CATS
Center for Asymmetric Threat Studies

*The Finnish Parliament Hearing*

# Cyber Security Challenges



*Helsinki*

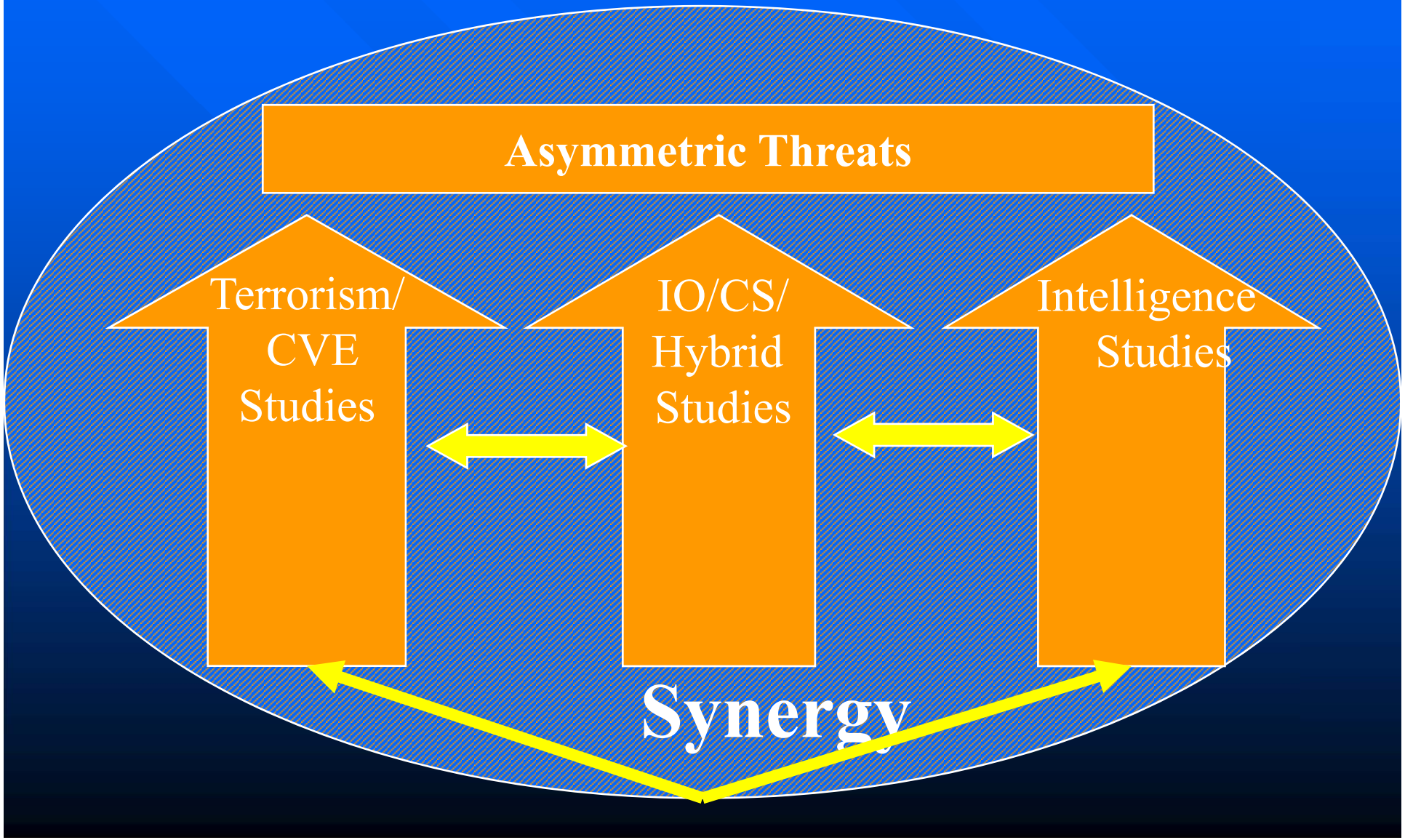
*9 May 2018*

**Dr. Lars D. Nicander, Center for Asymmetric Threat Studies, Swedish National Defence College**

SWEDISH DEFENCE UNIVERSITY

# CATS

## Center for Asymmetric Threat Studies



# Questions

1. How significant and imminent are cyber risks or threats, and to what extent are they a (national) security problem? What could be the worst, and what the most likely scenario?
2. Which objects or targets are most threatened by cyber-attacks? Is it more about disrupting infrastructure or about illegal access to information?
3. What does that mean in particular for a national cyber security/cyber defence structure?

# Threat context

- How significant and imminent are cyber risks or threats, and to what extent are they a (national) security problem?
  - "Total Defence" heritage
  - "Secure Market Place"
  - Estonian lessons (see pic)
  - Not Cyberwar but Cyber Deterrence (Stuxnet the highest level)
- What could be the worst, and what the most likely scenario?
  - Information breakdown of CI (interdependence Power-Telecom)
  - Digital espionage

# Specific threats

- Specific threats
  - Russian hybrid threats
    - » Espionage
    - » Influence Ops - Hack´n Leak
    - » Wartime preparations on criticial information infrastructure + ”Lawfare”
  - China
    - » Espionage (Cloud Hopper)
    - » Subtle intel ops for economic or R&D-purposes – mostly not illegal – SIGINT, students etc
    - » Hardware issues (Huawei and ZTE)

# Targets

- Which objects or targets are most threatened by cyber-attacks?
  - See pic
- Is it more about disrupting infrastructure or about illegal access to information?
  - The latter

# Prepardness

- Are state authorities in general prepared for cyber espionage, cyber terrorism and cyber operations?
  - No, NPM and outsourcing haven´t been balanced with proper Information Assurance
  - Split government responsibilities without oversight and coordination
    - » Situation awareness is missing

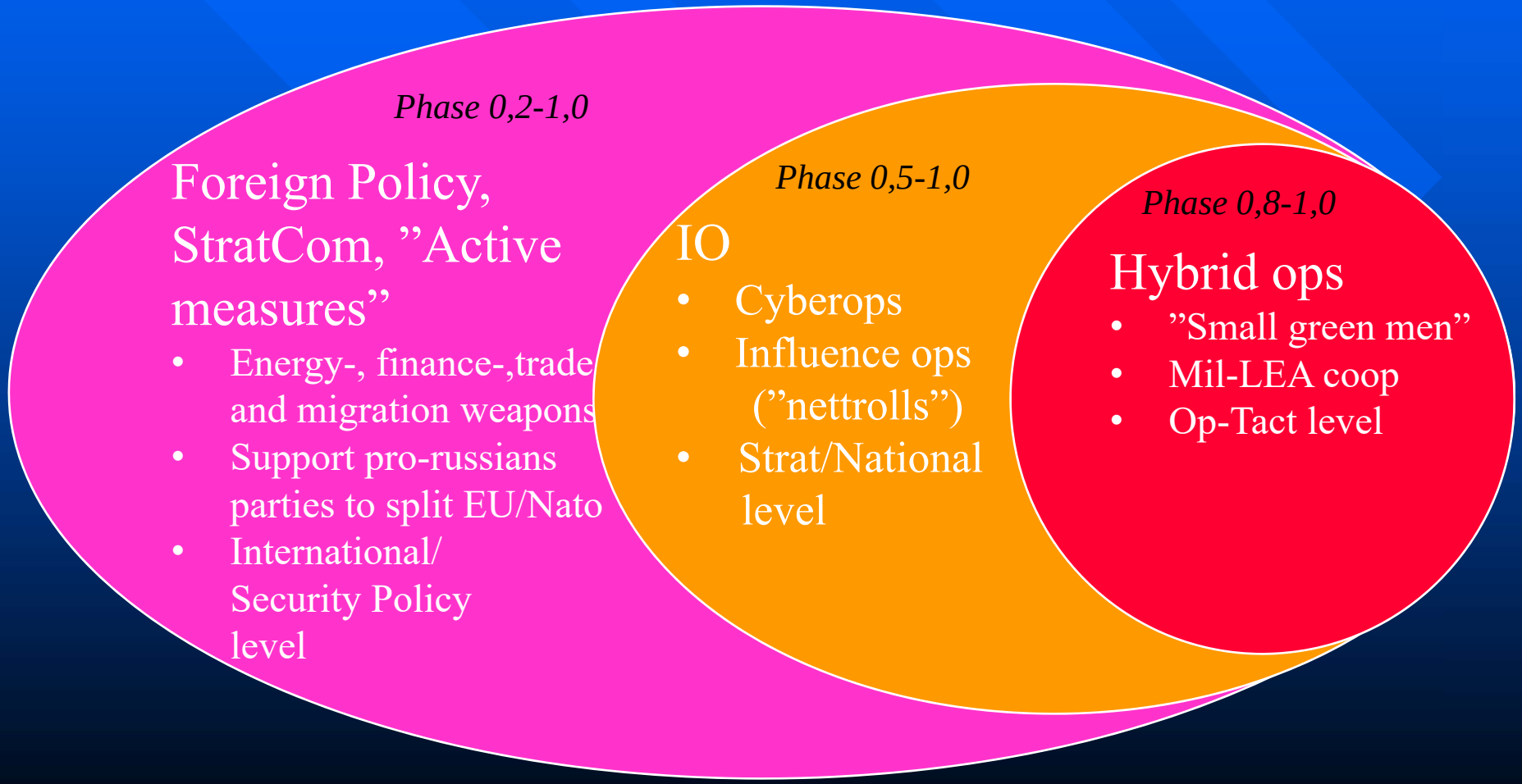
# Oversight/Coordination

- Do state and military and civil security authorities understand in what kind of environment they live and operate in today's world?
  - No, lack of coordination between the threat and planning communities within the government – i.e. IC versus the operational agencies and the private sector

# Civil-military relations

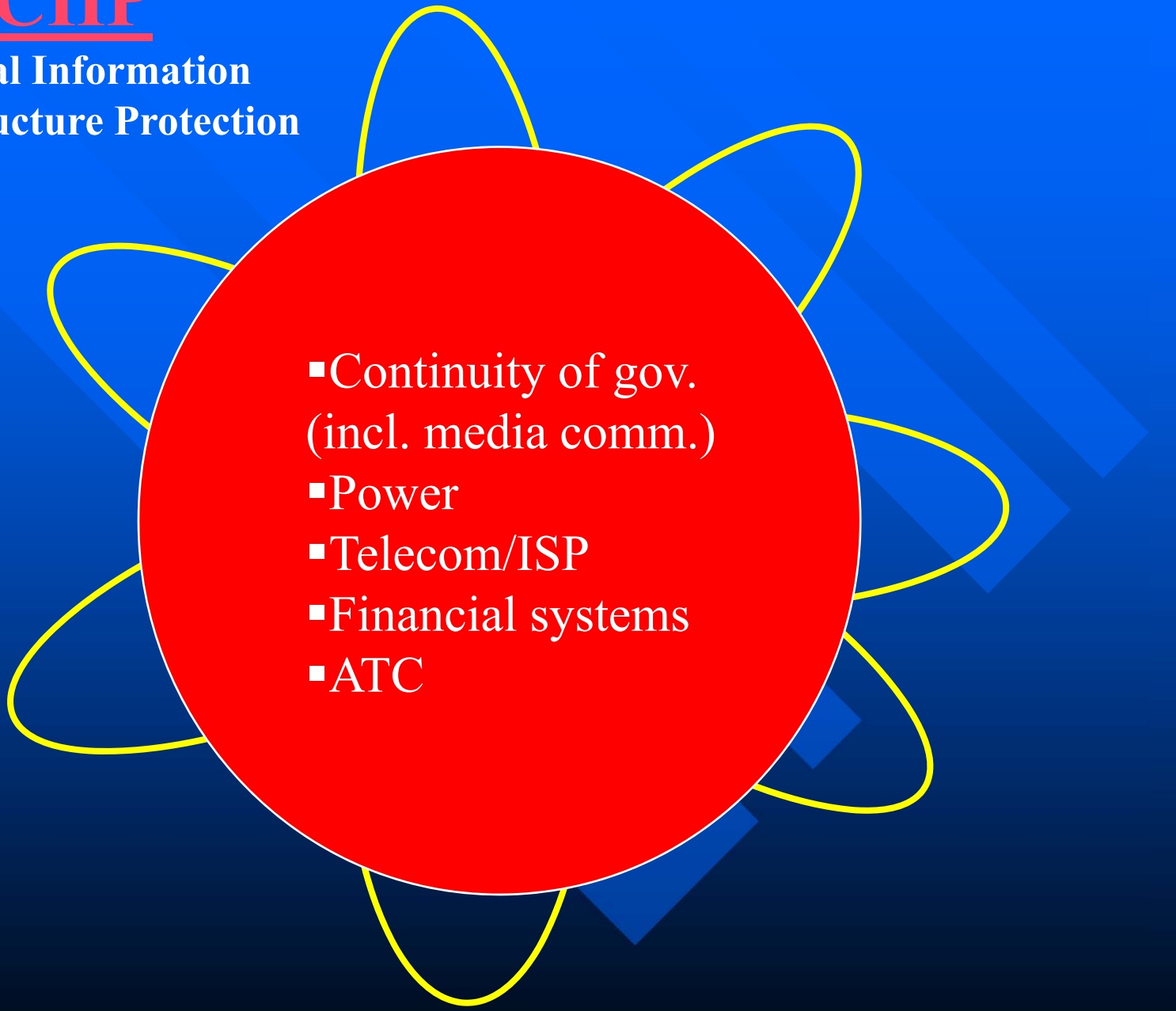
- What does that mean in particular for the armed forces; what kind of tasks should be assigned to them?
  - Definitions - Roles
  - Seamlessness CND-CNE-CNA where SIGINT play a crucial role
  - Red Teaming
- It´s a misunderstanding that (civil) cyber security is an CIO-issue instead of being an issue for the DG/CEO-level.

# Asymmetric Warfare



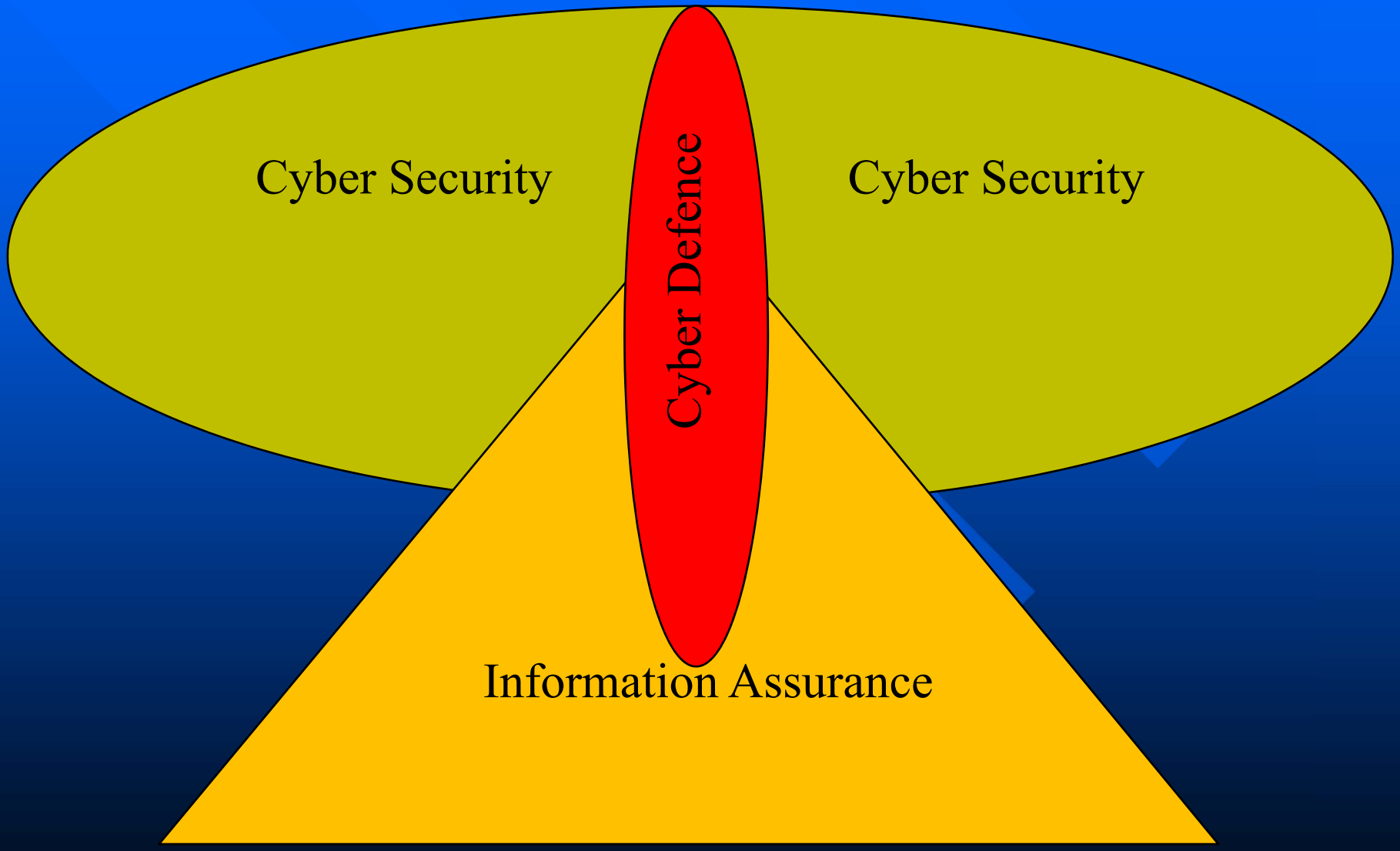
# CIIP

**Critical Information Infrastructure Protection**




X

# Definitions IA, Cyber Security, Cyber Defence




X

# Q&A

www.fhs.se/cats