Cybercrime@EAP III

Արևելյան Գործընկերություն
Східне партнерство Eastern
Partnership აღმოსავლეთ
პარტნიორობა Parteneriatul Estic
Şərq tərəfdaşlığı Partenariat
Oriental Усходняе Партнёрства

3608_30 Cooperation memorandum: Support to Internet Governance Forum 2017 Ukraine

6 October 2017, Ukraine
Provided under the Cybercrime@EAP III project

Cybersecurity and Cybercrime

Discussion points

In the strategy development phase the main discussions and decision points are:

- What should be the aim (purpose) of the national cyber security strategy
- What are the needs, goals and legislation of different stakeholders and how to share responsibility

The necessity of a National Cyber Security Strategy

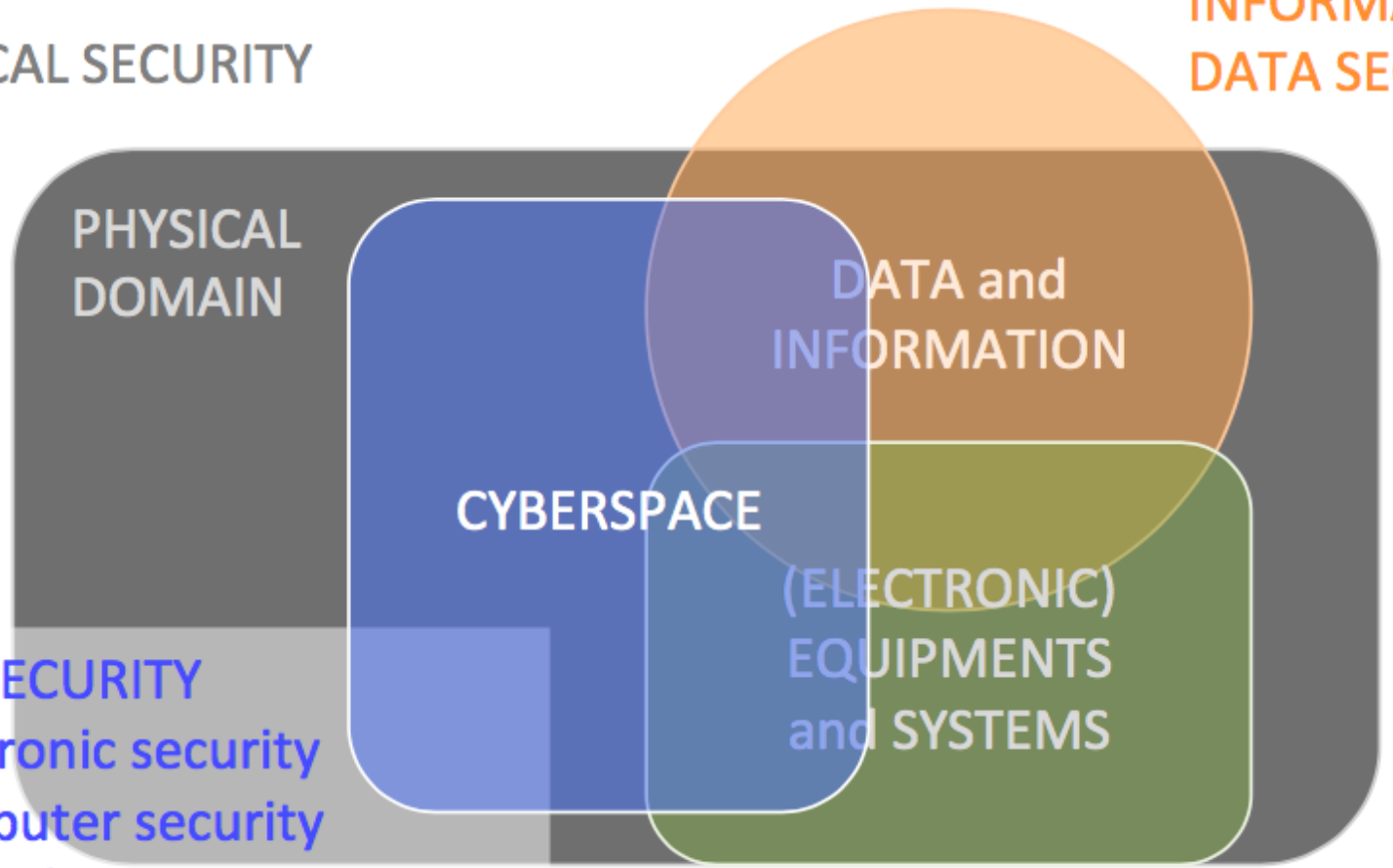
- Providing an open, reliable and secure cyberspace for activities and social interactions (including human rights); the economies and all national systems largely depend on application of information and communication technologies;
- The rise in the use of the IT systems increases the risk of abuse and emergence of new more sophisticated types of cybercrime, which makes the cybercrime one of the more serious threats to national security;
- Developing a cyber defense policy;
- Establishing an integrated, multidisciplinary approach to secure closer cooperation and coordination between the defense department, institutions involved in the combat against crime, private sector, and other relevant stakeholders;

The necessity of a National Cyber Security Strategy

- Strengthening the operational capacity, coordination and cooperation among the relevant institutions involved in the combat against cybercrime;
- Establishing common standards, training, and education of all institutions involved in the development of cyber security;
- Strengthening the national capacities for prevention and protection against cyber attacks, as well as implementing a campaign to raise cyber attack awareness.

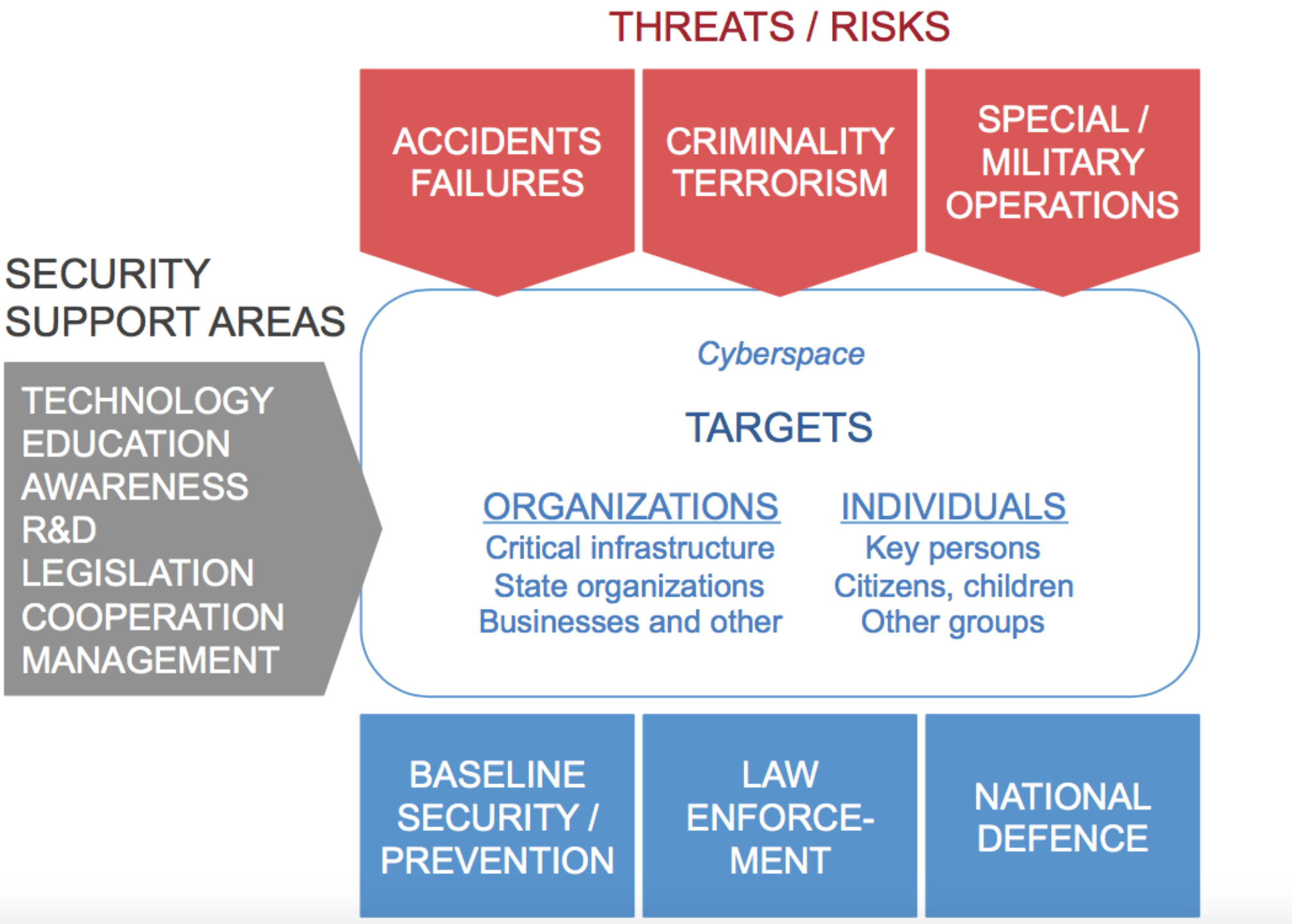
Cyberspace

- Physical security
- System security
- Data and information security
- **Cybersecurity**



CYBER SECURITY

- Electronic security
- Computer security
- ICT and IT security
- Partly information security
- Partly physical security


THREATS / RISKS
ACCIDENTS FAILURES
CRIMINALITY TERRORISM
SPECIAL / MILITARY OPERATIONS
SECURITY SUPPORT AREAS
TECHNOLOGY
EDUCATION
AWARENESS
R&D
LEGISLATION
COOPERATION
MANAGEMENT
Cyberspace
TARGETS
ORGANIZATIONS
Critical infrastructure
State organizations
Businesses and other
INDIVIDUALS
Key persons
Citizens, children
Other groups
BASELINE SECURITY / PREVENTION
LAW ENFORCE-MENT
NATIONAL DEFENCE

Cybersecurity model

- The **threat based approach** means that the strategic center of gravity is on the treats.
- The **target-based approach** means that the strategic center of gravity is on the targets – organizations, critical infrastructure, businesses, individuals, children, etc.
- The **security areas-based approach** means that the center of gravity is on the security areas – baseline security, law enforcement and national defense.
- The **security support areas-based approach** means that the center of gravity is on the security support areas – technology, education, awareness, R&D, legislation, international cooperation and management.

Structure and content of a fully- fledged Cyber Security Strategy

Description of the environment
1. Cyberspace
2. Society's dependency
3. Opportunities
4. Threats
5. Trends

Goals and objectives
1. Principles
2. Vision
3. Mission
4. Goal of the strategy
5. Objectives

Measures
1. Areas of activity
2. Measures
3. Implementation

Administrative aspects
1. Executive summary
2.Relationships with other strategic documents
3. Overview of a current situation
4. Cost of the strategy
5. Super vision of implementation

Scope of the cybersecurity

- Cyber prevention
- Cyber crime
- Cyber defense

- The general cyber security support areas at the national level are:
  - **Technology**
  - **Education**
  - **Awareness**
  - **Research and development**
  - **Legislation**
  - **International cooperation**
  - **Management**

Challenges

1. Defining the main definitions, scope and relationships (conceptual basis)

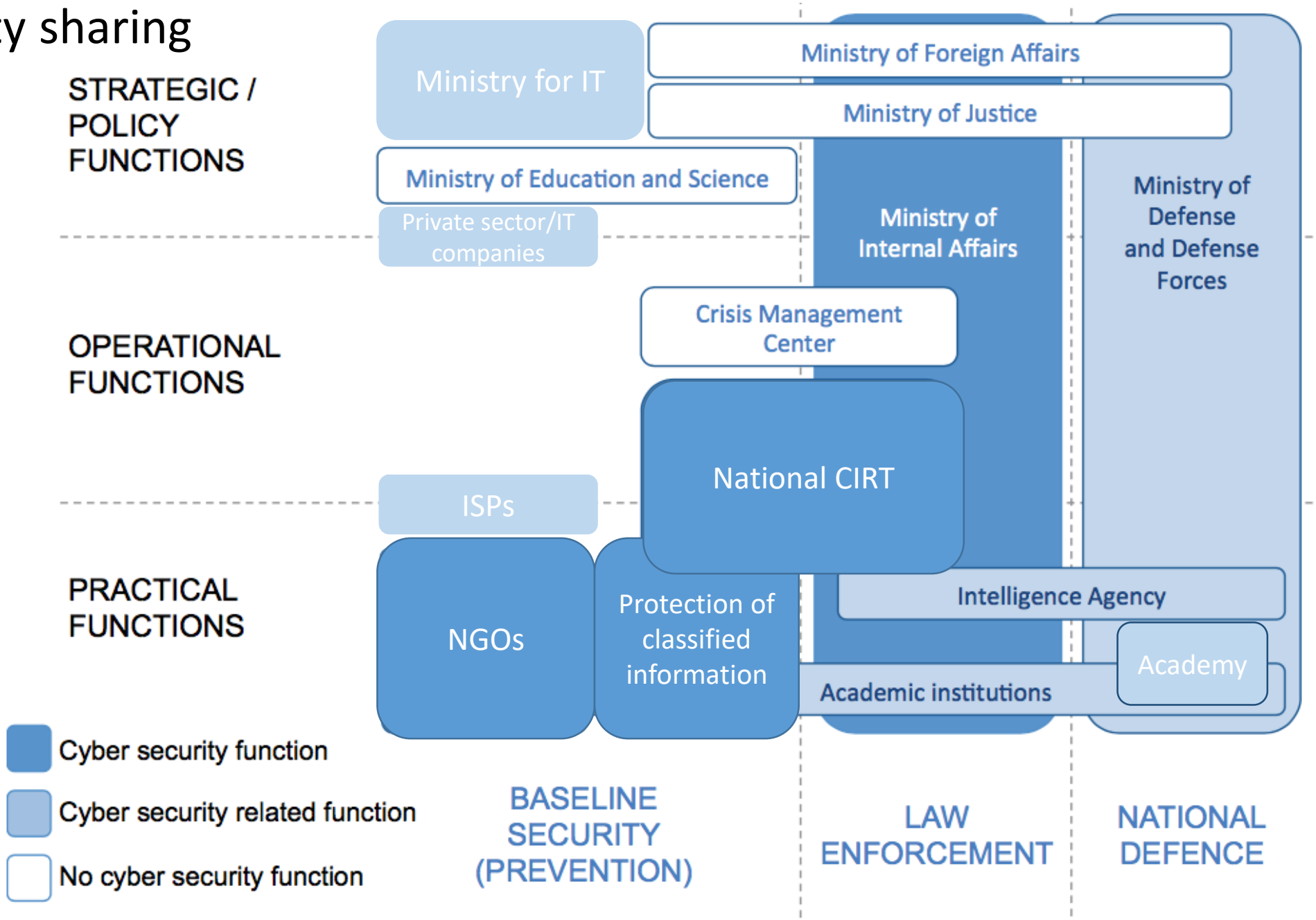
2. Defining the interests, needs and strategic goals

3. Defining the threats, risks and problems

4. Defining the security solutions / measures

5. Defining the constraints, restrictions and their impact (feasibility)

Responsibility sharing

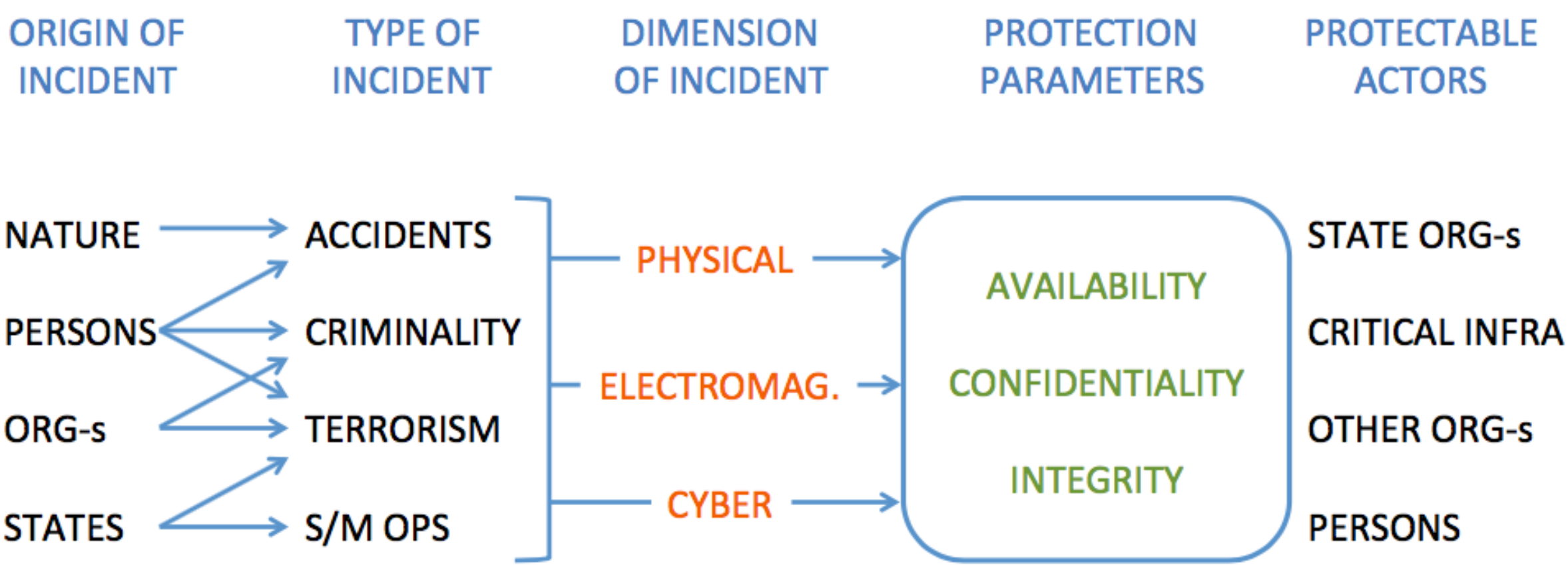


Main issues

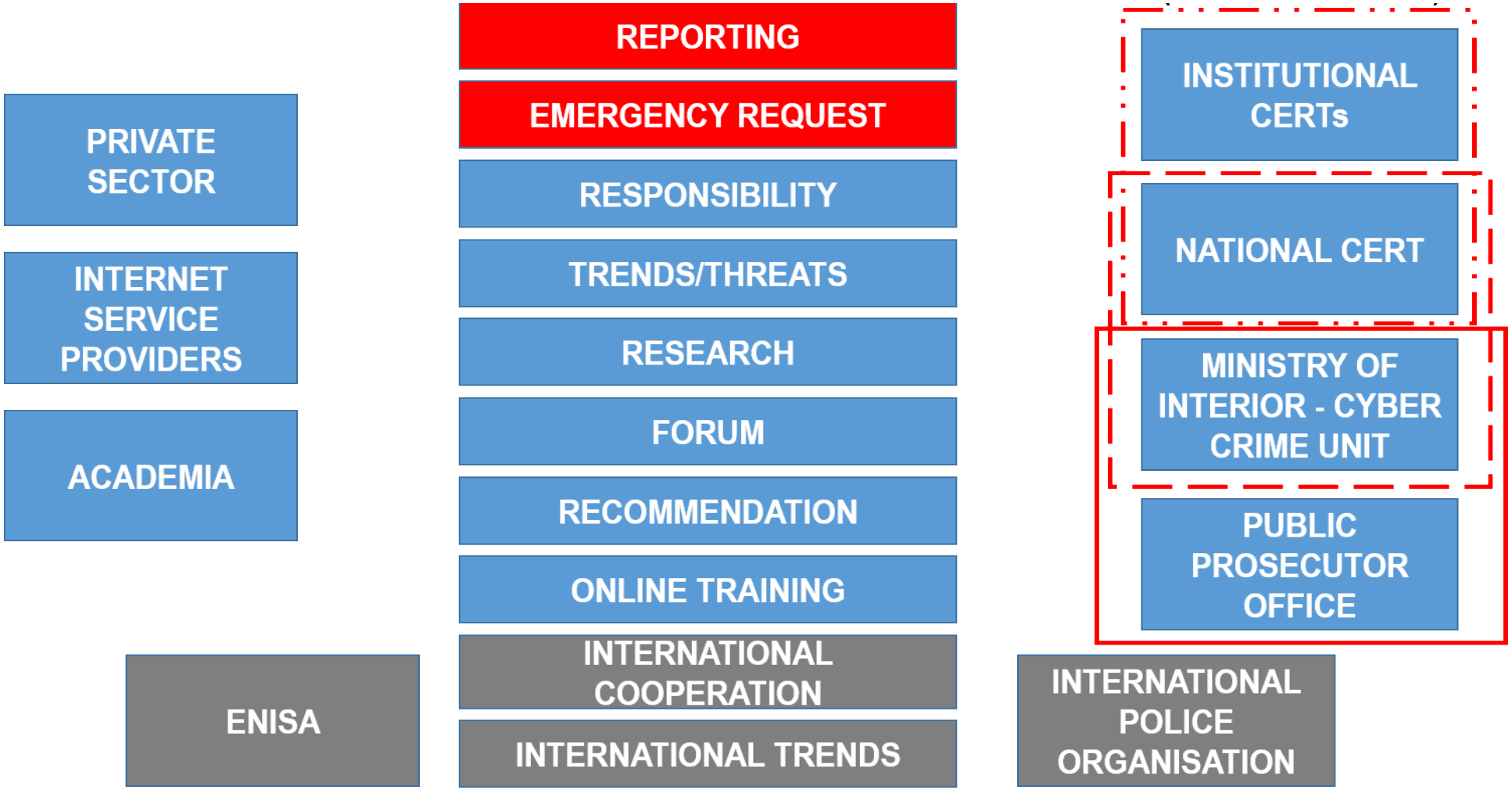
The most important issues regarding the strategy development are:

1. How to understand the difference between threats, risks and problems/challenges
2. How to develop a relevant threat picture
3. How to share important security information publicly

cyber security **threats and risks** analysis



Interagency cooperation



Questions