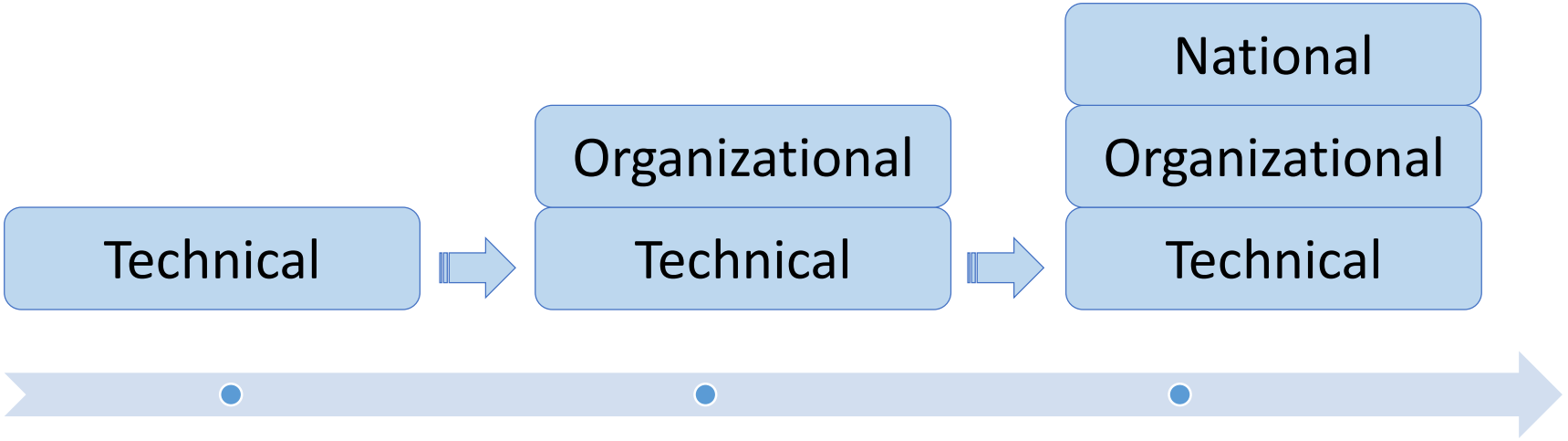
A Conceptual Nationwide Cyber Situational Awareness Framework for Critical Infrastructures

Hayretdin Bahşi, Olaf Manuel Maennel
Centre For Digital Forensics and Cyber Security
Tallinn University of Technology

Evolvement of Cyber Security



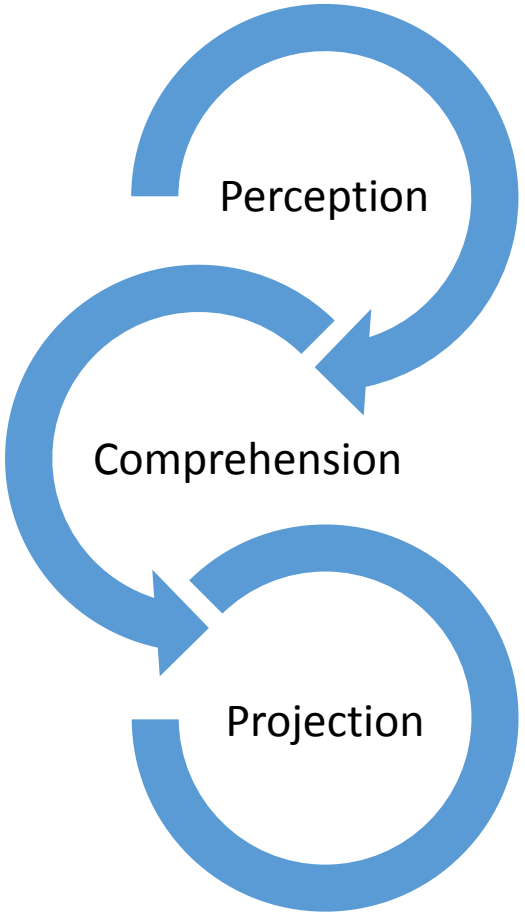
Cyber Security of Critical Infrastructures

- National security vs cyber security
- Physical effects of cyber threats
- Dependencies among national infrastructures
- Cascading effects
- Targets of various hacker groups including state sponsored ones

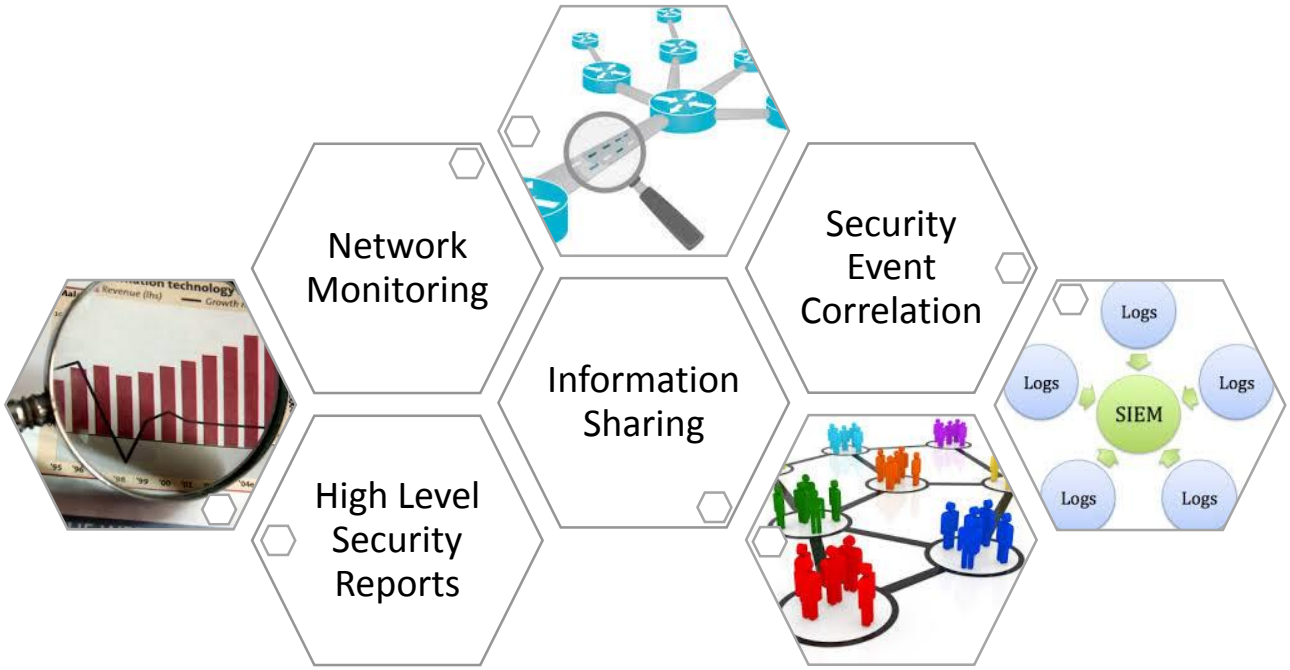
What is Situational Awareness (SA)?

Endsley's Definition

"The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future"



Different Interpretations of Cyber Situational Awareness



Cyber Situational Awareness at National Level

- Situational awareness and national strategies
- National CERTs to national cyber security operations
- Capability imrovement beyond of incident response
- Threat monitoring systems
- Information sharing

Objectives of Nationwide Cyber Situational Awareness

Risk Assessment Support

- Threat
- Vulnerability
- Bussiness
- Benefit from Safety Domain

Support for Different Decision Making Levels

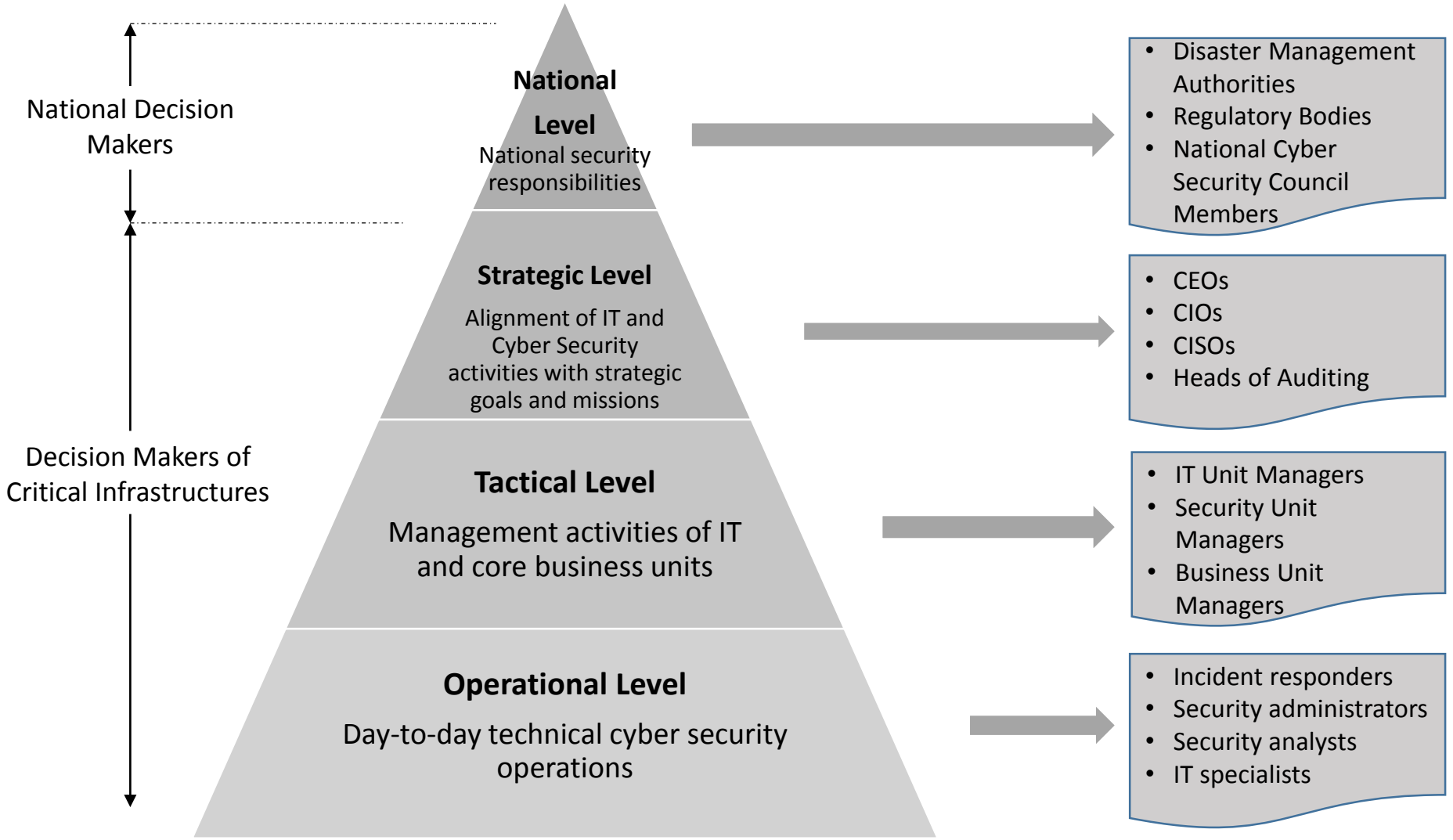
- National
- Organizational

Nationwide Analysis

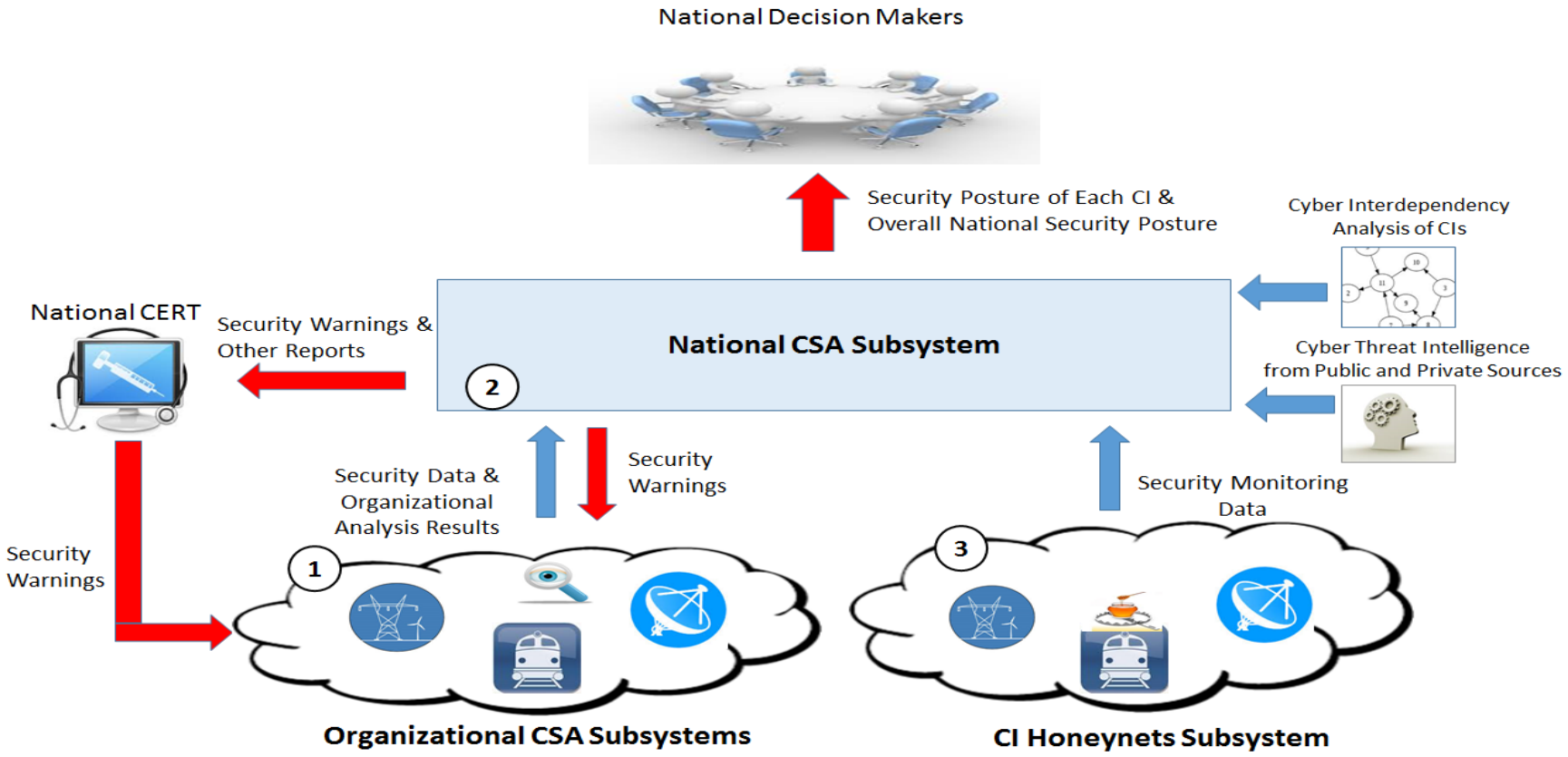
- Dependencies among different CIs
- Detection of coordinated attacks

Conceptual Nationwide Cyber Situational Awareness Framework

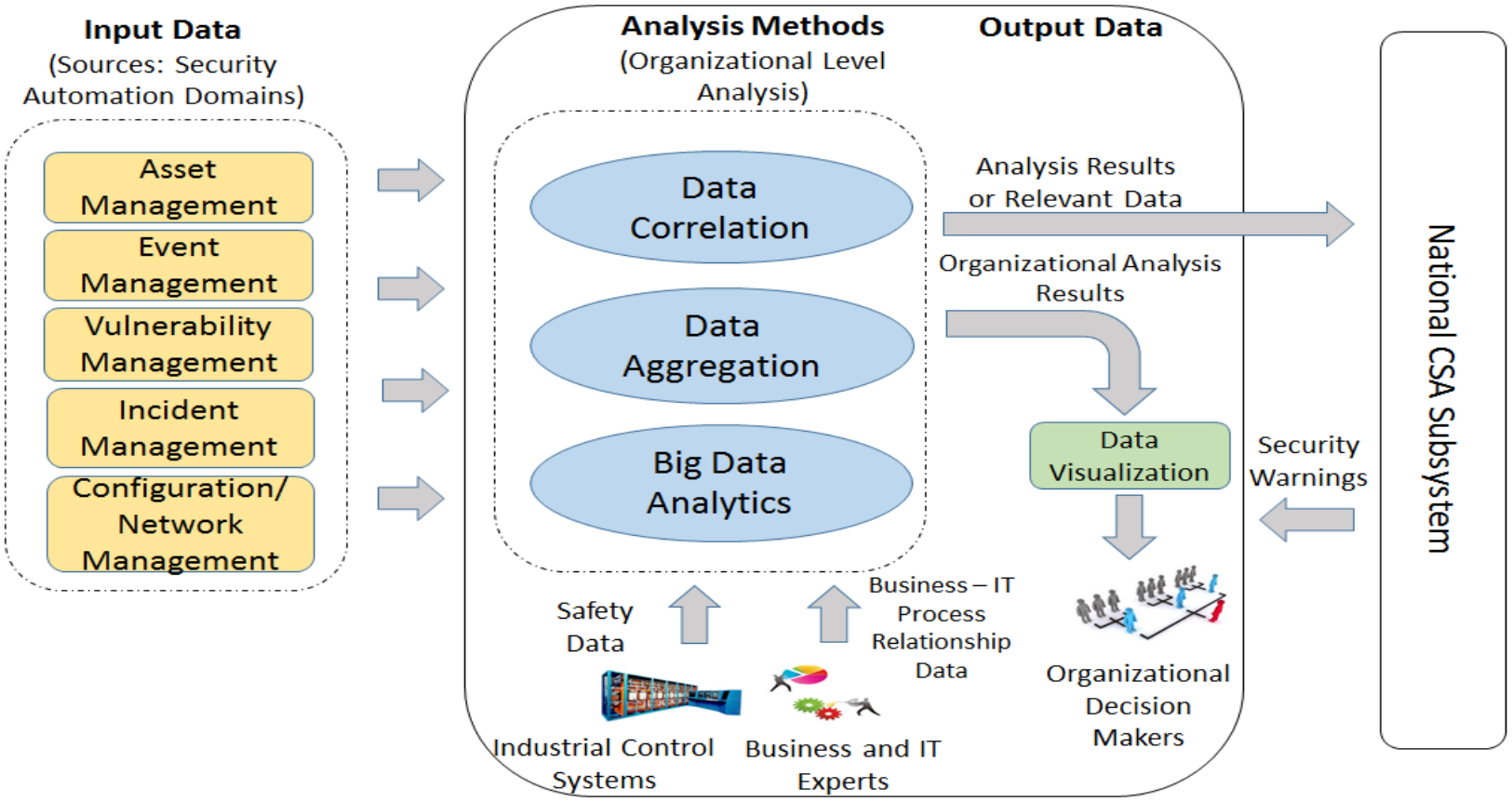
Decision Making Hierarchy



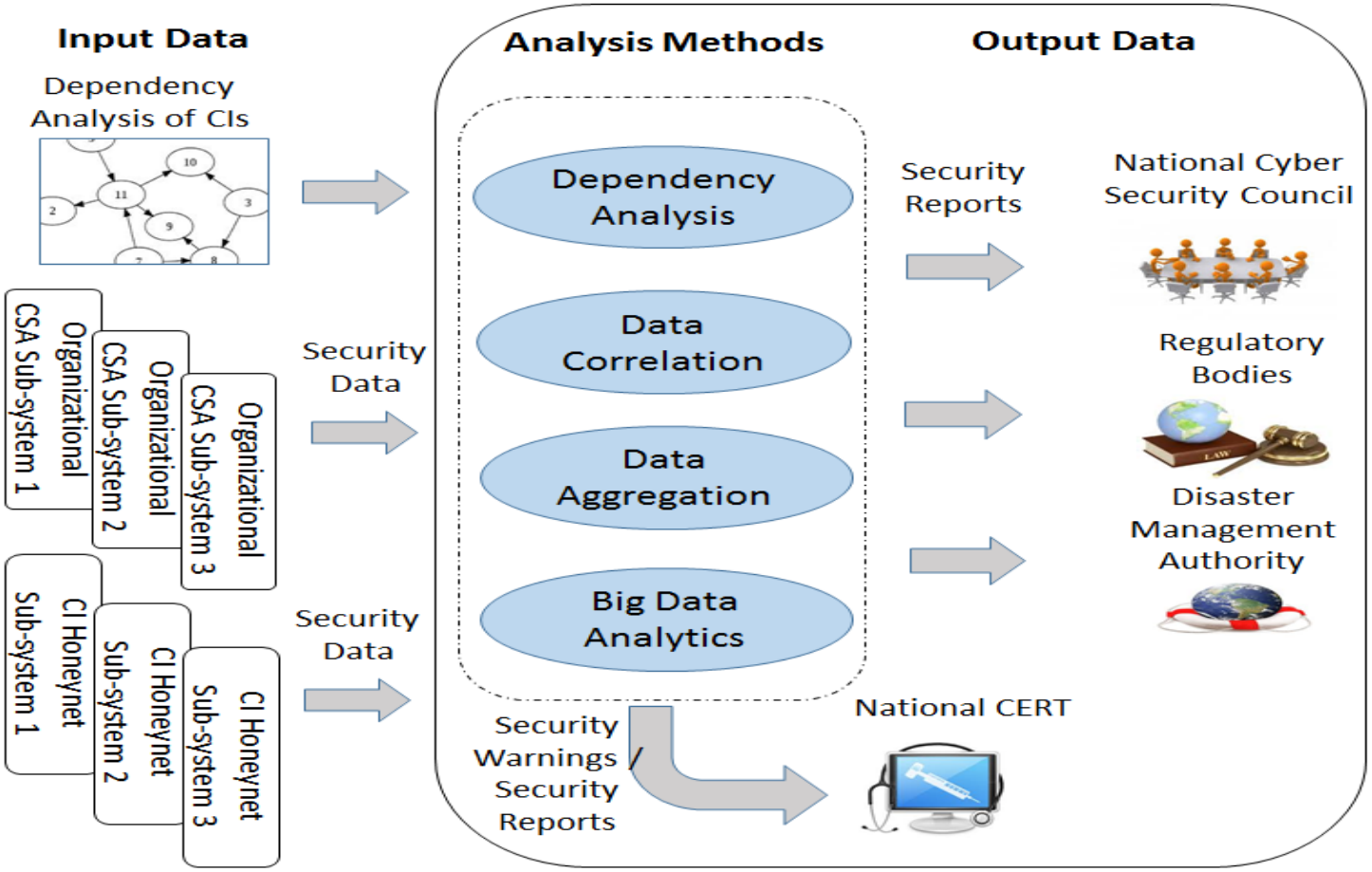
General View of Subsystems



Organizational CSA Subsystems



National CSA Subsytem



Research Agenda