Methodology for Assessing Vulnerabilities and Planning Measures for Protection of Critical Infrastructures

Dr. Todor Tagarev
ICT Fair for Trust & Security Research
Olomouc, Czech Republic
14 May 2009

Dr. Todor Tagarev

- Associate Professor
- Information & Security Department
- Institute for Parallel Processing
- Bulgarian Academy of Science
- www.caxbg.com/is
- E-mail: tagarev [at] bas [dot] bg

Recent studies

- 2005: General/ framework methodology; Interagency Commission for Protection of the Population in Emergencies
- 2006: Critical Information Infrastructure Protection, State Agency for Information Technologies and Systems
- 2007: Critical infrastructures at municipal level, Ministry of Emergencies

Publications

- Todor Tagarev and Nickolay Pavlov, “Planning Measures and Capabilities for Protection of Critical Infrastructures,” *Information & Security: An International Journal* 22 (2007): 38-48, http://infosec.procon.bg

CIP definition

- BGR Law on Crisis Management
- A set of assets, services and information systems, whose failure, impediment or destruction would have a grave and harmful impact on public health and safety, environment, national economy or the proper functioning of government

Decision making process

- Analysis and assessment:

1. Sector analysis: Identification of the main sectors, sub-sectors and assets of critical infrastructure and determination of the most critical among them
2. Identification, characterization, and evaluation of threats to the critical infrastructure

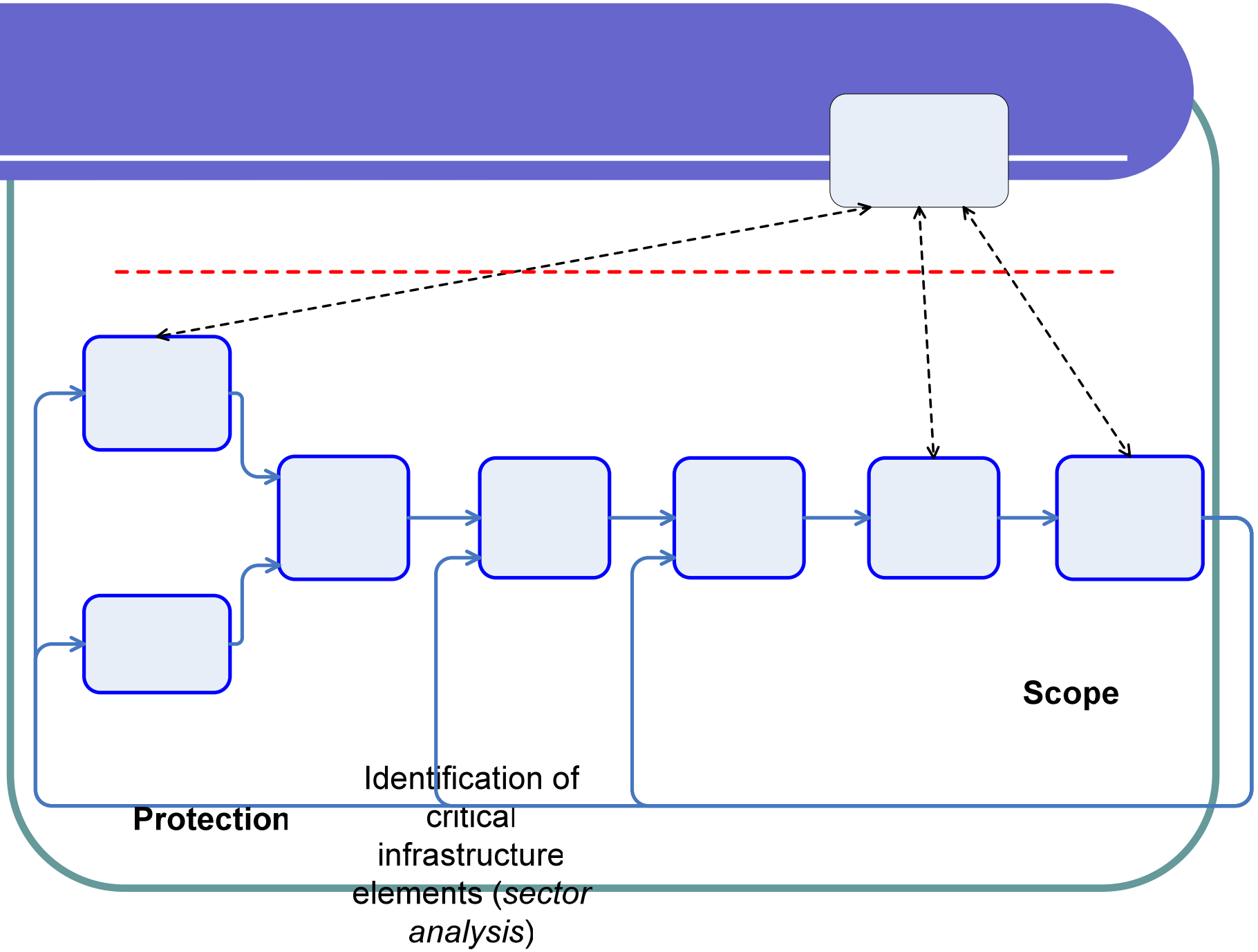
Decision making process

3. Vulnerability assessment
4. Assessment of *interdependencies* among subsystems and infrastructures, identification of those that potentially lead to cascading effects
5. Risk assessment

Decision making process

- Identification and prioritisation of risk mitigation strategies and measures:

1. Elaboration of a critical infrastructure protection strategy
2. Elaboration of a set of measures and capabilities for critical infrastructure protection and risk mitigation in the framework of the strategy


Scope
Identification of critical infrastructure elements (*sector analysis*)
Protection

Methods

- Treat critical infrastructure as a complex adaptive system
- Critical infrastructure models
  - Architectures
  - Agent-based models
  - Complemented by integration of expert assessments, including group decisions, e.g. made by participants in games, computer-assisted exercises and simulations

Value

- Transparent distribution of public and private resources in order to enhance the security of critical infrastructures, with solid understanding of the potential consequences

Importance for the ICT audience

- Understanding/studying the potential impact of IS/network vulnerability in a broader security framework
- Better understanding of criticality
- Supporting decisions to invest in protection measures
- Supporting decisions to invest in R&D
- Designing experimentation & demonstration projects/activities