Collaborative action
Enabling efficient use of knowledge for safety and security

PDT Europe, Paris

9-10 November 2016

Juha Rautjärvi

Mikkeli Development Miksei Ltd.

CBRNE Finland Association

Contents

1. Introduction
2. Research lifecycle management
3. Societal Security Stakeholders
4. Collaborative space to be established above the existing realities
5. Engagement of societal security stakeholders to collaboration
6. Collaborative space and the key stakeholders in action
7. Closing remarks

1. Introduction

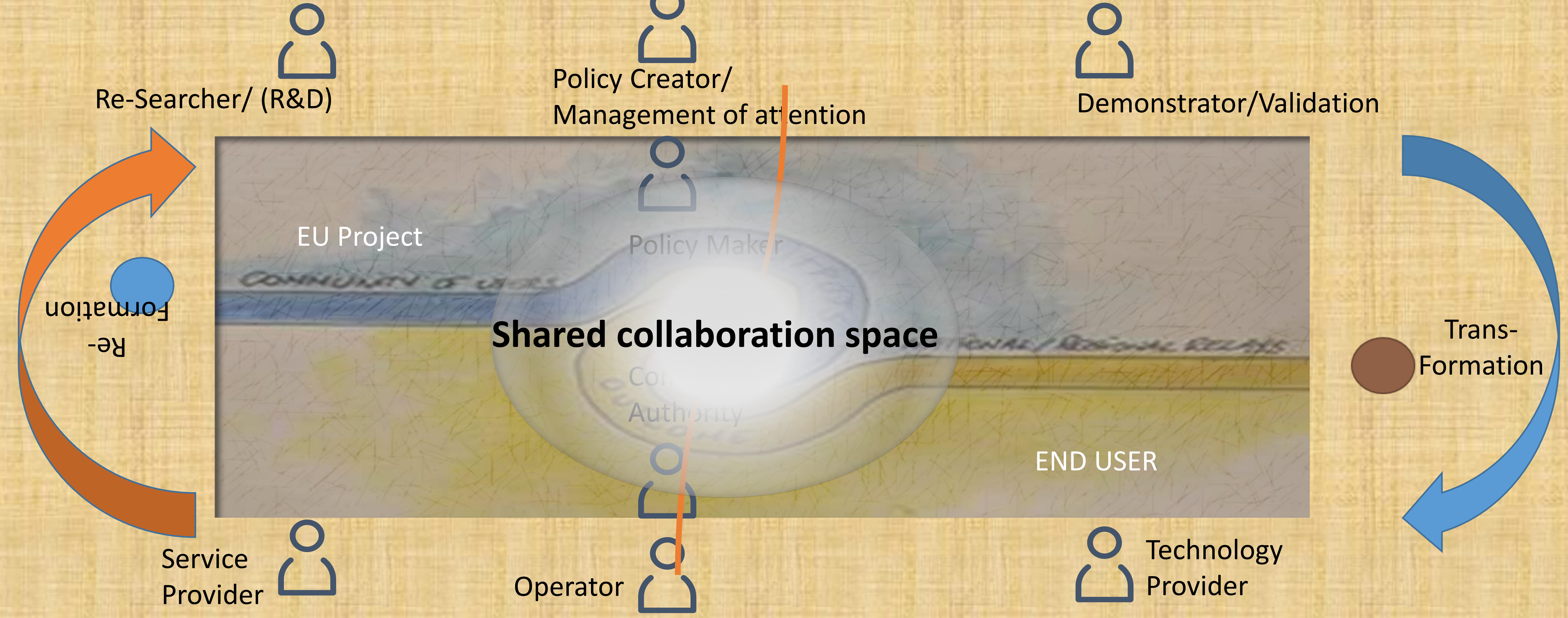
Collaboration for public safety and national security is not a trivial challenge.

The presentation is based on experience and practice. I will elaborate how collaborative methods and technologies used in industry could enhance administrative efficiency of processes aimed at taking care of the societal security, in particular for securing timely application of research and development results for intended use:

- Safety situation in society calls out for increased collaboration between all authorities involved and actors in charge of assets potentially under threats.
- Besides being under threats the same assets can also be used as weapons against society for instance if they involve chemicals. – Anticipation and risk mitigation must be in focus.
- A major issue is how to get a more rapid value from research and innovation in European RTD projects like Horizon 2020 as many promising solutions are coming out of these.
- The results must be made available and understood by authorities who set the rules and own the national and international security resources. A better collaboration between all involved is needed. Reliable and actionable body of knowledge is required and, trustworthy actors.
- Continuous validation of that body of knowledge is inherent quality of the process and imply evaluation also of the premises, legacy and obsolescence of the data and information the Knowledge is based upon.

2. Research lifecycle management (contextual reflections, an idea)

- **Challenge:** **Transformation R&D result to End User assets – Operational experiences to reform R&D programs**
- **Response:** **Collaboration enabling knowledge creation and sharing, reliable premises for decision-making and action**



Re-Searcher/ (R&D)

Policy Creator/
Management of attention

Demonstrator/Validation

Re-
Formation

EU Project

Policy Maker

Shared collaboration space

Com
Authority

END USER

Trans-
Formation

Service
Provider

Operator

Technology
Provider

3. Societal Security Stakeholders Framework

- **The stakeholders responsible for taking care of security must collaborate cross the sectorial borders**

- Security of citizen within its environment is in center and, also at stake – An object and subject of security measures
- Citizen is in interaction with members of community around, fellow citizens, organizations, NGOs and other

- Policy making bodies of a State construct are enabling transformation of policies to security operations
- Operatives, police, border, rescue services, etc. carrying out given tasks and perusing required reformations

- R&D as well as validation processes are providing proven premises for strategy development and its implementation
- Equipment and services providers as well as maintainers of critical structures enable operatives to deliver services in efficient manner

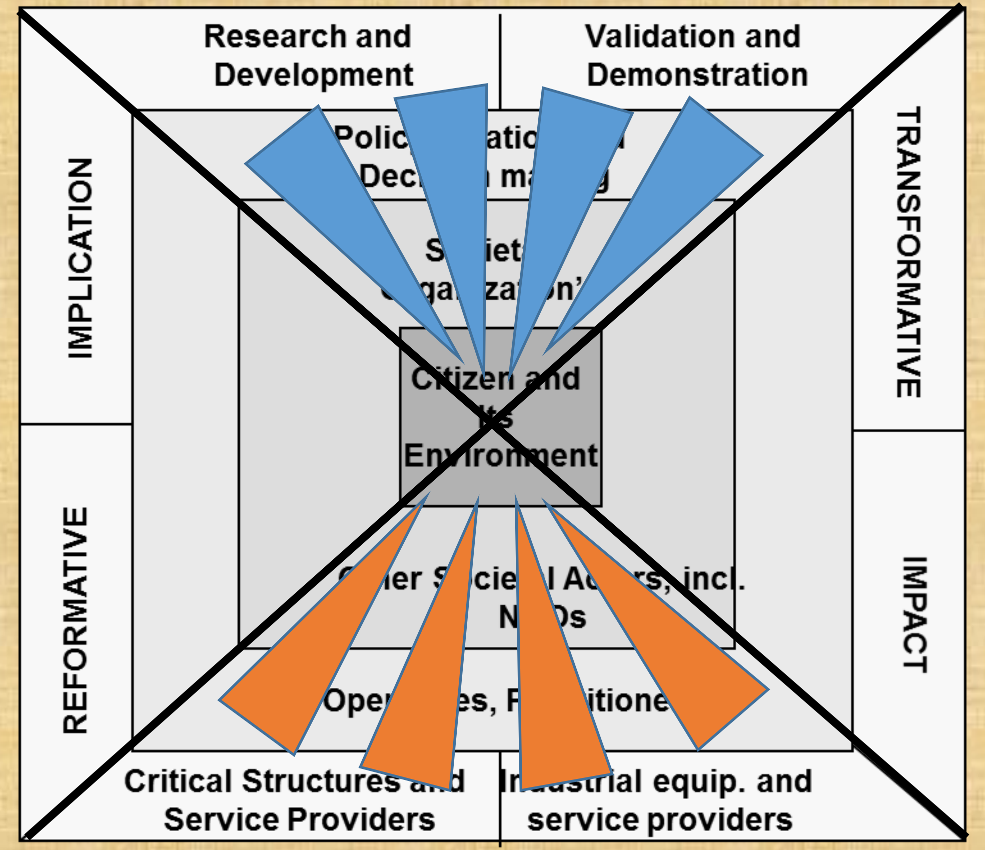
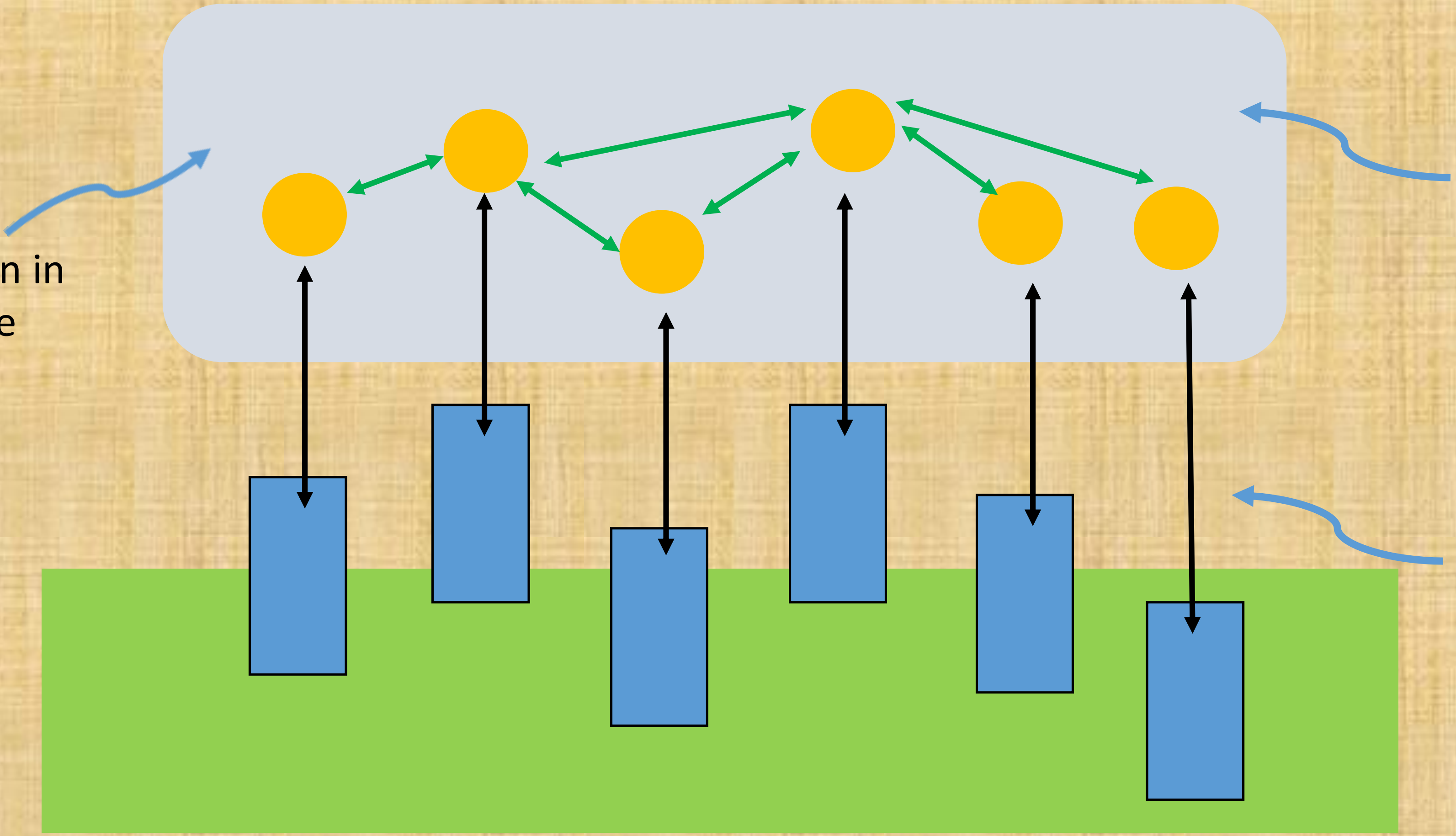


Figure 2. Complex set of societal security stakeholders

4. Collaborative space established above the existing realities

- **Collaborative space established in order to elaborate efficiently determined cases by the actors**



Enabling collaboration in secure space

Key stakeholders, the actors in collaborative space

Stakeholder organizations on the ground

5. Engagement of societal security stakeholders to collaboration

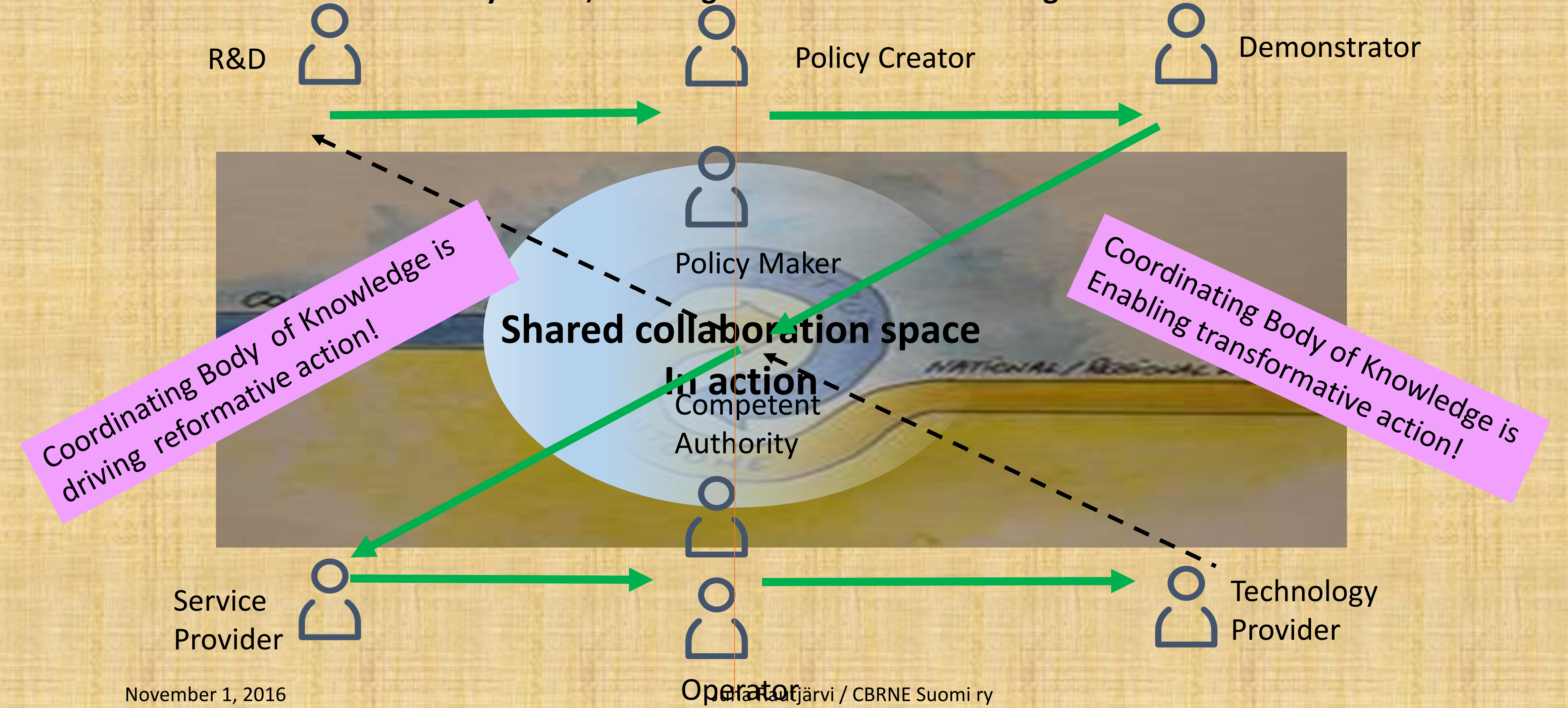
- **Identification, analysis and engagement of key stakeholders (actors) is the key to successful operationalization of end-users. –This, not being a trivial challenge!**
- Engagement of key stakeholders (actors) to collaborative undertaking is intended to provide efficient way to address particular challenges in collaborative manner. – It’s not aimed at interfering to any extent to normal organization life or normal delivery of projects.

- Essential steps for solid work with various stakeholders are:
  - Identification of key stakeholders
  - Systematic analysis of their motives, views and positions
  - Determination of their willingness to participate
  - Involvement in the given undertaking
  - Understanding the roles, expectations and associated needs

- Stakeholder analysis will enable organization of collaborative undertaking:
  - Well defined starting point and shared understanding of the goals
  - Road map, tasks aimed at reaching the goals understood
  - Roles and stakeholder (actors) relationships understood
  - Data and information needs as well as communications defined
  - Supportive supervision and management presence ensured and accessible

6. Collaborative space and the key stakeholders in action

- **Key actors securing currentness of premises (data and information) for knowledge creation and maintenance of its validity –Thus, enabling efficient decision-making and action**


R&D
Policy Creator
Demonstrator
Policy Maker
Shared collaboration space
In action
Competent
Authority
Coordinating Body of Knowledge is
driving reformative action!
Coordinating Body of Knowledge is
Enabling transformative action!
Service
Provider
Technology
Provider
Operator

7. Closing remarks

- There is normally good cooperation at policy and strategy level, including R&D, development and demonstration of feasibility. Same is valid at operative level, between authorities, industry and infrastructure service providers.
- There is **lack of collaboration at strategy implementation level** between sectorial ministries and domain specific (CBRNE) disciplines and networks. Particularly, lack of coordination when assessing and developing capabilities to anticipate and when considering allocation of resource for preparedness.
- The proposed approach and technology solution enables to create a reliable **Body of Knowledge (explicit and tacit)**, which is readily accessible and available for use by all relevant stakeholders for timely decision-making and action.
- Availability of such a Body of Knowledge for practical use by the one responsible for decisions and for operations is essential for successful mitigation of risks and response. – Complex, evolving threat scenarios, imply necessity to pay attention to both ORGANIZATIONAL and ENABLING TECHNOLOGY resilience.
- Continuous validation of that Body of Knowledge is inherent quality of the process and imply evaluation also of the premises, **legacy and obsolescence** of the data and information the Knowledge is based upon. –This is to be understood as a maintenance routine.