Appropriate Roles of the Military and Governmental Institutions in Protecting Cyber Aspects of Critical Infrastructure and Critical Information Infrastructure

Dr. Velizar Shalamanov
Assoc. Professor, IICT-BAS
20.04. 11:15 – 12:00

Agenda:

1. *Evolution of Cyber domain and Critical Infrastructure protection (CIP)*
2. *Stakeholders in Cyber domain and their role: NATO Cyber Defense Cooperation Platform*
3. *SEE cooperation in Cyber and CIP: Academia (IICT-BAS) role in cooperation with national IT organizations, NATO and EU*

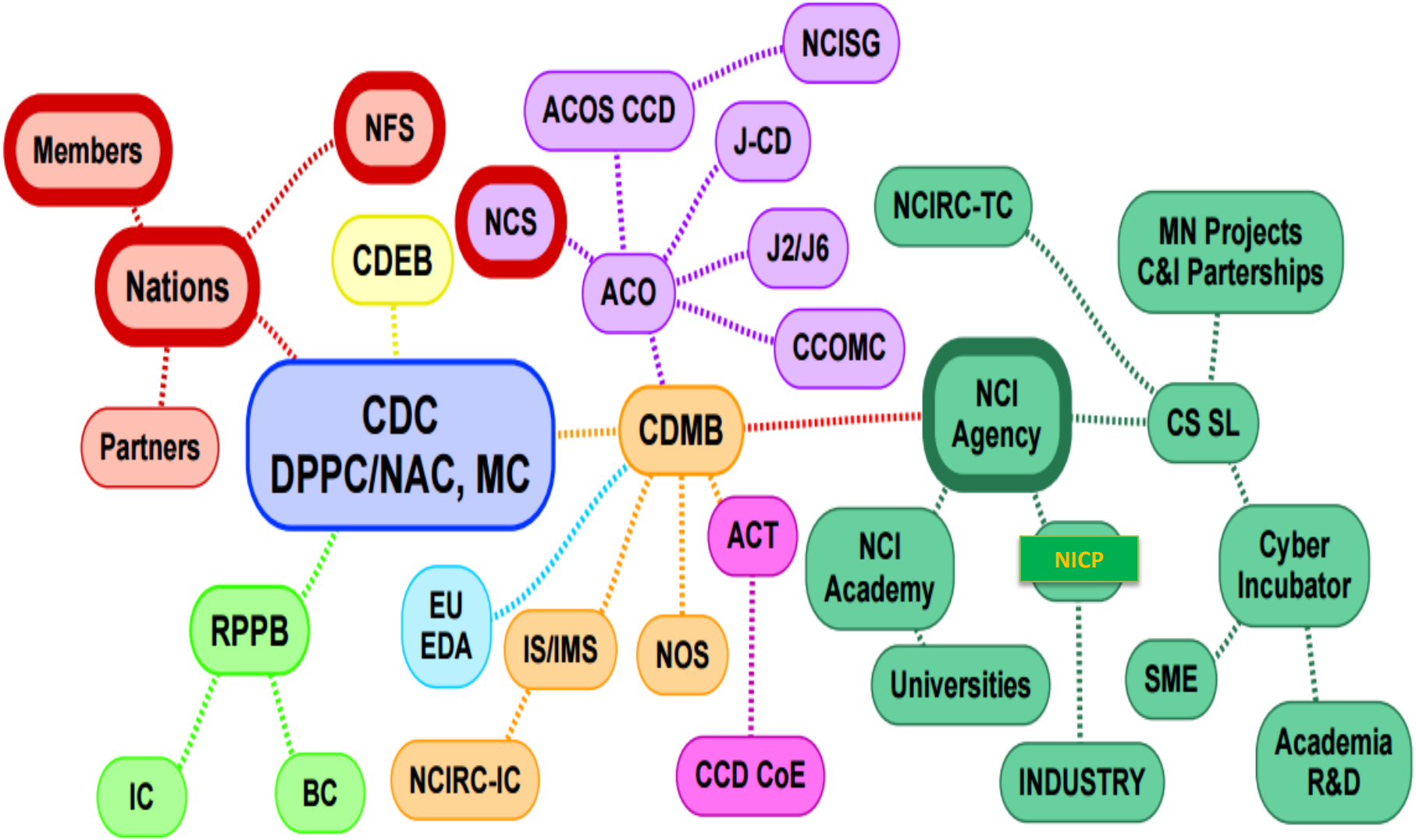
NATO as a reference model

1. NATO is the Nations, not above the Nations and is a consensus based organization
2. NATO is a confidence and a solidarity, based on an interdependence and shared values
3. Defense is the most critical infrastructure and Cyber is operations domain
4. NATO is an unique internaitonal organization with NCS, common funding for (infrastructure) capabilities and executive agencies
5. NATO is a reginal organization, but with global reach and partnerships (the core of all the free democratic nations)
6. Success of NATO is in the change management and interoperability (transformation)
7. Instrument of Change/Interoperability: From Marshall Plan to Mattis Plan (Cyber and CIP related aspects)

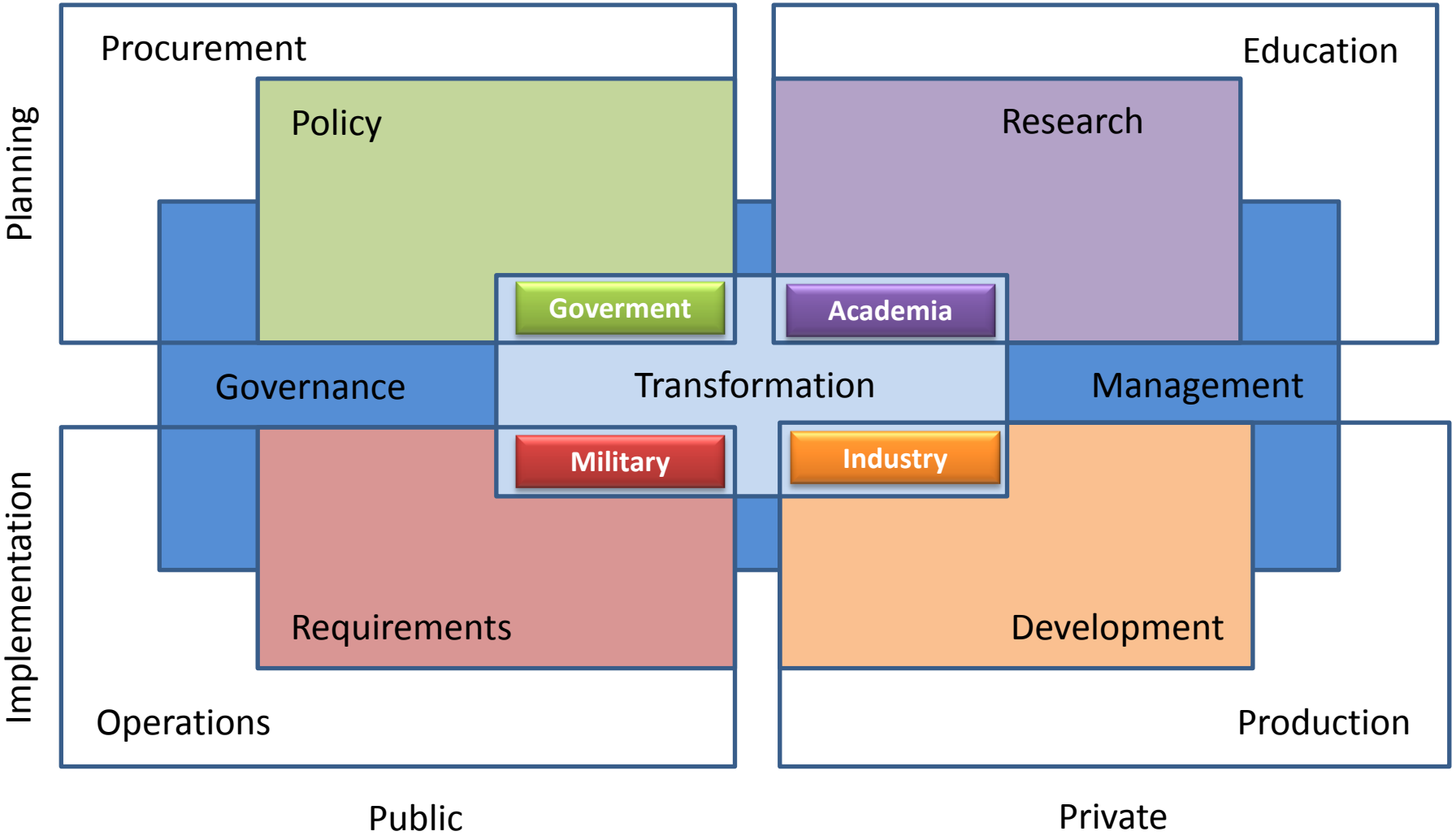
Evolution of Cyber domain and Critical Infrastructure protection (CIP) in NATO context

- Identify the topic (start in 2002, but practical actions mostly after 2007 cyber attacks in Estonia)
- Defining roles and responsibilities, key capabilities
- Cyber Defense Policy and Action Plan
- NATO Industrial Cyber Partnership
- Opertationalization of Cyber (2016) – **10 years**
  - Cyber as an Operational domain
  - Cyber pledge
  - From ASG ESC to ASG I&S
  - **Resilience pledge / NFIU-RAP**

Cyber Defence Stakeholders and respective Governance / Management Structure in NATO context

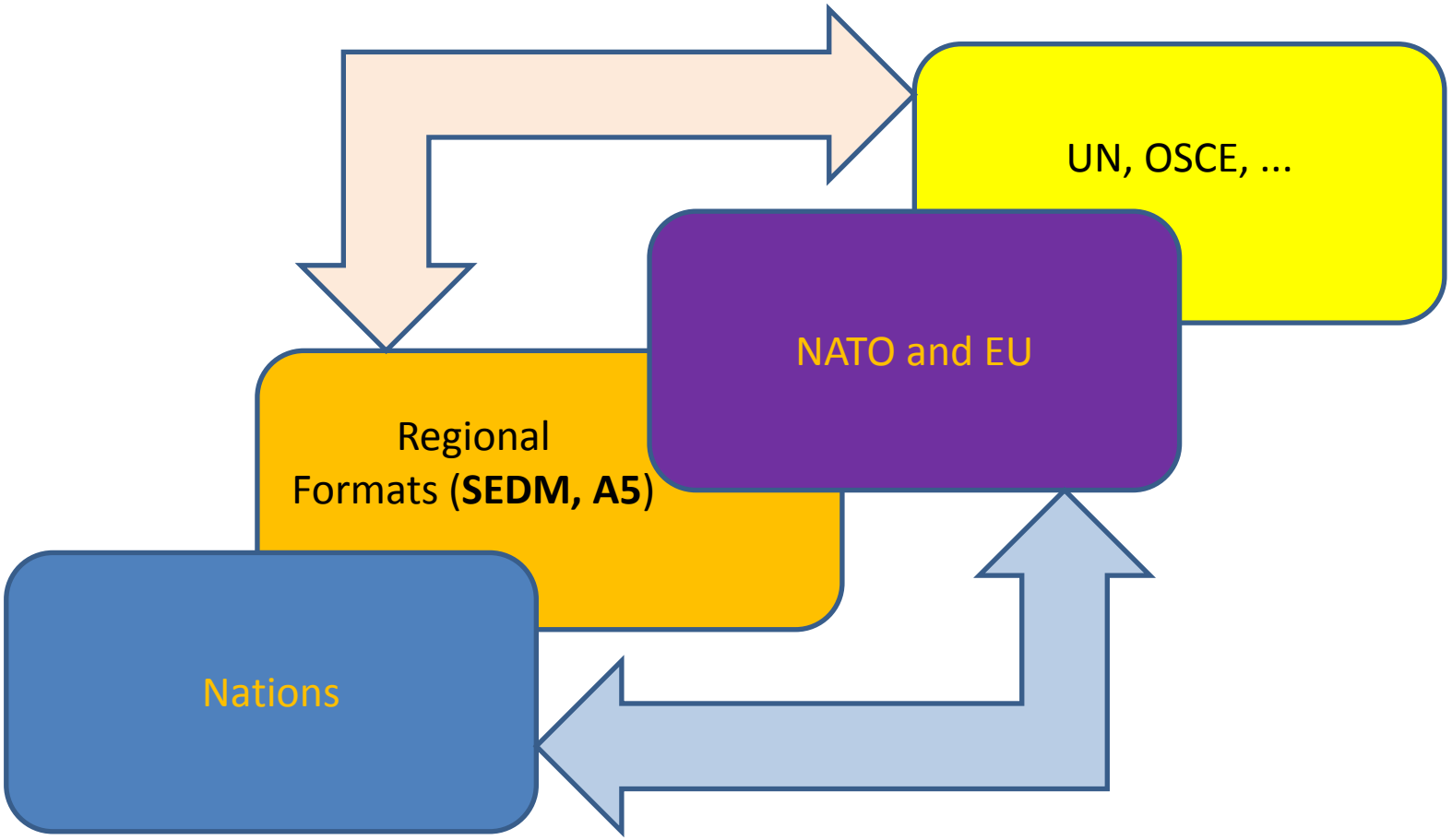


Appropriate Institutional Roles in Protecting Cyber Aspects of Critical Infrastructure

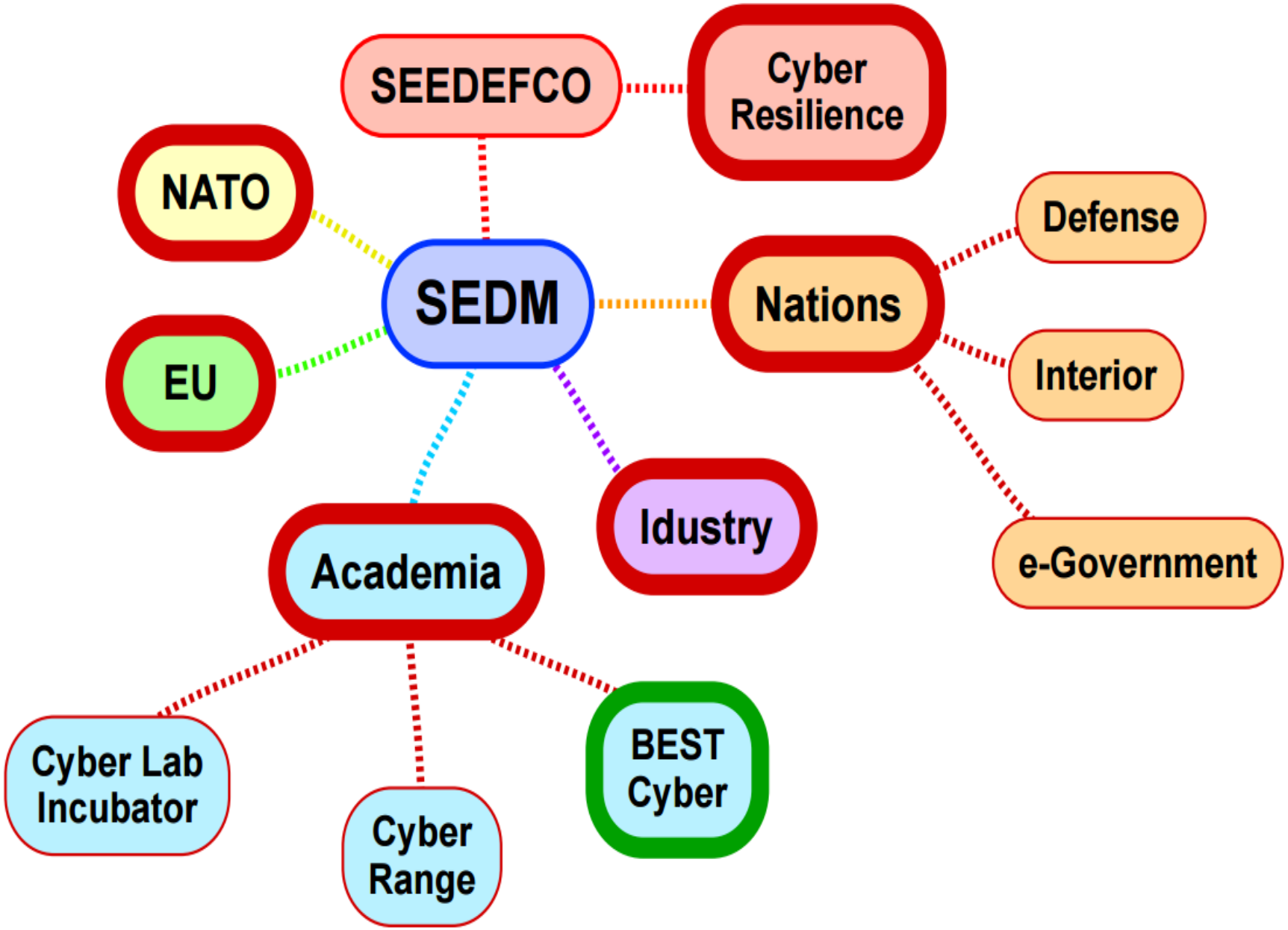


10 countries + 4 more to the East

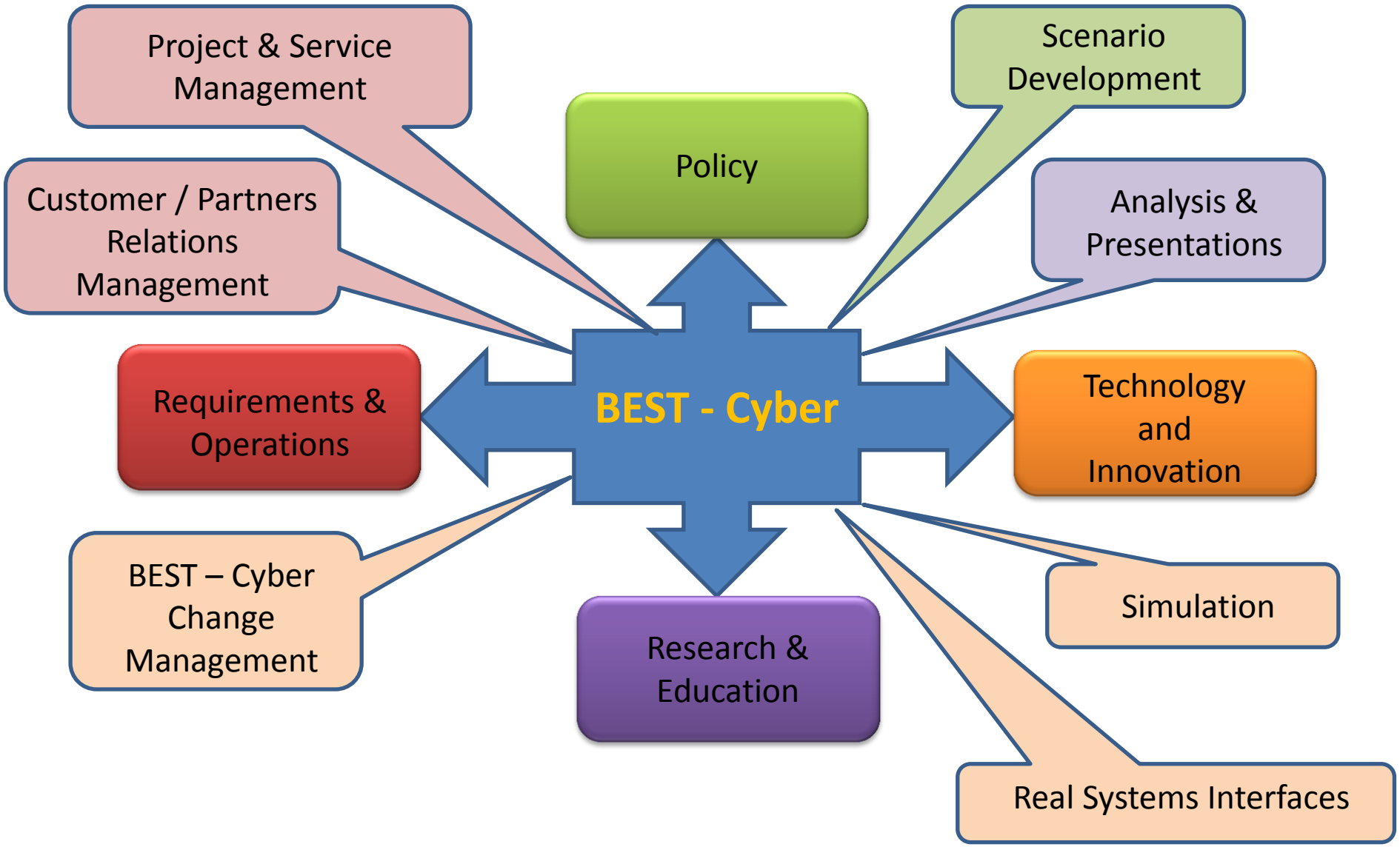
„Vertical“ Roles in Protection Cyber Aspects of Critical Infrastructure



Development of SEE Cyber cooperation and the role of Academia



Basic Environment for Simulation & Training - Cyber



Conclusions:

1. Cyber is a new domain for NATO (Warsaw Summit) but recognized by EU and all the members states, some of them well ahead in comparison of the consesnus based decisions in NATO.

2. Cyber Defense and Critical Infrastructure Protection are closely related. Cyber is the core of the protection from hybrid threats.

3. Governance and management in the area is esential, especially on alliance and regional level (in the framework of the leading alliances).

4. Responsibility stays with Nations (members, partners).

5. Colloboration between Military, Government, Academia and Industry is Essential on National level and in internaitonal context.

6. Innovation is a critical factor for superiority / dominance – best way to win in Cyber / CIP.

7. E&T is essential for success and Academia is playing pivotal role.

Next steps?

1. National self-assessment of the maturity and roadmap for improvement as part of the „Mattis Plan“ in Cyber/CIP domain (in NATO context or / and in EU context)
   - Funding
   - Capabilities
   - Operatioins
2. SEDM development of SEEDEFCO with Cyber / CI Resilience for SEE project in NATO/EU context
   - Cyber/CIP awareness – public and institutional
   - Training and Reserach: CIO/CISO institutionalization (best practices / compliance)
   - Exercises: BEST-Cyber/CIP for SEE (example of EU TACOM 2006 in Cyber domain for 2018/19)
3. NATO/PESCO and defense Innovation Greenhouse in the Hague / NCIA,TNO-DR
   - SEE consolidation of Cyber / CIP capability development cooperation
   - Participation in DIG and related initiatives for innovation in Cyber/CIP
   - Harmonization of NATO projects and PESCO in SEE with partners