Session III: Resilience, Information, and Cyber Security

Resilience: Cyber / Technology dimension

Dr. Velizar Shalamanov

Senior Researcher, Institute of Information and Communication Technologies, Bulgarian Academy of Science

Visiting Professor, Defense Staff College (2017/18)

ACERTA: Academic CERT Association

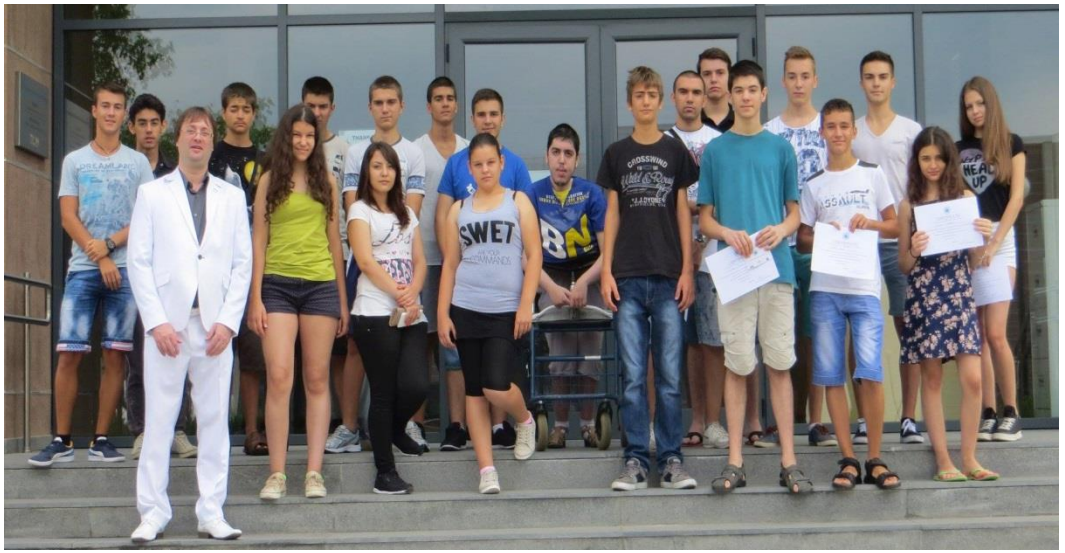
Roots of resilience related work till 2009 an beyond till 2014

1. Establishment of **SA Civil Protection** in 2000
2. **Scientific Coordinational Council** on Civil Protection in 2003
3. **White paper** on „Civil Prtotection“ to cover resilience in all critical areas – 2003/2004 with large **research program on building resilience** (incluing CIP)
4. **EU TACOM SEE** – 2006 and **IEMS / 112 ECS** - 2007
5. **ESRIF** 2007-2009
6. NATO/ACT CoE on **Defense Support to Civilian Authorities** as an instrument for improved resilience in 2008 (later CoE on CM and Disaster Recovery)
7. Introduction of **Cyber Reserve** in SCIS at MoD in 2013

Based on ESRIF ... EU Crisis Management: from 2011 ACRIMAS / DRIVER / DRIVER + to 2020, but real **turning point is 2014** for both NATO and EU

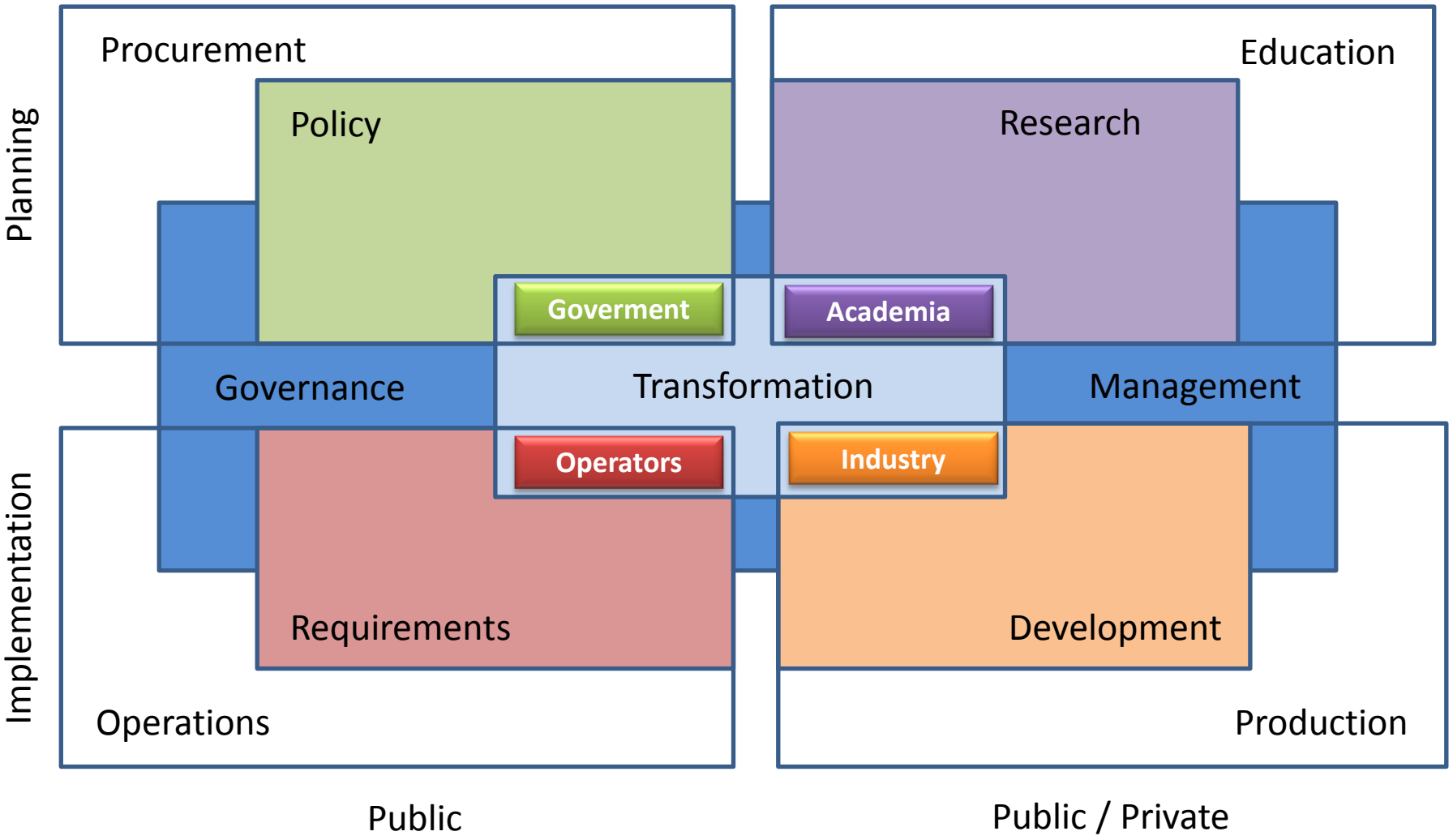
HPC Future Threats Modelling Cooperation (with ESGI, since 2012)

Young Researchers Cooperation with America for Bulgaria & AUBG (since 2005)



EU Network of Excellence on Cyber Security 2010-2014

Four dimensions of transformaiton in the area of resilience (cyber/technology field)



Framework for improvement

- NATO dimension and relations with EU / regional cooperation
  - Resilience Pledge
  - Cyber Defense Pledge
  - Parallel and Coordinated Exercises (PACE)
- **Vulnerabilities and Response** in Cyber / Technology fields for the structures:
  - Political: decision making / funding – strategy / action plan
  - Societal: awareness / understanding – public campaigns / high visibility exercises
  - Security: balkanization / sharing – consolidation / federation approach
- Nature of challenge (**ADKAR** as a method for change in Resilience area with focus on Cyber / Technology)
  - Low level **awareness** and understanding
  - Lack of firm **decisions**
  - Limited **knowledge** and **abilities** (capabilities)
  - **Reinforcement** mechanisms maturity (**risk** management)

Achievements since 2014 (turning point)

1. 2014: Approved MoD Cyber Defense Vision, first draft of **Cyber Security Strategy** „Cyber Resilient Bulgaria 2020“ (approved in 2016) and **Cyber resilience Adviser** to MoD established (**National coordinator on Cyber Resilience**)
2. 2016: E-Government law improvement to form **SA e-Gov**
3. 2017: **Cyber defense cell** established at SCIS for defense networks
4. 2018: **ACERTA** initiative for E2CR of ITO and CISO course of IPA, sponsored by SA e-Government
5. 2018: **Cyber security law** in the Parliament for approval
6. 2018: Project for **cyber security CoC** under OP “E&R for intelligent growth”
7. 2018: Initial capabilities of **Cyber/Resilience range** and application for **E**uropean network of **C**yber security centres and competence **H**ub for innovation and **O**perations – **ECHO** (H2020: **SU-ICT-03-2018)**
8. 2018: Participation in preparation of the second **PACE**
9. 2018: **National Cyber Resilience exercise** with focus on energy resilience, planned for the Autumn (ESI/CyRes Lab in lead with MoD and UK support)

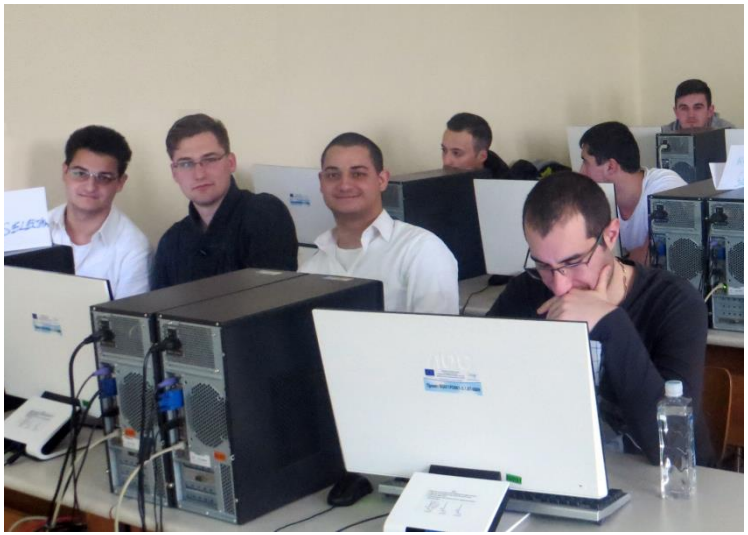
... and some more activites

1. NATO Cyber Coalition Exercise since 2012 as a partner and Cyber Europe Exercise - 2014, 2016
2. Leadership of the WIG on Information Warfare and Assurance (IST panel NATO STO)
3. Participation in Ad-hoc working group on R&T on Cyber Security (EDA)
4. 2016: National competition The Cyber Games in 2016 and 2017 https://thecybergames.net
5. 2016: NATO STO IST panel Research Symposium on Cyber Defence Situation Awareness and STO HFM panel „Human aspects of Cyber Security“
6. 2017: NATO STO Research Lecture Series in Cyber Security Science and Engineering (host) with Directorship of the whole lecture series (Washington, Bordeaux, Sofia, Budapest, Tallinn, Vancouver, ...)
7. 2017: NATO SPS project CyRADARS (https://cyradars.net) and NATO SPS ATC „Countering Terrorist Activities in Cyberspace“ (http://ebooks.iospress.nl/volume/countering-terrorist-activities-in-cyberspace)
8. 2018: EDA International conference on cyber defence Building a Rapid Response Sofia, Bulgaria (https://www.cybersec.events)
9. 2018: Development of the Taxonomy for Cyber Emergencies Management during the EU Presidency of Bulgaria

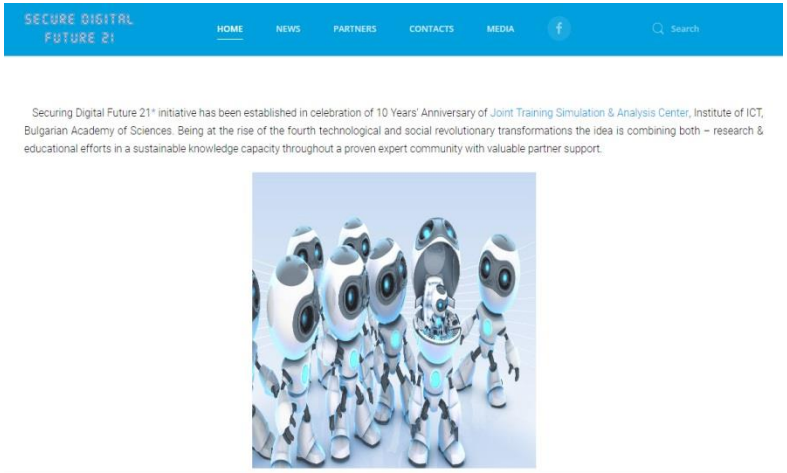
Concept validation & verification for the future

CYREX 2015

CYREX 2018

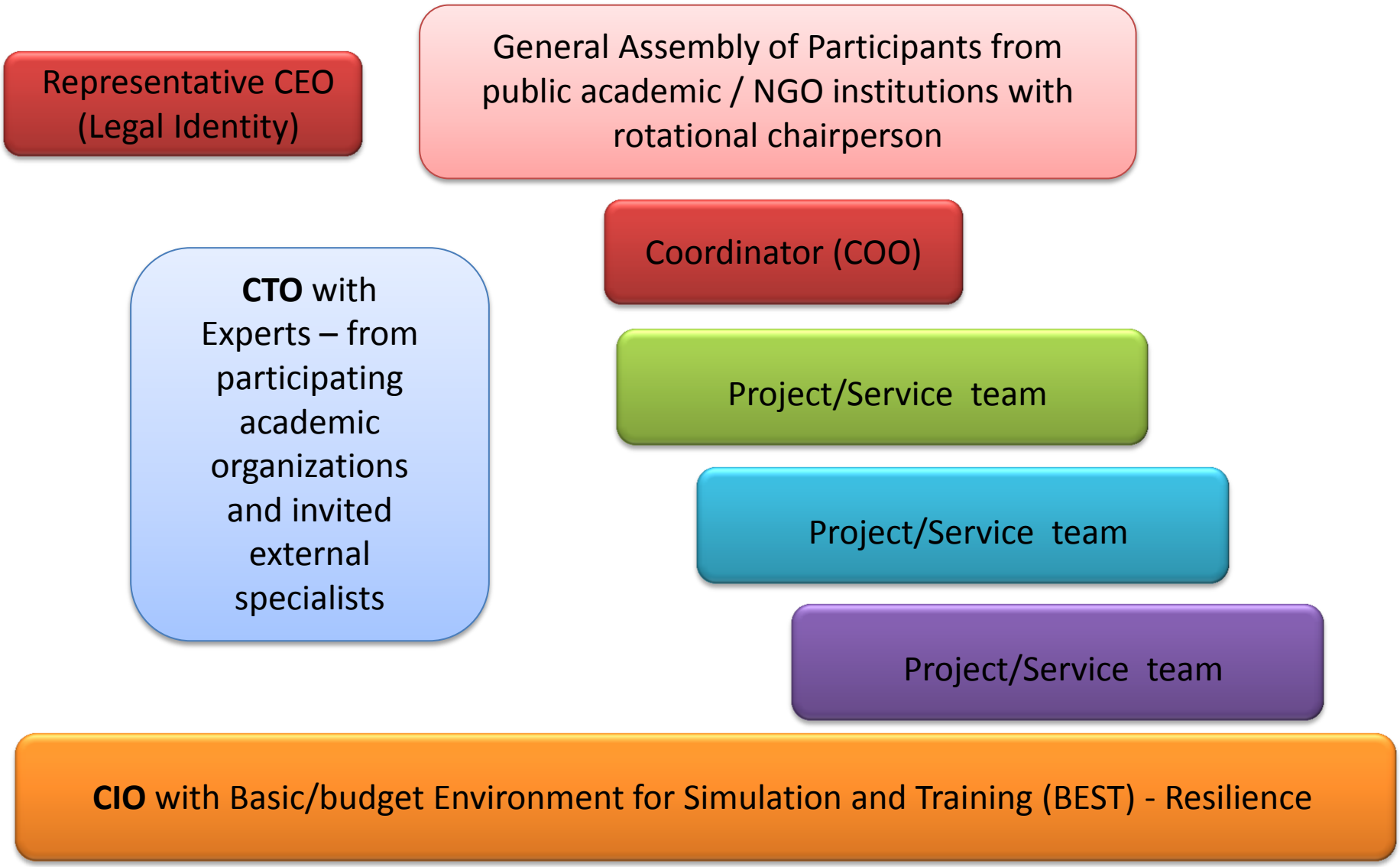


Future Digital Society Resilience 2018 -> 2028

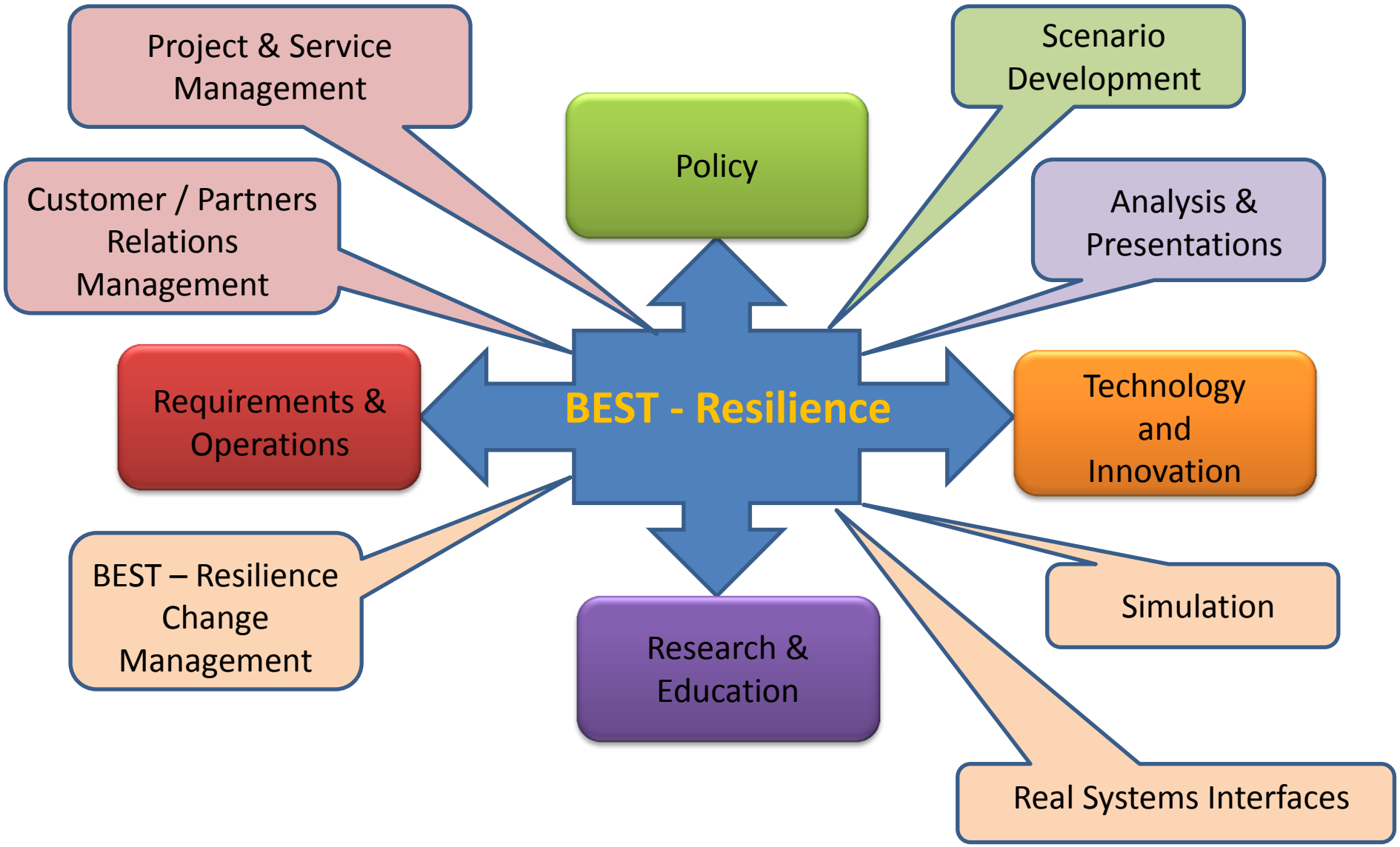


http://securedfuture21.net

Academic (Cyber) Resilience Services Organization (Academic CERT Association - ACERTA)

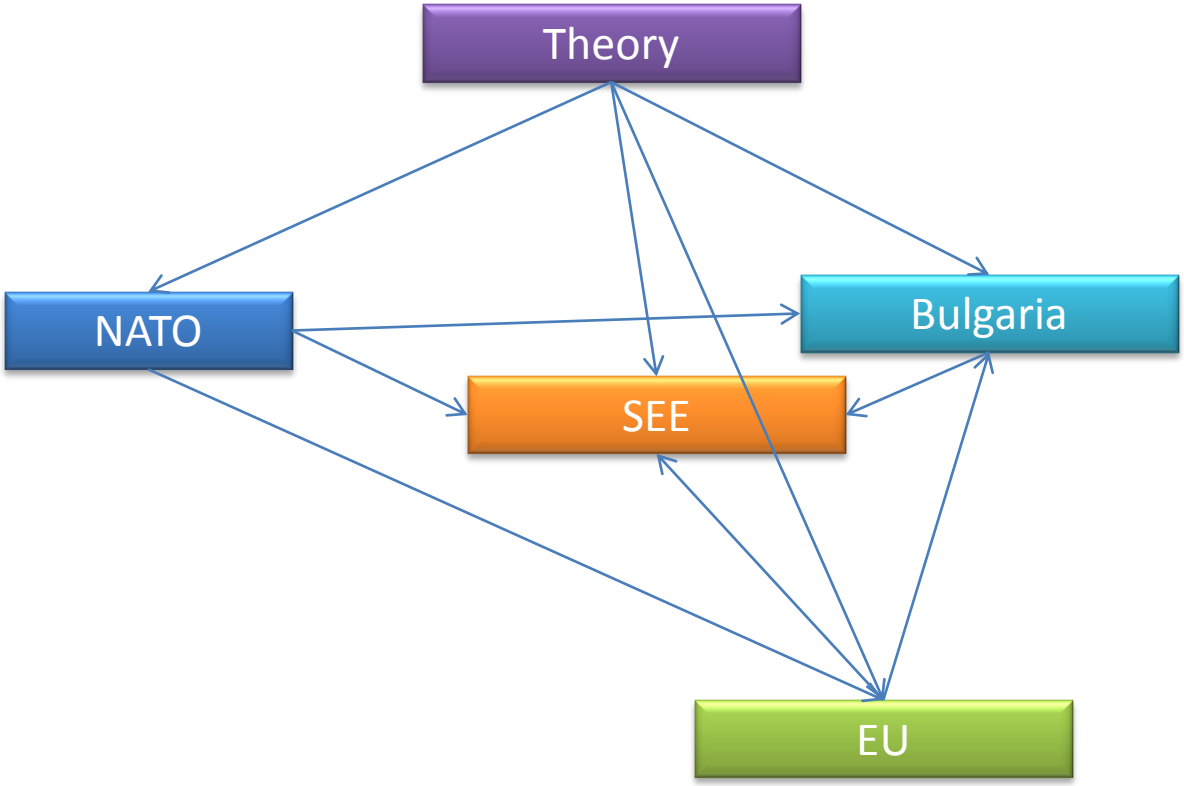


Basic Environment for Simulation & Training: „Resilience“

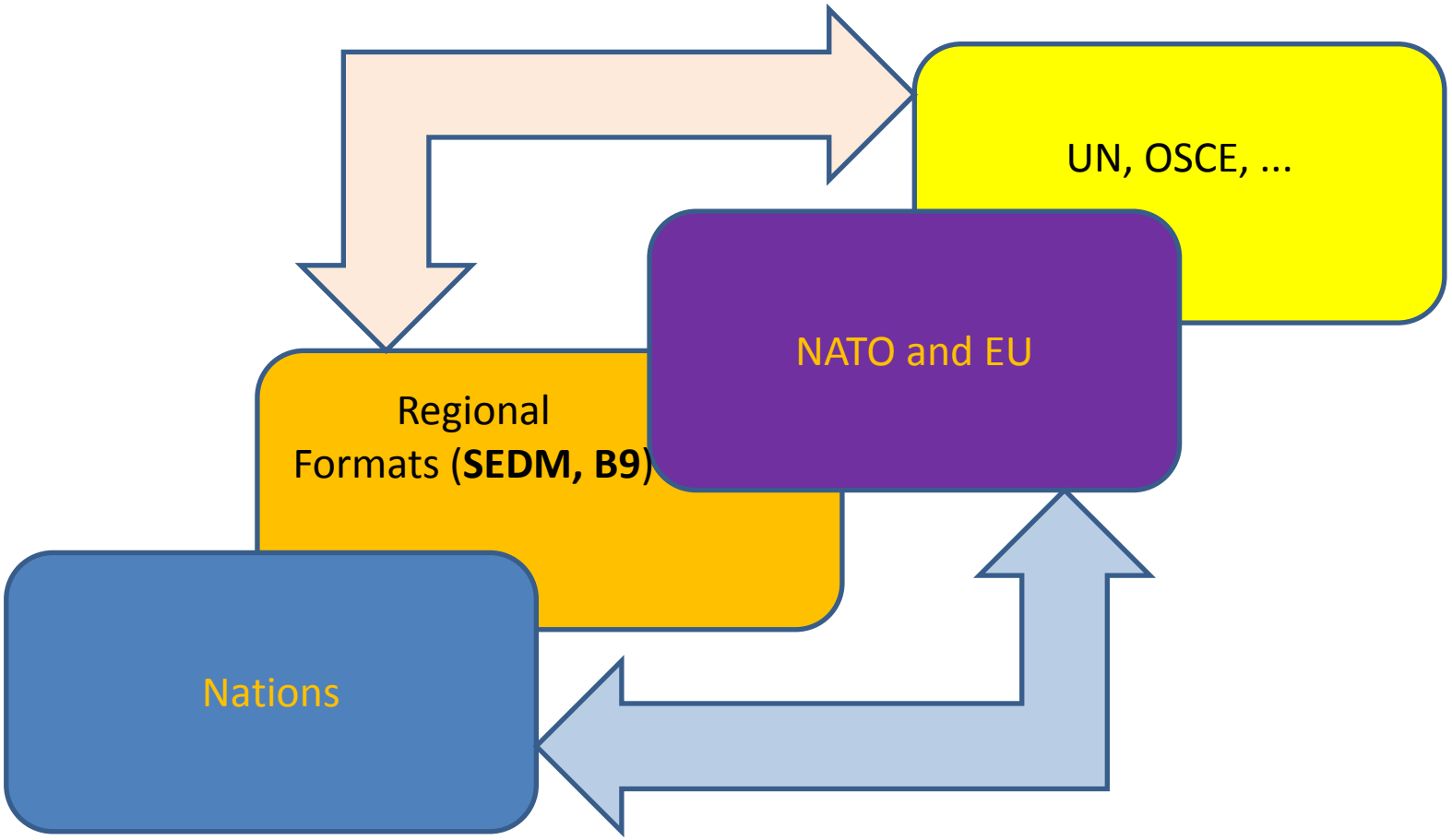


Balkans (10 countries) + Black Sea-Caucasus (4 more to the East)

Development of a model
„Bulgaria in NATO and EU with increased role in SEE“



„Vertical“ Roles in Regional Cooperation on Resilience



Lessons learned / identified

1. **Vision and strategy** are prerequisite for action.
2. Resilience requires **transformaitonal effort** with technology playing impoirtant role, but without changes of processes, organizaiton and development of people, the technology can‘t bring real positive change.
3. Resilience is a **leadership** issue and continuous effort of risk management is required.
4. Lack of **funded national action plan** is still the main show stopper, including for NATO/EU and regional cooperation.
5. Main challenge is the **consolidation** of national, even academic capacity for effective action.
6. Main shortage is **personnel** – qualified people to work on practical spects of cyber resilience.
7. **Partnership** „Government-Operators-Academia-Industry“ is still lacking dynamism, so need energy and regulation.
8. **Exercises** (open enough on one side and on the other in NATO/EU/regional format) are the key driver for change.
9. Main focus of the **hybrid warfare** is to reduce the resilience, so initial effort to broke this „spiral down“ is essential.