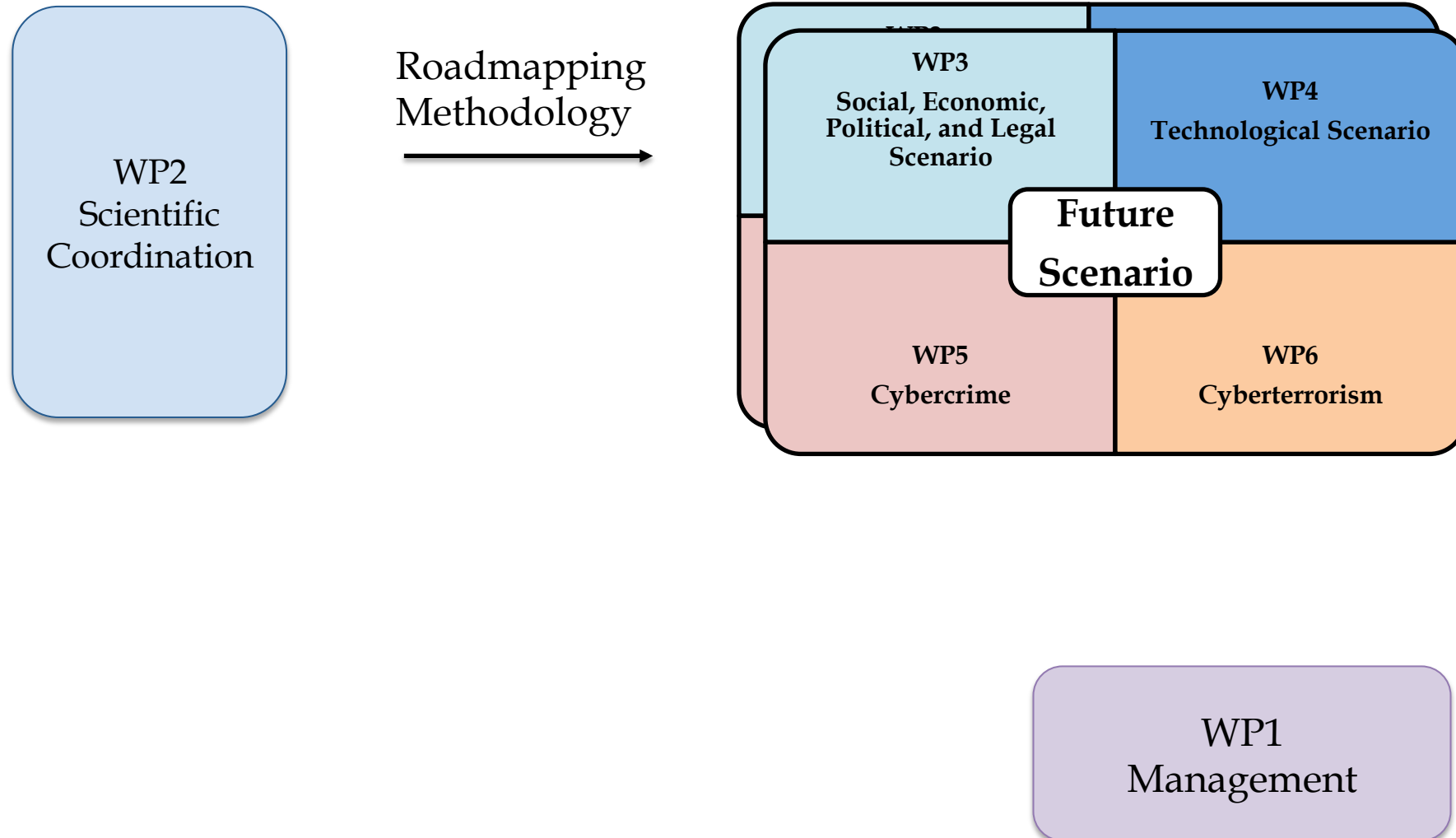


WP organization



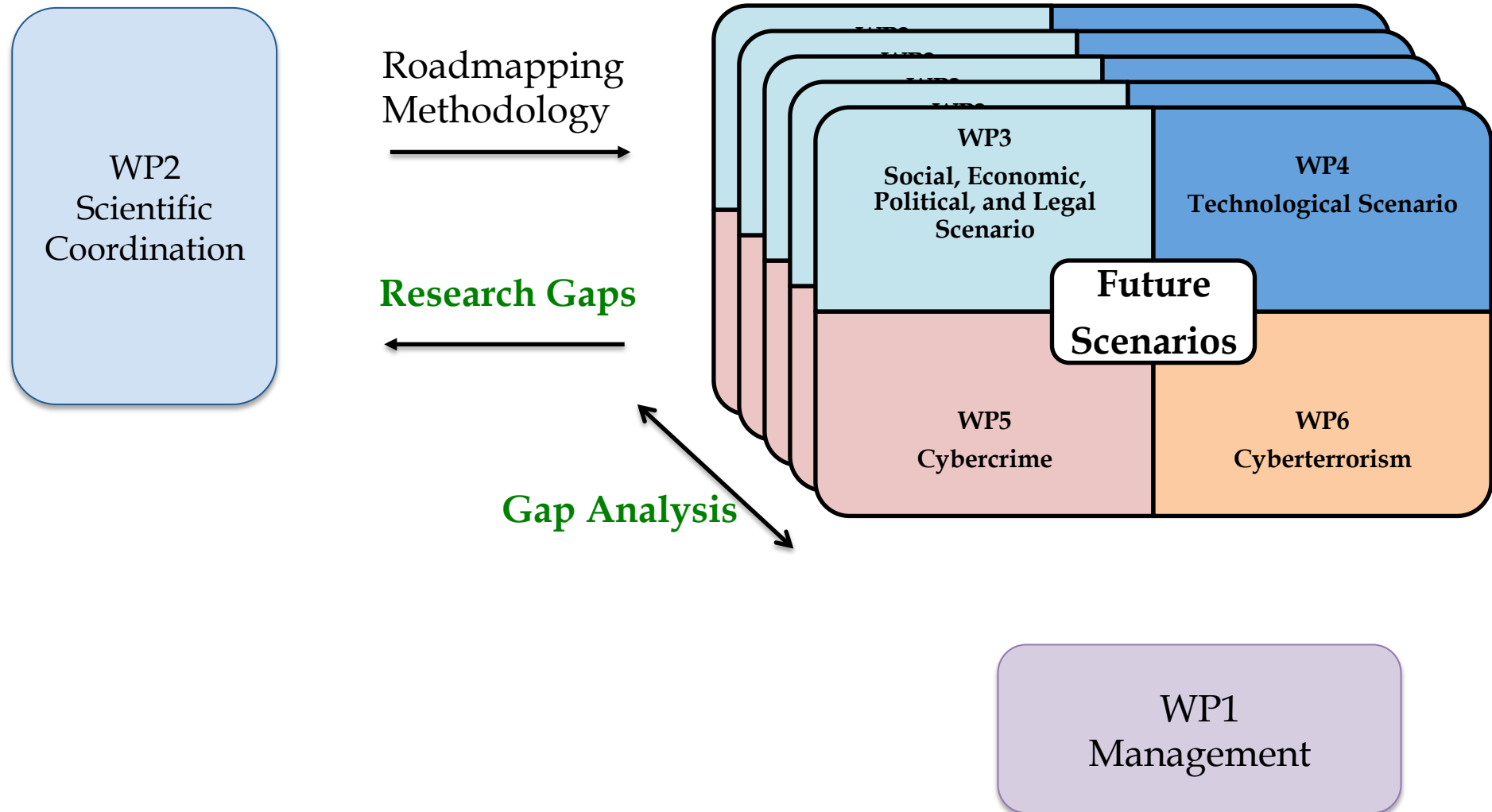


WP organization





WP organization



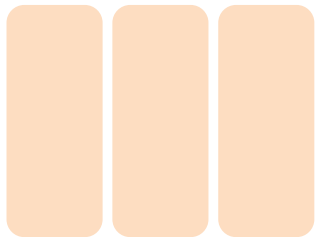


Gap Analysis

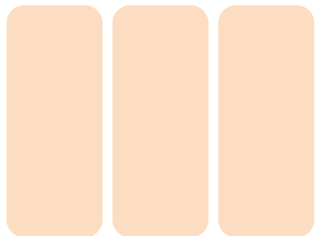


GAP ANALYSIS: the process of comparing actual and future views (i.e., the current knowledge and future needs) in order to identify **research gaps**

Set of actual scenarios



Set of future scenarios



Gap analysis



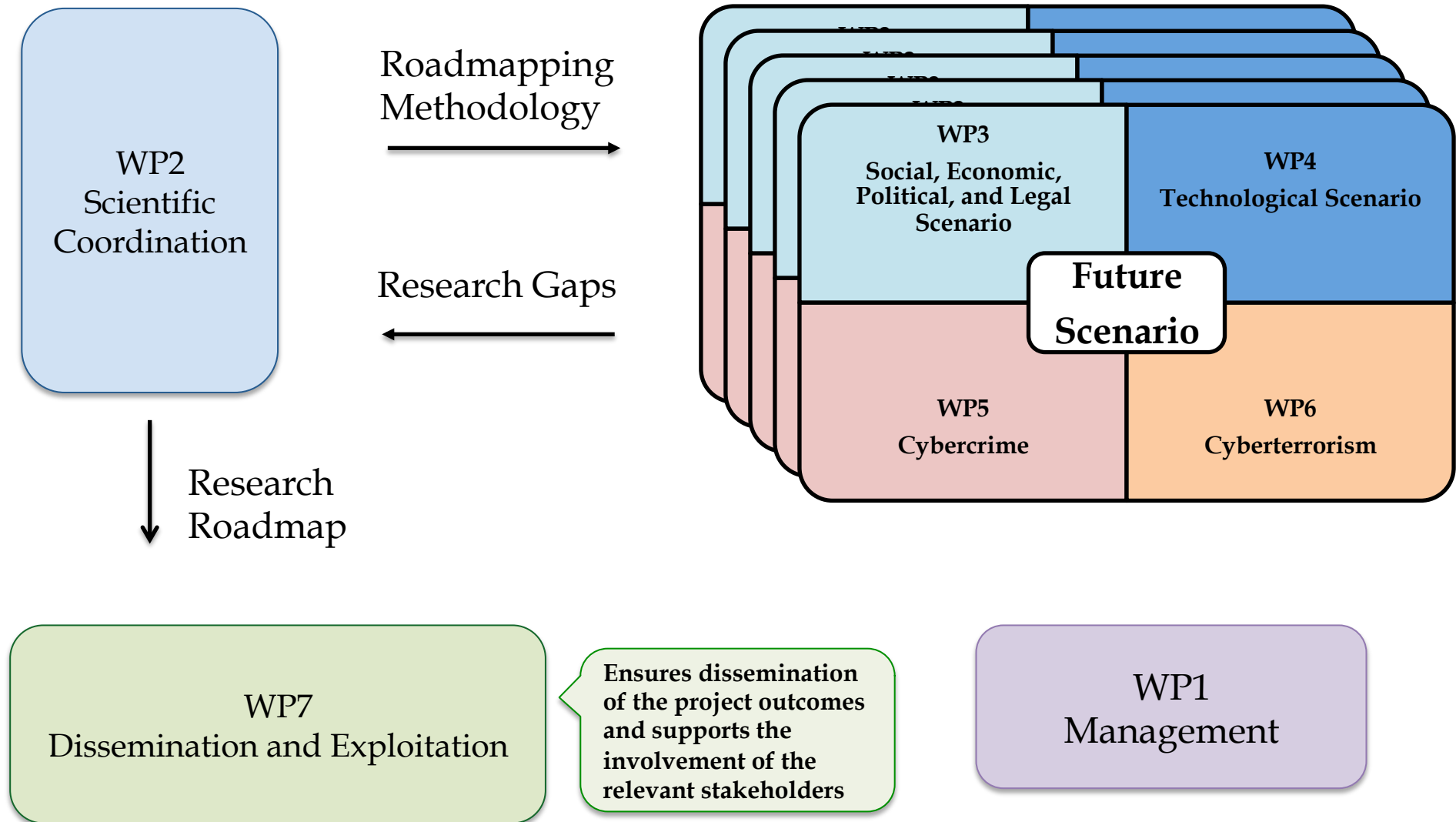
Gaps ○○

○○○

○○○

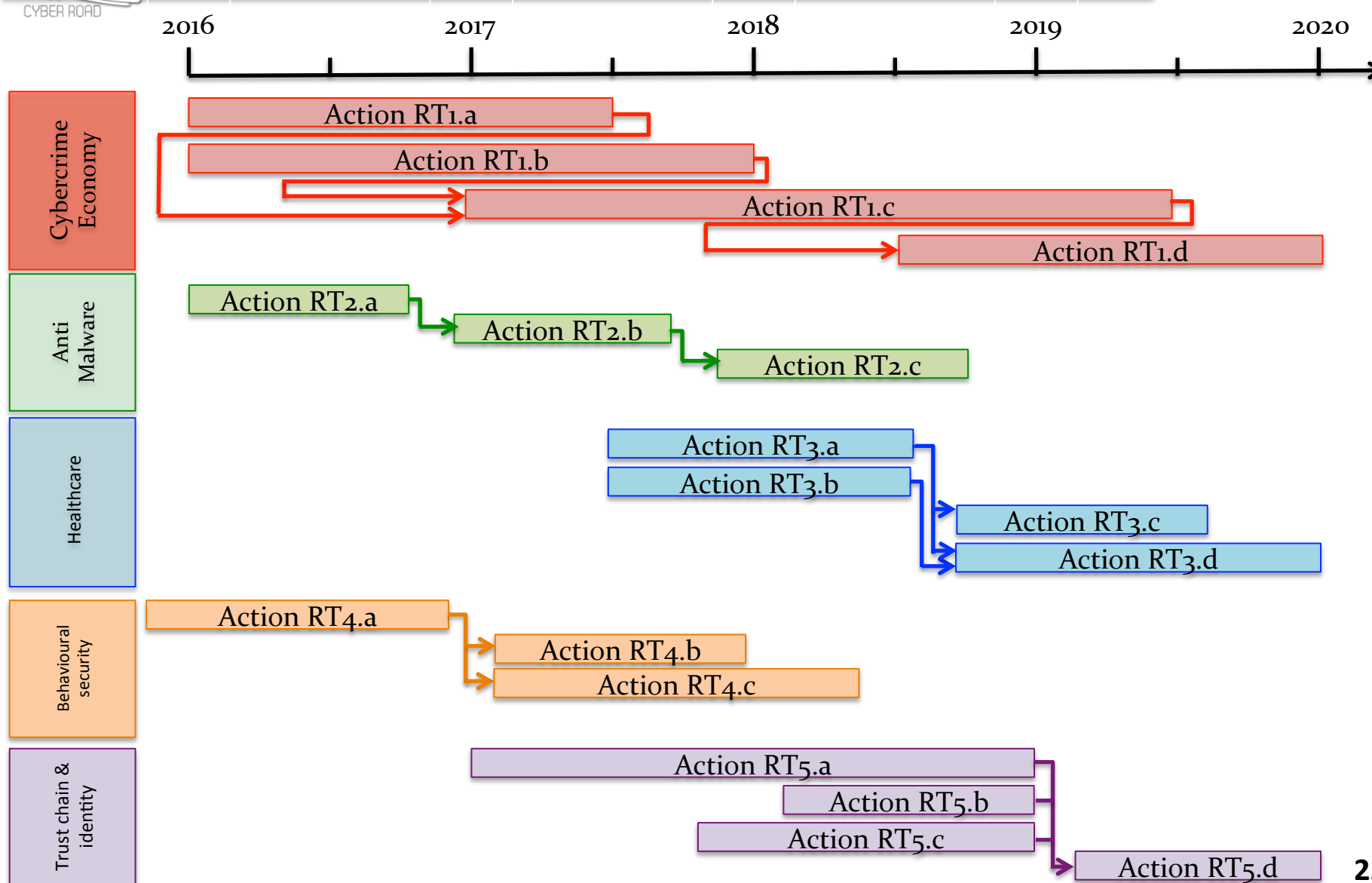


WP organization





Main output: research roadmaps





No crystal ball...



- We do not claim to make definitive predictions on the future of cyber crime and cyber terrorism, or to provide a complete roadmap of research priorities
- We did an **understandable** and **accountable** research roadmap that can help policy-makers to consider and explore the potential evolutions of cyber crime, and to allocate resources on plausible research actions to address research gaps