CYBER ROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

European Commission
Seventh Framework Programme

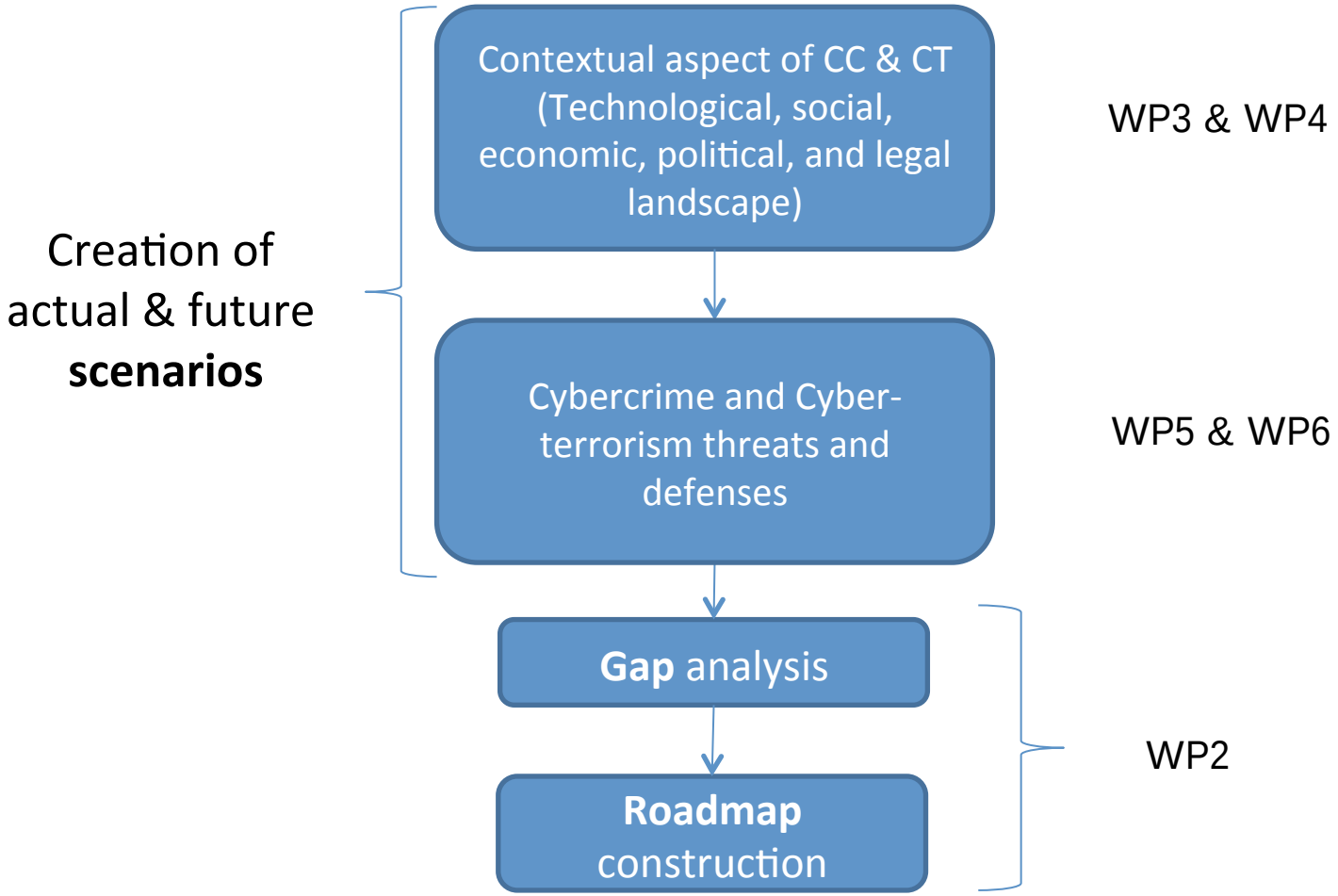
A practical look into scenario building and identifying relevant research gaps

Piotr Kijewski, CERT Polska/NASK
@piotrkijewski

Elisa Costante, SecurityMatters BV

Challenges in Cyber Crime and Cyber Terrorism Research: the CyberROAD perspective,
Cagliari, 25th May 2016

Main steps of CyberROAD roadmapping



Scenario building & templates

A widely used approach in exploratory roadmapping (see Refs.)

In the Cyber ROAD context:

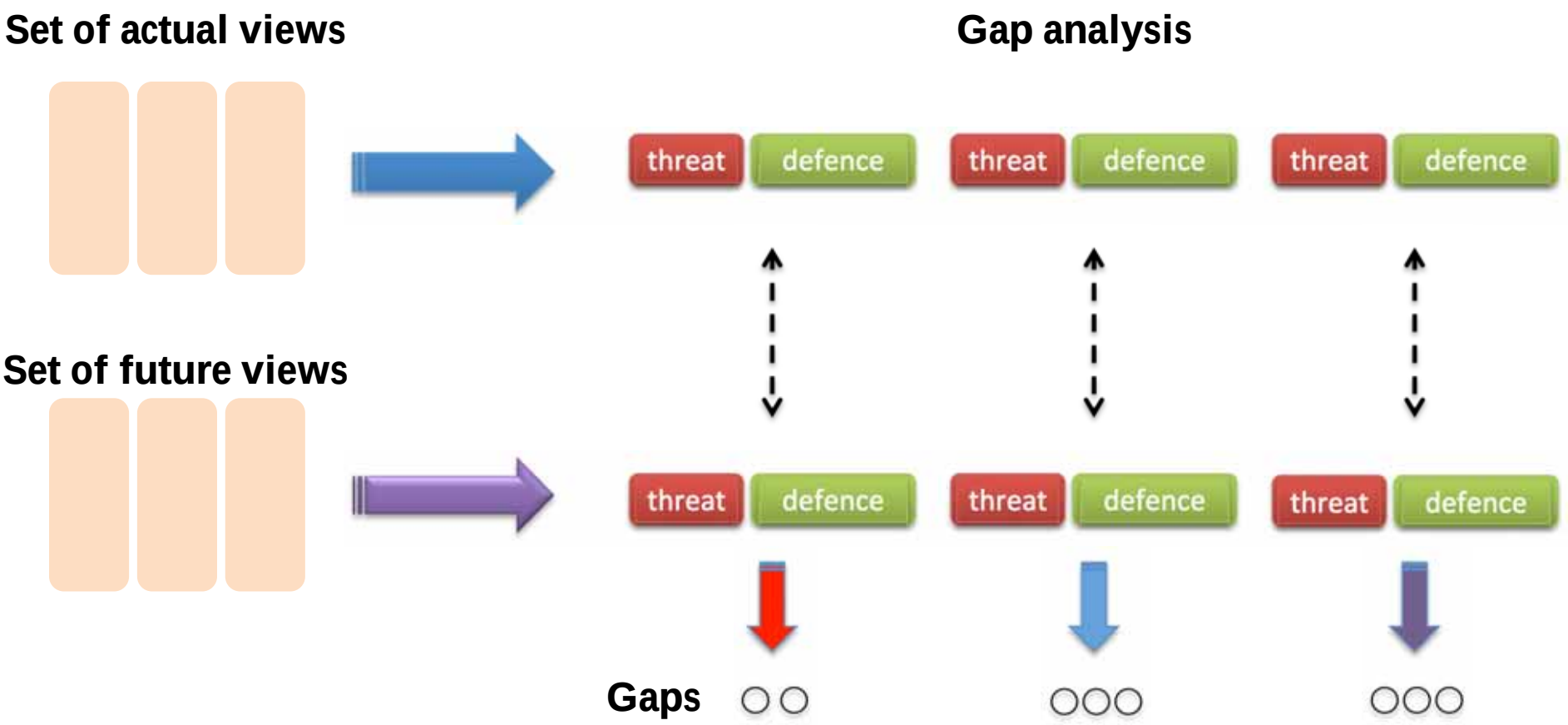
- **SCENARIO**
  a concise and schematic representation of the actual or of a future **state**, aimed at identifying **threats** and **defences**

- **STATE**
  - the whole set of technological, social, economic and political conditions that define the *context* of CC and CT
  - the corresponding specific threats and defenses

- **THREAT**
  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

- **DEFENCE**
  any mechanism, not necessarily technological (i.e., a policy, a legislative framework, etc.), with the potential to either stop or mitigate a threat, or to make its legal prosecution easier

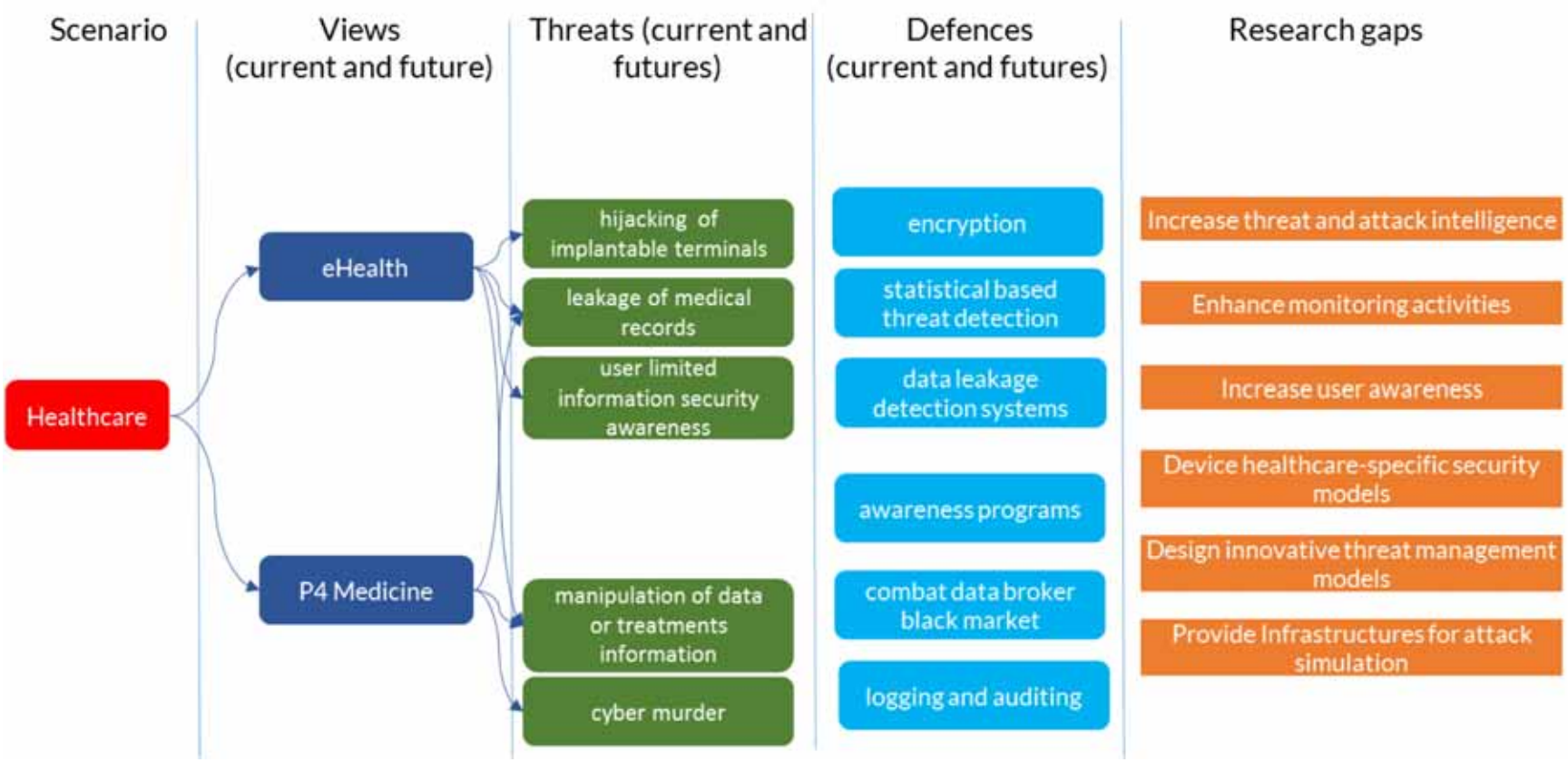
Gap analysis



Scenarios & Views: Cybercrime and Cyberterrorism perspective

Scenario	View
Social Sharing	(i) Social Network
	(ii) Life logging
	(iii)Wearable device
Building Automation	(i) Smart Building
Energy/Utilities	(i) Water Utilities
	(ii) Gas Utilities
	(iii) Smart Grid
Transportation	(i) Rail Transport
	(ii) Aviation
	(iii) Maritime Transport
	(iv) Road Transport
	(v) Freight
Healthcare	(i) eHealth
	(ii) P4 Medicine
Security and safety	(i) Cybercrime as a Service
	(ii) Attribution of cyber crime
	(iii) Trusted Components
Workforce	(i) Enterprise 2.0
Industry	(i) Industry 4.0
	(ii) Just in time production
Financial Services	(i) Cryptocurrencies
	(ii) Online Banking
Data Driven Economy	(i) Big Data
	(ii) Control over Data

Gap identification methodology



Social Networks: Cybercrime

Strengths:	Weaknesses:
✓ The users are not familiar with malware threats on social media. ✓ Sharing malicious content is easy by (ab)using API.	✓ The platforms employ content filters. ✓ Users report unsafe or harmful content.
Opportunities:	**Threats:**
✓ Lots of easily accessible private information, leading to identity theft. ✓ Content tailored to specific, no matter how generic, needs can easily be shared with large group of people. (e.g. “earn money using this simple app!”) ✓ New applications (such as health and wellness apps) are being integrated with social networks	✓ Short time windows for cashing out. ✓ Warning about the attack can be spread as easily as the actual attack. ✓ Platform-wide attack mitigation mechanisms.

Social Sharing: Example Gap analysis

Originating Scenario/ View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Social Sharing (Social Network) **Healthcare** (eHealth) **Workforce** (Enterprise 2.0)	Abuses on new targets (Human, IoT, Infrastructure, linked open data, social, connected things…)	Statistics and detection of preferred attacks pattern	Threat intelligence and detection of new opportunities before they are exploited; emulate human behaviour and creation of "human honeypots"	Threat and attack intelligence, attack simulation infrastructures

Social Sharing: Example Gap analysis

Originating Scenario/ View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Social Sharing (Social Network)	Advanced malware designed to act on social networks to steal PII, commit click fraud and spread harmful messages and media	Malware research and takedowns	Automatic malware defences	Automatic malware research, advanced automatic malware defence and shielding

Social Sharing: Example Gap analysis

Originating Scenario/ View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Social Sharing (Social Network) (Wearable devices)	People are more exposed to attacks in social networks and in wearable devices relying on IoT (e.g. phishing, identity theft, information disclosure)	Legal, awareness, technical	The right to be forgotten. Advanced anonymization techniques	Advanced research in authentication and anonymization

Social Networks: Cyberterrorism

Strengths:	Weaknesses:
✓ Young people, often seek guidance, advice and relationships through social media. ✓ The platforms supply easy, cross-platform, encrypted communication mechanisms.	✓ Social media activities are monitored by state actors (e.g. NSA). ✓ Social media activities are recorded, so becoming anonymous requires additional steps (e.g. using an anonymous proxy)
Opportunities:	**Threats:**
✓ Messages can go viral. ✓ It is easy to target specific groups for recruitment, organization, coordination, communication, reconnaissance and propaganda.	✓ Content opens dialogue which can be countered by comments. ✓ State actors can create their own counter-propaganda contents.

Social Sharing: Example Gap analysis

Originating Scenario/ View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Social Sharing (Social Networks)	Propaganda and recruitment over social platforms	Counter-propaganda, social media management, censorship	Media-analysis technologies	Research on information propagation in non-centralized media (available research is focused on state-controlled media)

Attribution: Cybercrime

Strengths:	Weaknesses:
✓ In cybercrime it is easy to anonymize oneself online. ✓ In cybercrime it is easy to create fake trails online. ✓ Inadequate international cooperation & legal framework. ✓ Hosting providers turning a 'blind-eye' or unable to detect nefarious practices	✓ Bulk traffic monitoring is carried out by governmental agencies. ✓ Offline means of obtaining information (HUMINT). ✓ Extortion attempts may be subverted by third parties (easy impersonation). ✓ Re-use of known malware & attack tool code, which can be detected via stylometry.
Opportunities:	**Threats:**
✓ It is easy to frame somebody else ✓ Easy access to cybercrime tools (github etc) makes analysis of code reuse difficult. ✓ Digital anonymity tools and services ✓ Open access to current cyber vulnerabilities, blacklists, what methods & tools are currently detected (in order to develop counter measures).	✓ Monitoring & threat analytics from LE and private companies ("threat intelligence"). ✓ Progress in work on attribution of authors of code and other forensic techniques. ✓ Possible analysis of relationships between tools.

Attribution: Example Gap analysis

Originating Scenario/ View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Safety & Security (Attribution)	Inadequate information sharing mechanisms between parties. With a lack of clarity, differences, and misunderstandings between EU countries relating to privacy, traffic monitoring, data storage & analysis	Ad hoc, provisional, information sharing platforms, often informal	(international) legal frameworks & formalized sharing platforms	Analysis of international, and inter-EU country data protection - how & what can we legally share this data, for cyber forensics

Attribution: Example Gap analysis

Originating Scenario/ View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Safety & Security (Attribution)	Lack of enforcement of internet-wide policing standards	Voluntary implementation /enforcement of actions against cybercriminals	Robust legal frameworks for ensuring coordinated actions against cybercriminals	Creation of world-wide policing standards

Attribution: Example Gap analysis

Originating Scenario/ View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Safety & Security (Attribution)	Framing others	Police work following the money or motives	Evolution of methods of fighting organized cybercrime	Research on tools, tactics, procedures of organized crime

Attribution: Cyberterrorism

Strengths:	Weaknesses:
✓ No toolset or framework to perform systematic & meaningful attribution ✓ Despite data collection, agencies keep information to themselves or do not recognize their importance to act in a preventive manner (for political or formal reasons) ✓ Hosting providers turning a 'blind eye' to suspicious practices	✓ Difficulties in maintaining long-term OPSEC ✓ HUMINT capabilities of LE ✓ Potentially difficult to prove authorship of certain acts (which may defeat part of the purpose of a cyberterrorism act)
Opportunities:	**Threats:**
✓ False flag operations (eg. for political gain) ✓ Easy access to cybercrime tools (github etc) makes analysis of code reuse difficult ✓ Use of anonymity tools & services, and defeating stylometry or HUMINT based investigation e.g. Anonymouth	✓ Growth in private companies providing SIEM (Security information and event management) services i.e. "threat intelligence". ✓ Progress in work on attribution of authors of code and other cyber forensic techniques, e.g. stylometry. ✓ Possible analysis of relationships between tools.

Attribution: Example Gap analysis

Originating Scenario/ View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Safety & Security (Attribution)	Difficulty in identifying meaningful information on upcoming threat (information overflow: needle in haystack problem of finding what is important)	Ad-hoc analysis tools for intelligence analysis, tip-offs, HUMINT	Artificial intelligence, machine learning, big data applied to threat intelligence	Intelligence has access to great volume of information but lacks of tools to identify the most meaningful

Attribution: Example Gap analysis

Originating Scenario/ View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Safety & Security (Attribution)	Lack of knowledge where cyberterrorism comes from (root cause)	Current cyber aspect of war on terrorism - investigation of known terrorism suspects	Understanding motivation of cyberterrorists, enabling profiling for early identification of radicalization	Research on cyberterrorism motivations/ root cause

Attribution: Example Gap analysis

Originating Scenario/ View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Safety & Security (Attribution)	Wide proliferation of easy to use offensive tools	Active countermeasures disseminating backdoored/ subverted offensive tools, active infiltration of tool development markets	Refined fingerprinting of tools aided by contextual attack information	Next generation of analysis, fingerprinting tools with context

Industry 4.0 – Cybercrime

Strengths:	Weaknesses:
✓ Intense machine-to-machine connectivity allows to easily move around once inside the network.	✓ In case separation between the corporate network and the control network is in place, entering the system might be more difficult
Opportunities:	**Threats:**
✓ Protocols in use do not support encryption ✓ Large amount of data collected ✓ Aging workforce	✓ Monitoring solutions might be in place to spot intrusions or leakages ✓ Increasing security awareness from operators

Industry: Example Gap analysis

Originating Scenario/View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Industry (Industry 4.0) (Just in time Production)	Industrial espionage will increase because of the intense interconnectivity of components.	Encryption and password protected files	Reliable exchange of manufacturing data and plans through secure channels.	Enforce data security for intellectual property (IP) protection

Industry: Example Gap analysis

Originating Scenario/View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Industry (Industry 4.0) (Just in time Production)	Manipulation of sensor & actuator data as well as meta data and communication data.	Well-accepted cryptographic primitives such as encryption, message digests and signing of messages.	Industrial protocols more resilient to cyberattacks	Strong and fast lightweight encryption that is also practical for resource-constrained devices.

Industry 4.0 – Cyberterrorism

Strengths: ✓ **Once inside a network, the high level of machine-to-machine connectivity enables attackers to easily move within the network to e.g. find sensitive information.**	**Weaknesses:** ✓ **System might be extremely customized** ✓ **Time necessary to gain insight about the control logic**
Opportunities: ✓ Extensive automation of the production process makes possible that, once in, it is possible for an attacker to change every small part of the process (e.g. change recipe of food or rotation speed of machines).	**Threats:** ✓ Monitoring solutions might be in place to spot intrusions or leakages ✓ Industry 4.0 might use innovative technologies designed with security in mind

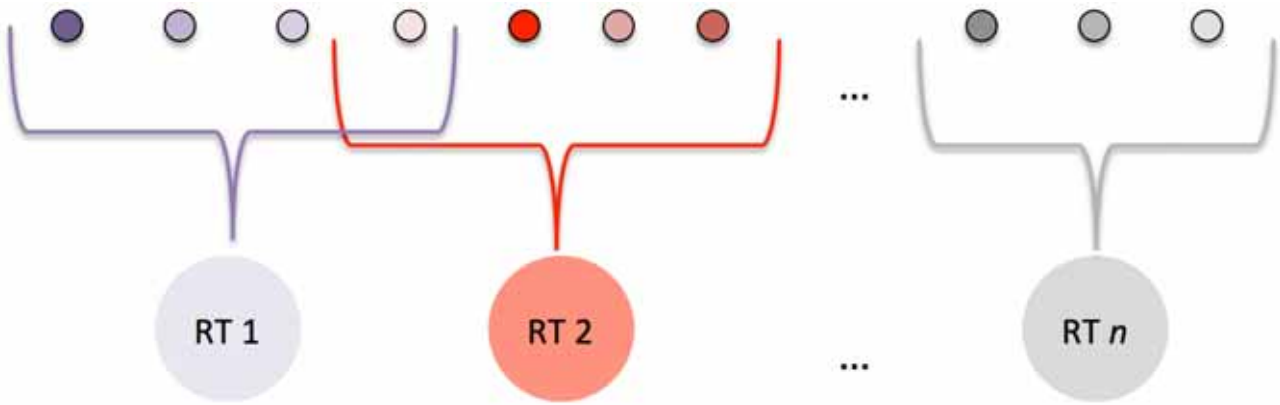
Industry: Example Gap analysis

Originating Scenario/View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Industry (Industry 4.0)	Highly automated production processes enable cyber terrorists to remotely control and tamper with the process.	Strong access control systems and activity monitoring.	Detection techniques able to alert in case of suspicious activities in the factory (e.g. detect change in the manufacturing process and activities)	Innovative technique for the detection of anomalous changes in the process activities and status. Process awareness embedded in security tools Improve Incident Response

Industry: Example Gap analysis

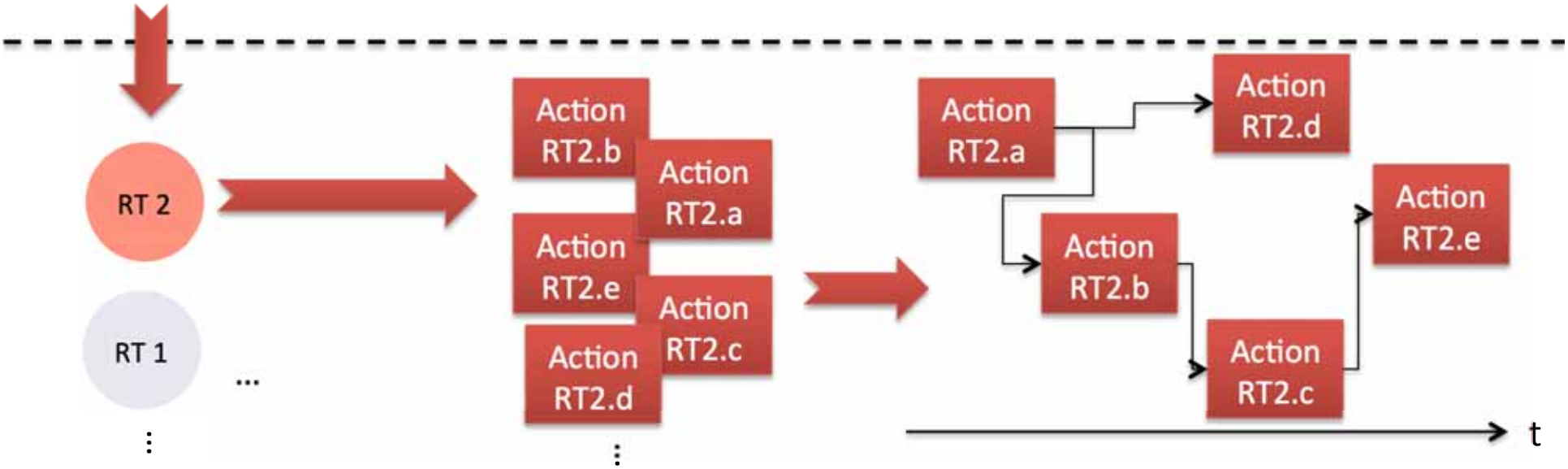
Originating Scenario/View	Threat (future view)	Defence (current view)	Defence (future view)	Research Gaps
Industry (Just in time Production)	Hardware backdoors in smart devices / actuators / sensors	Certified hardware, trust towards device developer.	Transparent and efficient scanning techniques in order to reveal hidden hardware features.	Technologies and algorithms to efficiently reveal unintended / hidden hardware components or features.

Roadmap construction



Research gaps
(from gap analysis)

Research topics
(clusters of research gaps)



Prioritizing gaps and research topics

Identifying **research actions** for each research topic

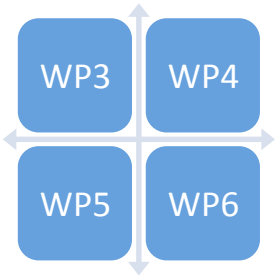
Placing the actions in a **time frame**

Summary of the roadmapping technique

Current state (WP3-6)

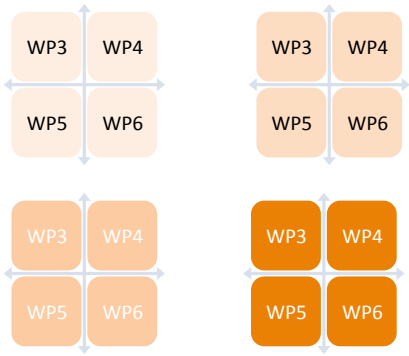
1

several views that compose the **current scenario**



2

construction of a set of **future views (scenarios)**



3

gap analysis: comparison of actual and future (desired) defences

4b

construction of a **vertical roadmap** for each research topic

4a

identification of **research topics** (clusters of research gaps)

References

- Codagnone, C. & Wimmer, M.A. (eds.): *Roadmapping eGovernment Research: Visions and Measures towards Innovative Governments in 2020.* MY Print snc di Guerinoni Marco & C, Clusone, 2007

- Geschka, H. & Hahnenwald, H., "Scenario-Based Exploratory Technology Roadmaps - A Method for the Exploration of Technical Trends"; in: *Technology Roadmapping for Strategy and Innovation*, Moehrle, M. G.; Isenmann, R. & Phaal, R. (Eds.), Springer Berlin Heidelberg, 2013, 123-136

- Wright, R.B. & Cairns, G., "Does the intuitive logics method – and its recent enhancements – produce "effective" scenarios?", *Technological Forecasting & Social Change* 80 (2013) 631–642

- Bradfield, R., Wright, G., Burt, G., Cairns, G. & Van Der Heijden, K., "The origins and evolution of scenario techniques in long range business planning", *Futures* 37 (2005) 795–812

Thank you for your attention