网络空间安全态势感知

Cyber Security Situational Awareness

2021-2022学年（春） 专业普及课

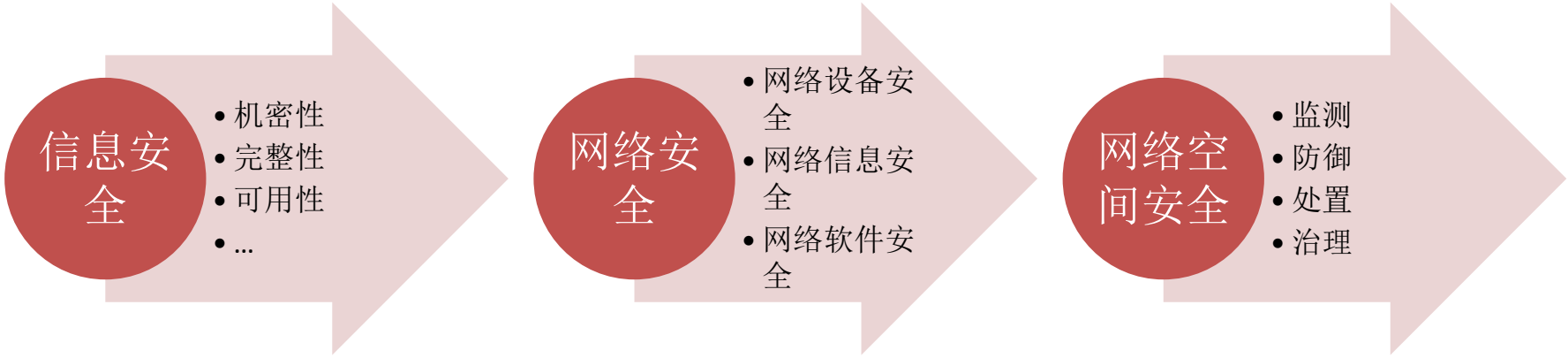
新兴领域网络安全态势技术

中国科学院大学
University of Chinese Academy of Sciences

提纲

一、新兴领域网络安全态势感知概述

- 信息技术不断发展，网络安全范畴越来越大



2016年12月27日，经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布《国家网络空间安全战略》

（二）坚决维护国家安全

（三）保护关键信息基础设施

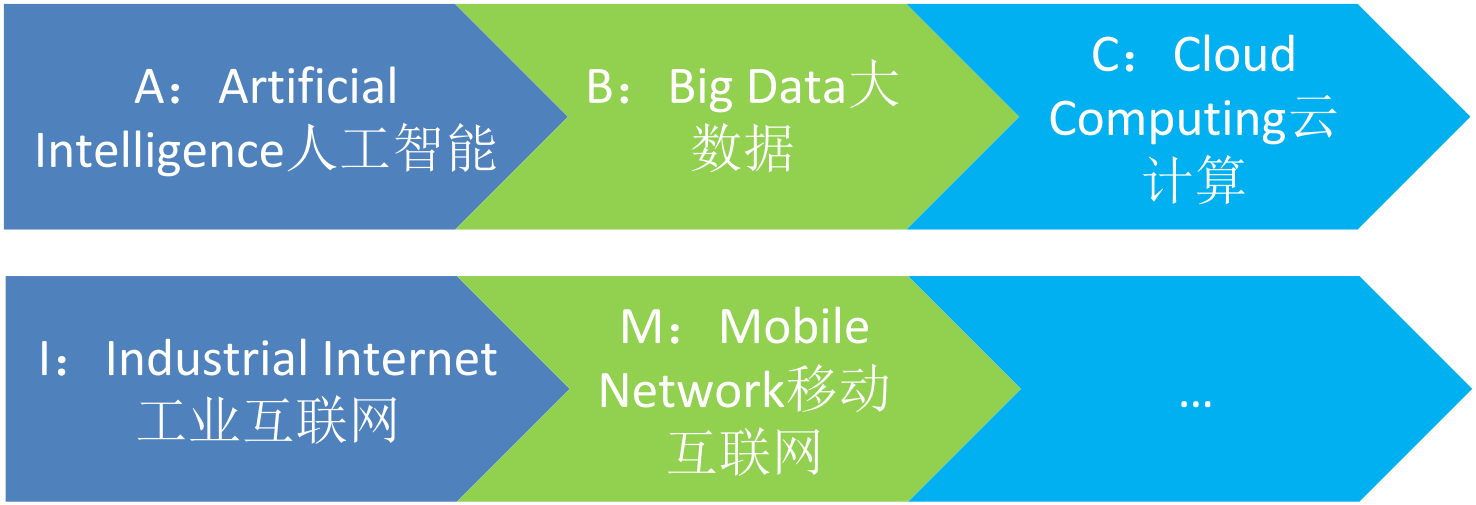
（五）打击网络恐怖和违法犯罪

（七）夯实网络安全基础

（八）提升网络空间防护能力

一、新兴领域网络安全态势感知概述

- 新技术新应用不断涌现，对网络安全态势感知既是机遇又是挑战



面向新兴领域，并利用各种新兴技术，不断提高网络安全态势感知能力

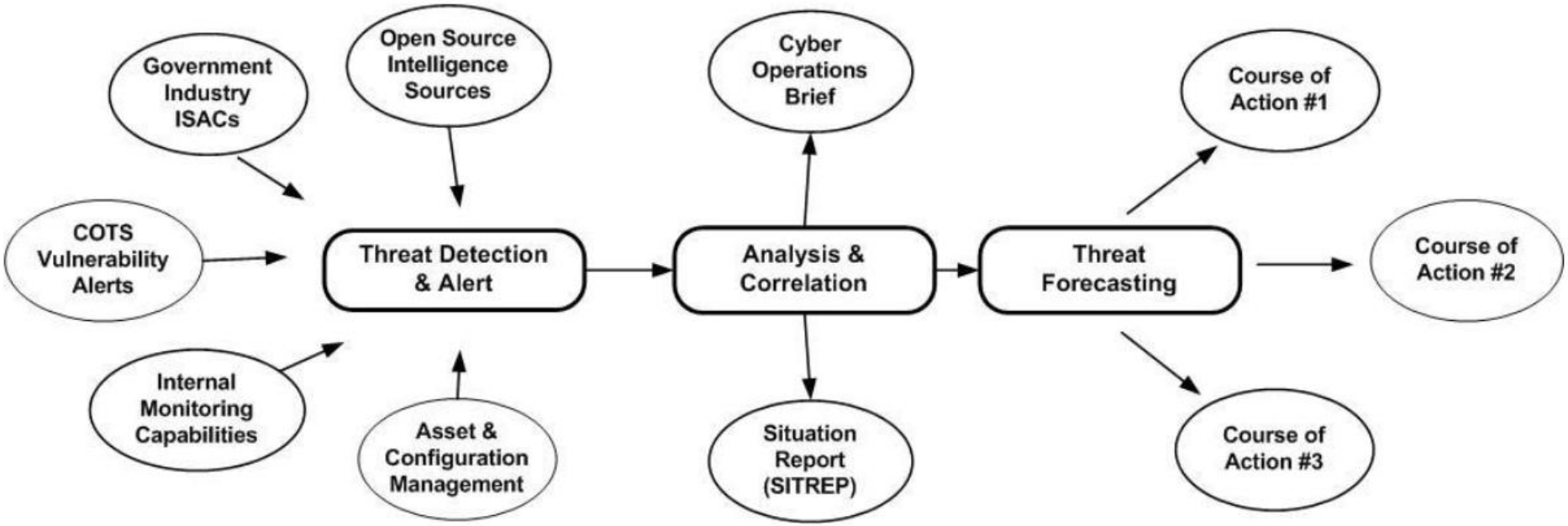
提纲

二、面向新兴领域的网络安全态势感知

- 各个新兴领域的安全特性不同
  - 工业互联网
    - 实时性要求高
    - 可靠性要好
    - 人的高度参与
  - 物联网
    - 设备种类多样
    - 协议通用性差
  - 云计算环境
    - 动态性
    - 虚拟化程度高
  - …

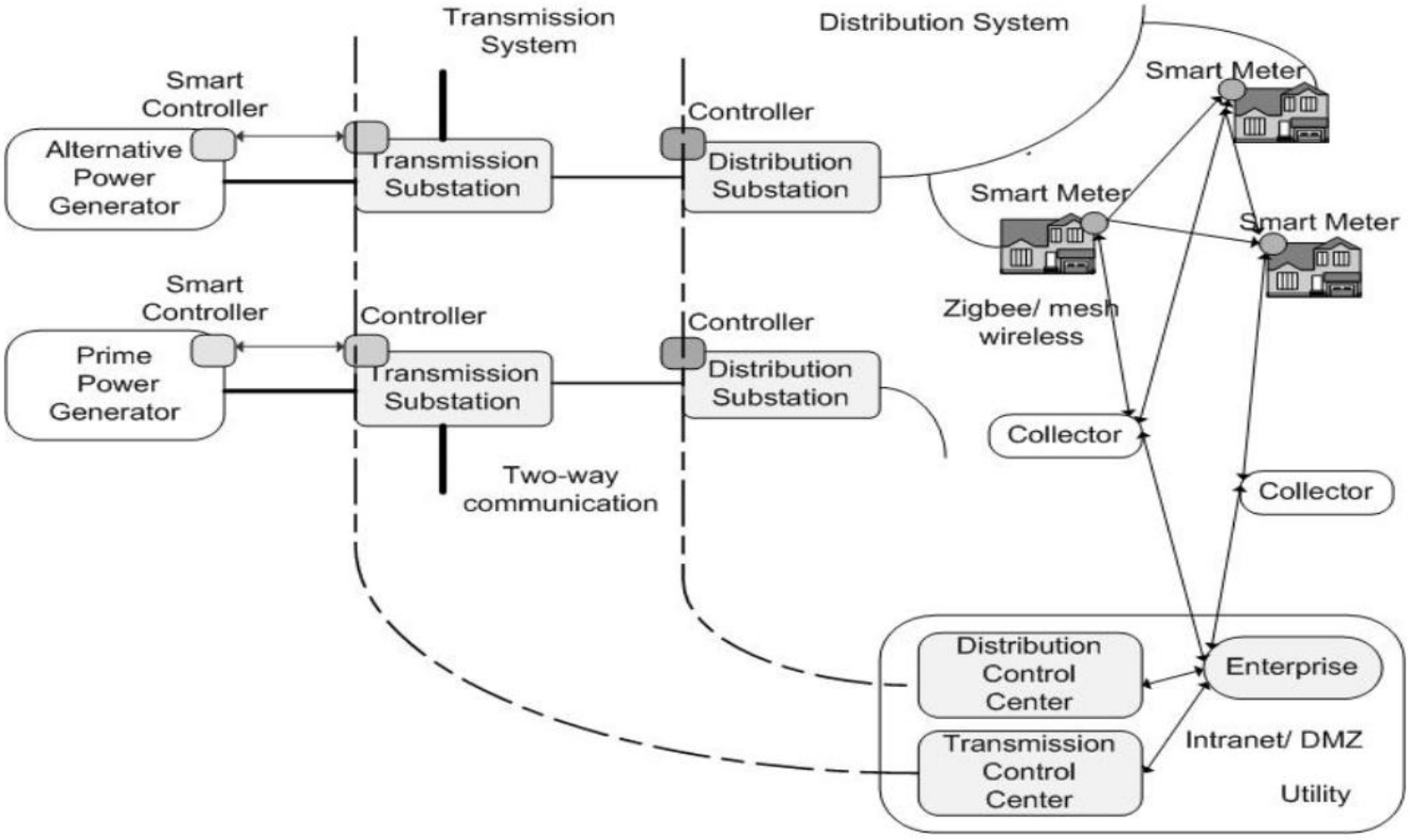
二、面向新兴领域的网络安全态势感知

- 美国国土安全部DHS提出了工控系统的三个安全原则
  - 自动化Automation — 快速的事件检测和响应能力
  - 互操作Interoperability —分布式的威胁检测能力之间的交互性
  - 授权Authentication — 设备众多（如传感器、工业组件



二、面向新兴领域的网络安全态势感知

- 面向工业互联网（智慧电网）的安全态势感知模型（1）
  - 智慧电网的主要组件



A Situational Awareness Architecture for the Smart Grid", Anastasia Mavridou and Mauricio Papa

二、面向新兴领域的网络安全态势感知

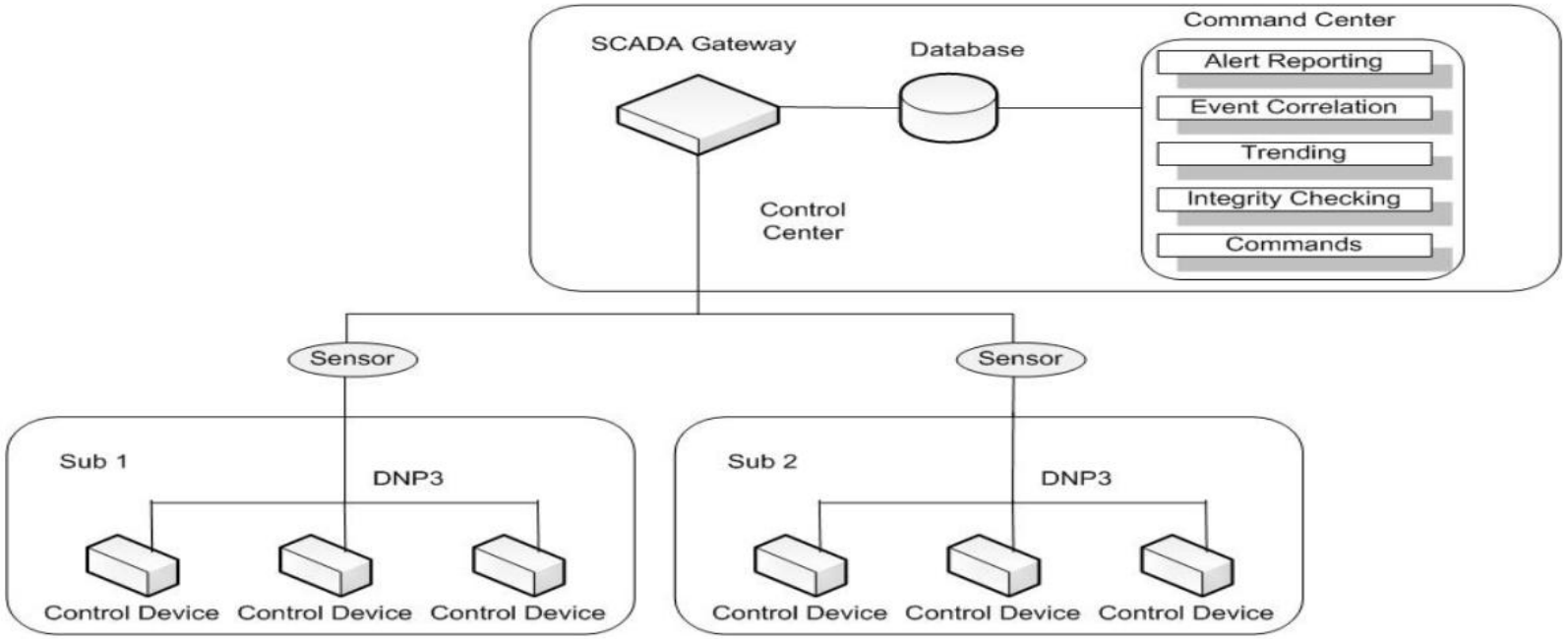
- 面向工业互联网（智慧电网）的安全态势感知模型（2）
  - 智慧电网的态势感知需求
    - 强调质量评估
    - 强调预测评估

	Requirement	Description
1	Situation perception	Be aware of the current situation. Situation recognition and identification.
2	Impact assessment	Be aware of the impact of the attack. Vulnerability analysis.
3	Situation tracking	Be aware of how situations evolve.
4	Trend and intent analysis	Be aware of actor (adversary) behavior.
5	Causality analysis	Be aware of why and how the current situation is caused.
6	Quality assessment	Be aware of the quality of the collected situation awareness information items.
7	Future assessment	Assess plausible futures of the current situation.

A Situational Awareness Architecture for the Smart Grid， Anastasia Mavridou and Mauricio Papa

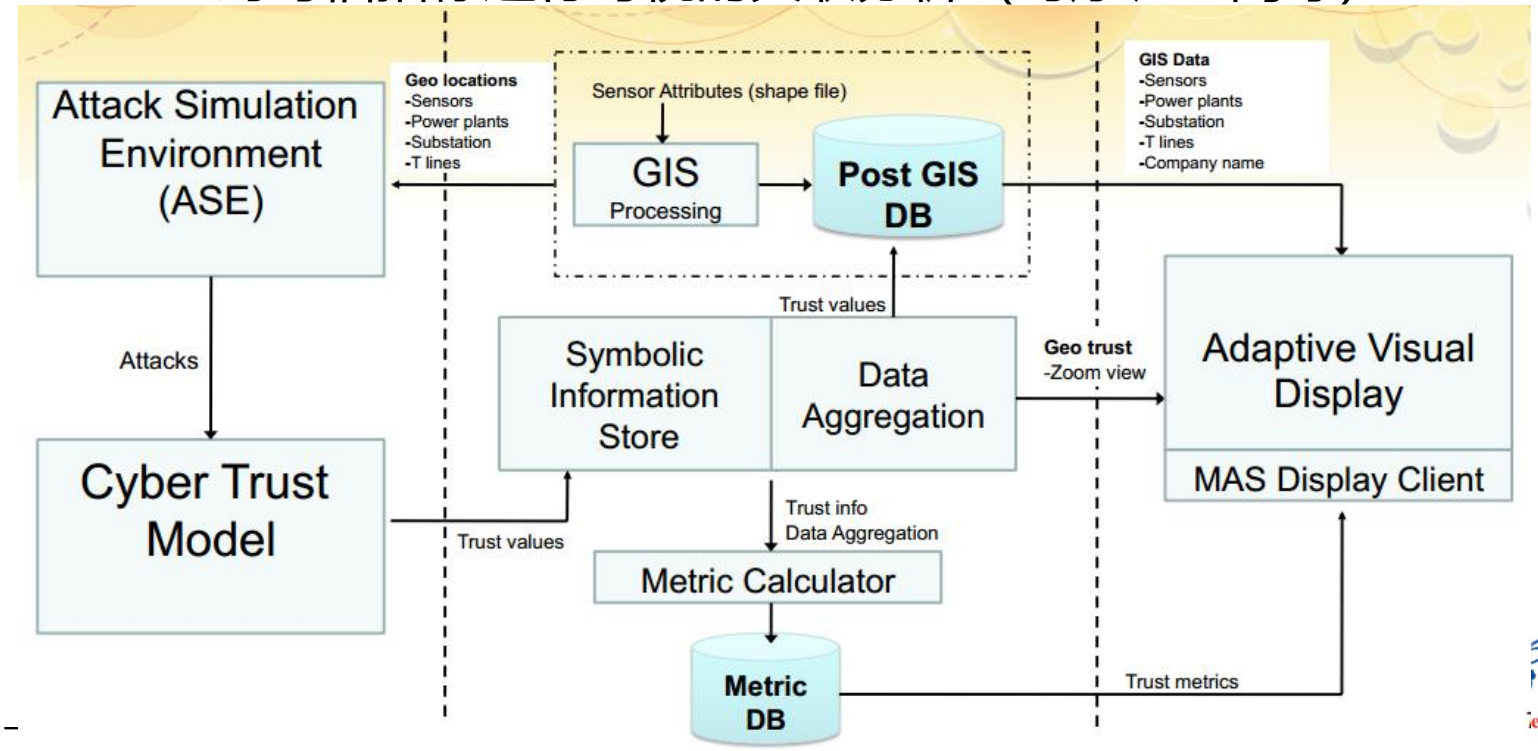
二、面向新兴领域的网络安全态势感知

- 面向工业互联网（智慧电网）的安全态势感知模型（2）
  - 智慧电网的态势感知框架
    - 注重传感器的数据采集
    - 强调SCADA网关的作用



二、面向新兴领域的网络安全态势感知

- 面向工业互联网（智慧电网）的安全态势感知模型
  - 智慧电网态势感知的可视化
    - 对网络可信进行了数学建模
    - 对智慧电网进行了时空展示
    - 对可信指标进行可视的关联分析（时序、空间等）



二、面向新兴领域的网络安全态势感知

- 面向物联网IoT的安全态势感知模型
  - 引入随机颜色Petri网（SCPN）用来表示网络攻防环境

$$SCPN = (A, T, P, C, \Im, TR)$$

    - A表示资产
    - T表示不同类型的威胁
    - P表示IoT节点在网中的可能位置
    - C表示威胁传播

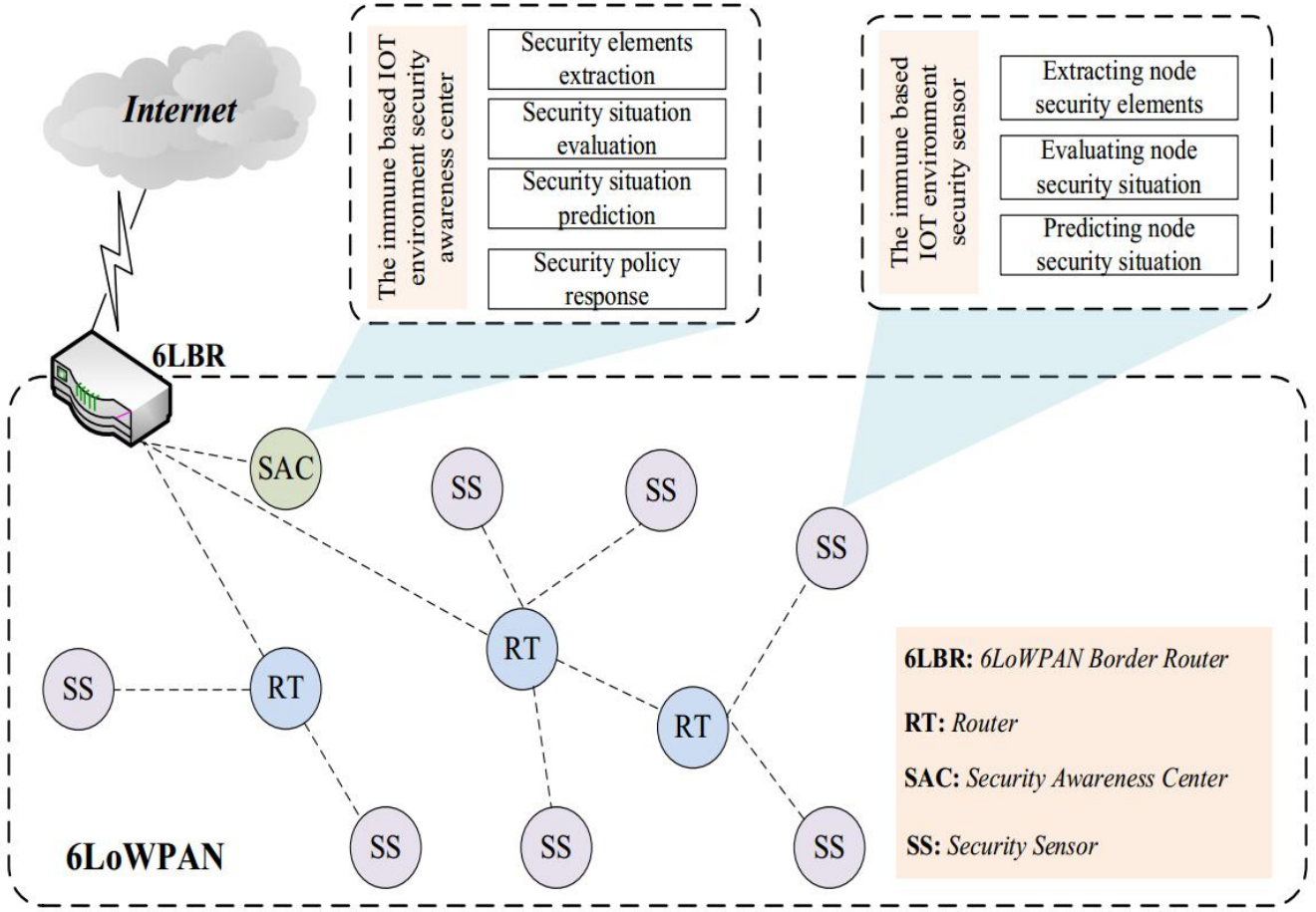
  引入马尔科夫博弈模型来进行态势计算

    - 博弈参与者
    - 状态空间
    - 行动空间
    - 转换规则

$$MGM = (\lambda, S, \Omega, \Phi, \Re)$$

二、面向新兴领域的网络安全态势感知

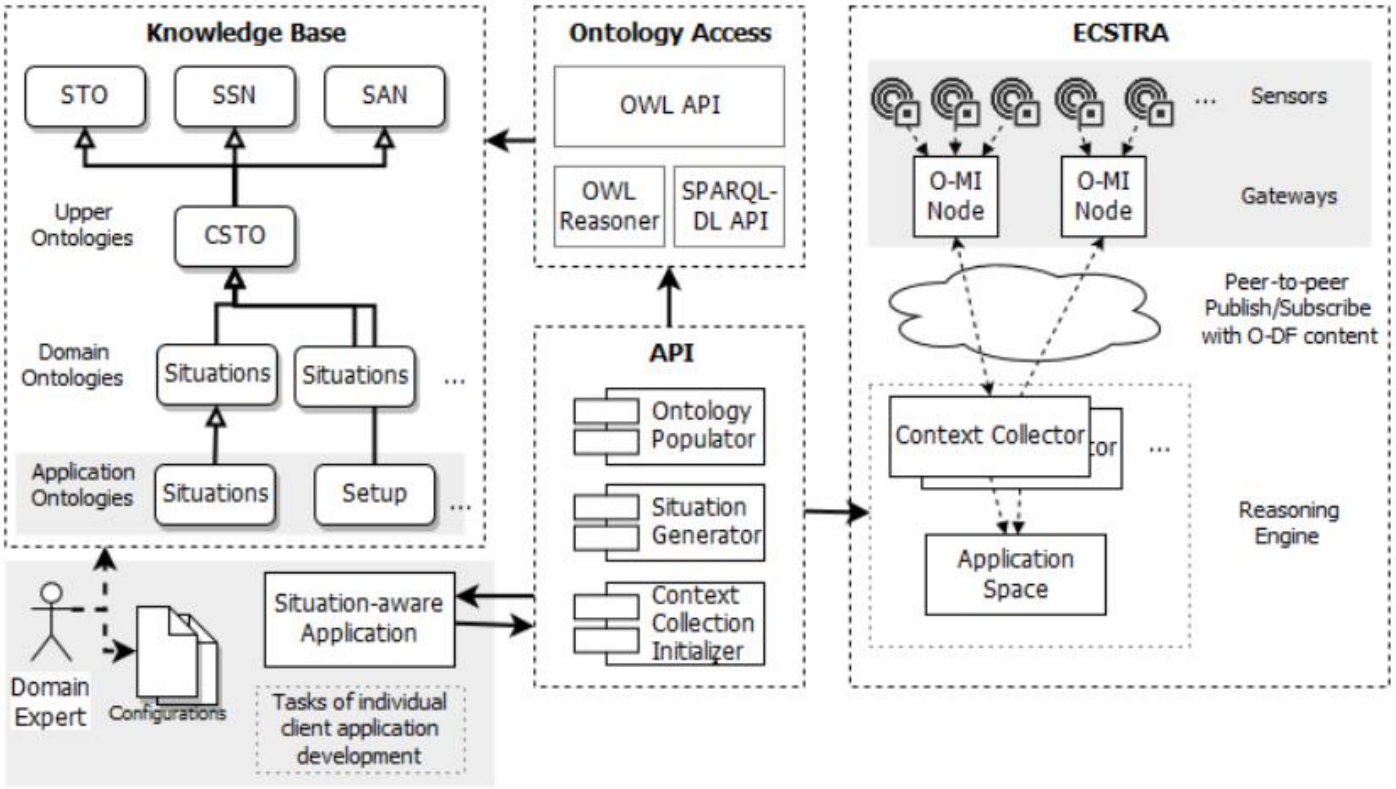
- 面向物联网的安全态势感知模型
  - 特点：基于免疫理论构建安全感知中心



An Immunity-Based IOT Environment Security Situation Awareness Model, 2017

二、面向新兴领域的网络安全态势感知

- 面向物联网的安全态势感知模型
  - 特点：引入了本体理论进行环境构建、知识推理进行态势理解



二、面向新兴领域的网络安全态势感知

- 面向物联网（可穿戴设备）的安全态势感知
  - 特点：面向可穿戴健康监测设备，采取调研式研究了其安全性和隐私性

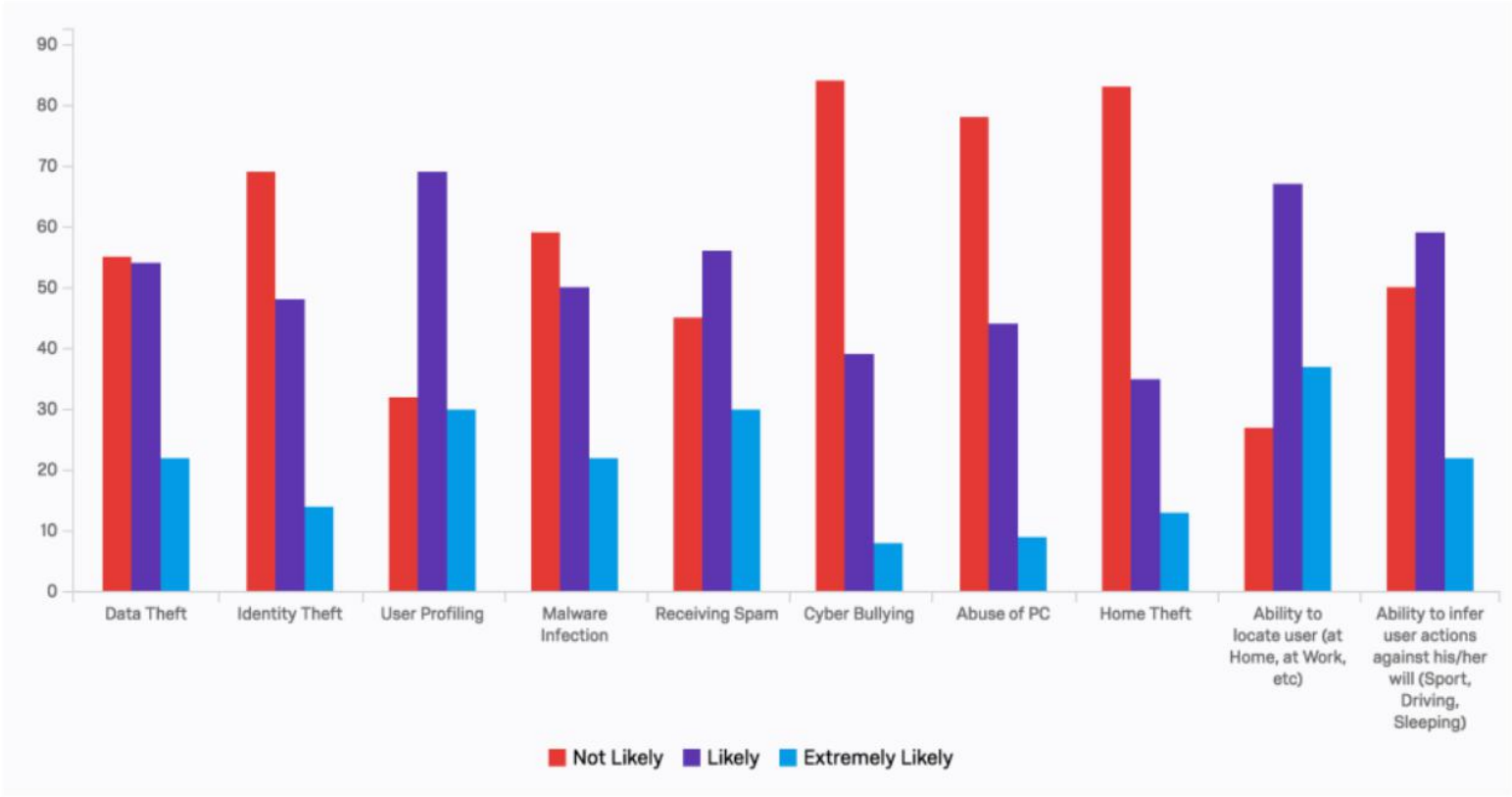


FIGURE 2 THREAT LIKELIHOOD

A Study on Situational Awareness Security and Privacy of Wearable Health Monitoring Devices", Xavier Bellekens, 2016

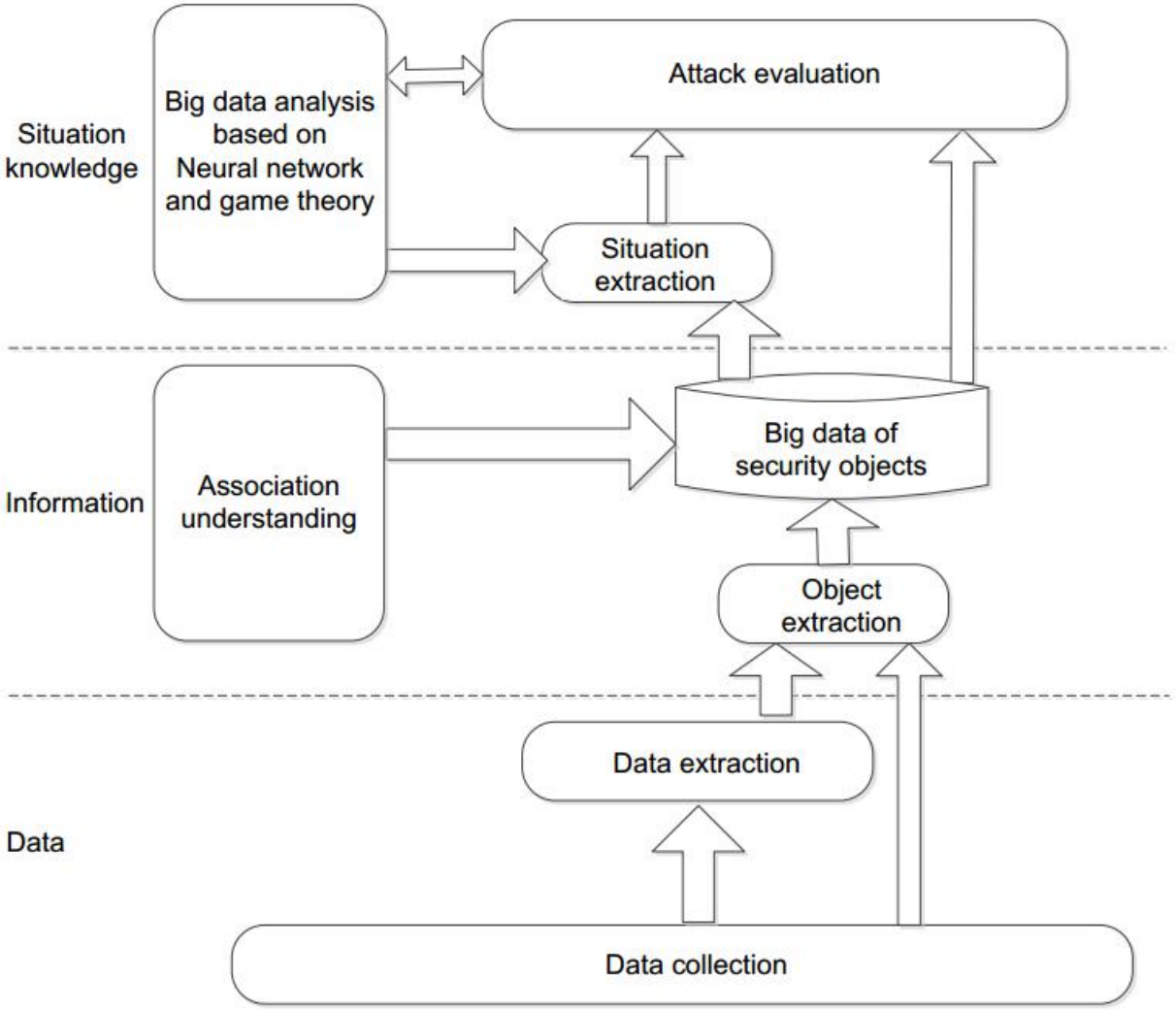
提纲

三、利用新兴技术的网络安全态势感知

- 总体思路
  - 充分利用大数据、云计算、人工智能等
    - 提高数据收集能力（如传感器、云架构）
    - 提高数据分析处理能力
    - 提高知识发掘能力
    - 。。。
  - 如美国在其2016年的Federal Cyber Security Research and Development Strategic Plan中就强调了新技术的应用
    - increasing complexities of hybrid cloud/on-premise deployments
    - an increased use of mobile devices
    - an increasing number of siloed departmental applications
    - Augmenting Situational Awareness with AI

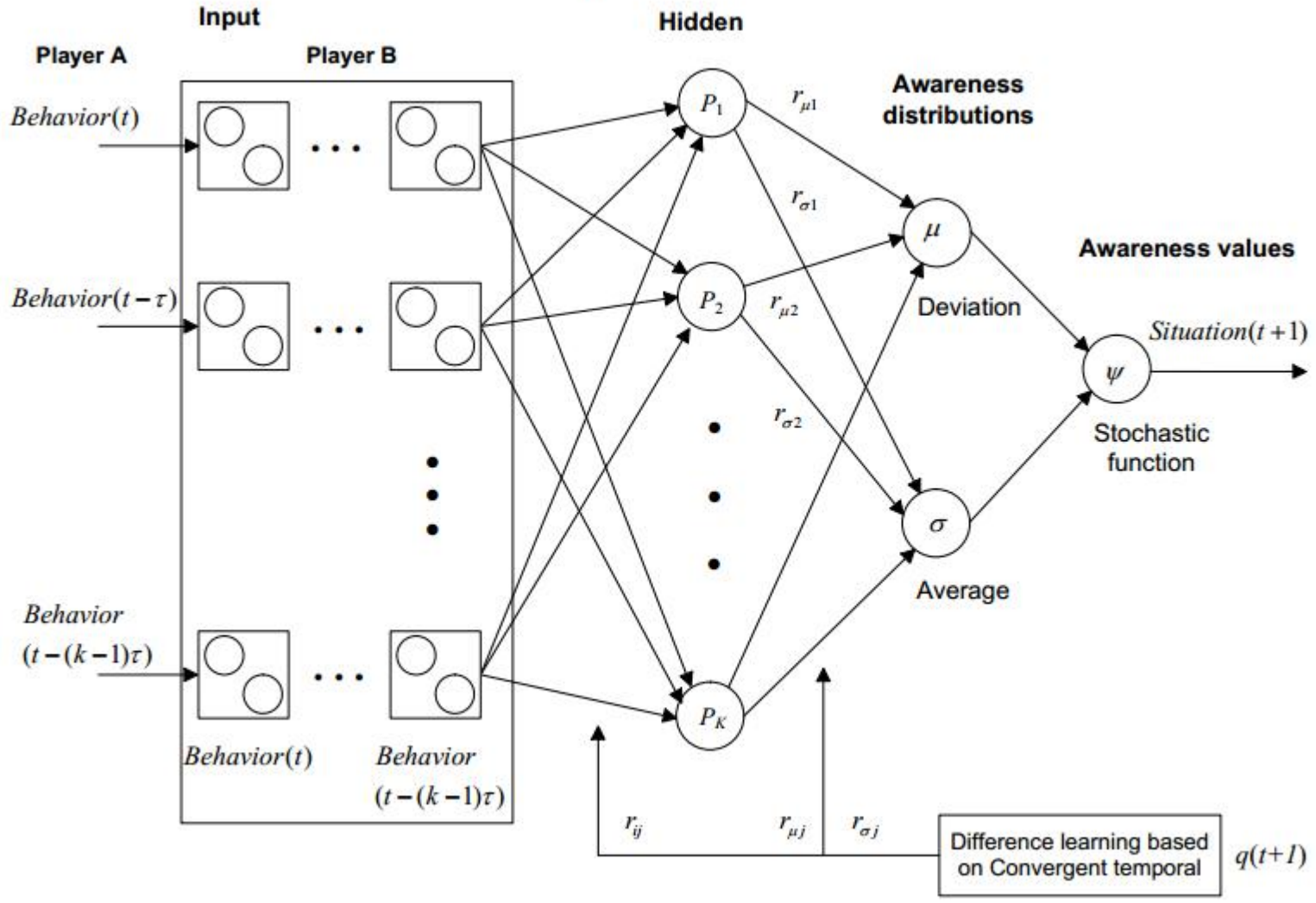
三、利用新兴技术的网络安全态势感知

- 利用大数据技术提高安全态势的能力（1）
  - 面向智慧电网开展工作
  - 综合利用了关联分析、博弈论等方法
  - 设计原则遵循：数据—信息—态势知识



Big Data Analysis-based Security Situational Awareness for Smart Grid， 2016

三、利用新兴技术的网络安全态势感知



提纲

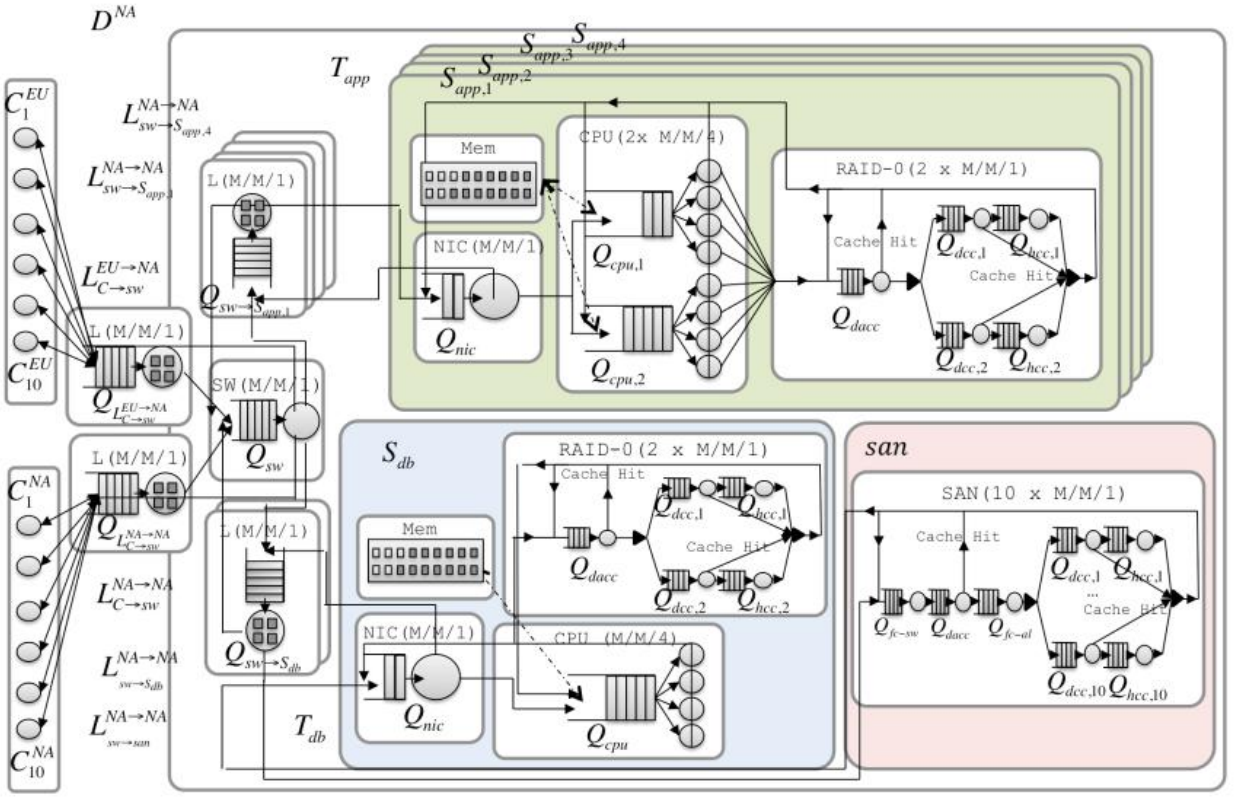
四、新兴领域网络安全态势感知实例

- 能源行业的案例-态势感知框架（1）
  - 除了信息技术（information technology，IT），还强调操作技术（Operations Technology，OT）
  - 业务特点：业务实时性强、功能组件相对稳定
  - 安全特点：基于风险分析的理念开展
  - 三大核心部件
    - 面向全部数据架构的模拟器
    - 风险排序平台SAFARI
    - 基于系统理论的过程安全分析STPA-Sec

Situational Awareness Framework for Cyber Security Event Prediction and Quantification (SAFFRON)，Abel Sanchez and John R. Williams

四、新兴领域网络安全态势感知实例

- 能源行业的案例-态势感知框架（2）
  - 面向全部数据架构的模拟器
    - 攻击预测
    - 效能评估
    - 能力调度
    - 软硬件配置
    - 瓶颈检测
    - …

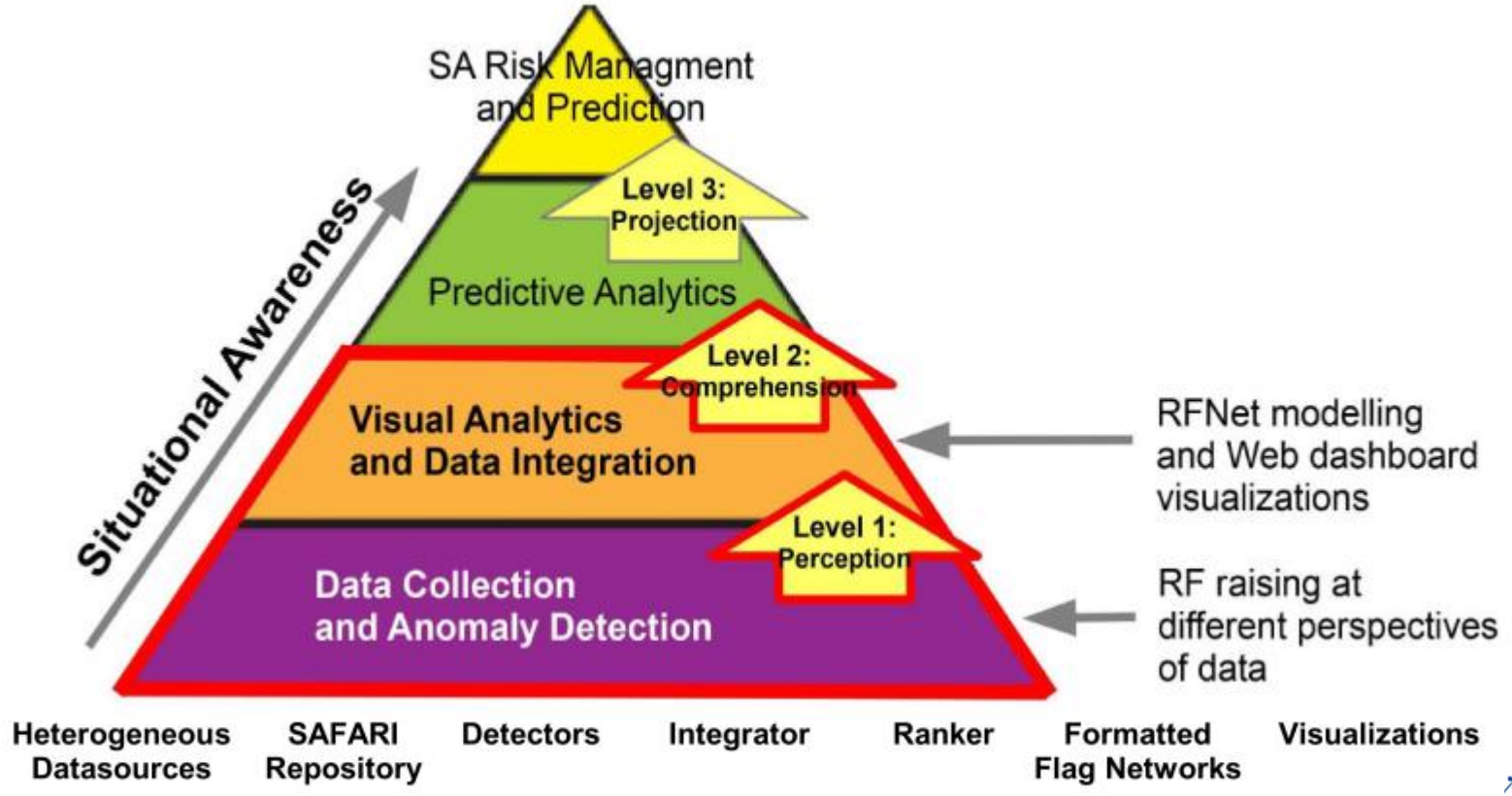


Situational Awareness Framework for Cyber Security Event Prediction and Quantification (SAFFRON)，Abel Sanchez and John R. Williams

University of Chinese Academy of Sciences

四、新兴领域网络安全态势感知实例

- 能源行业的案例-态势感知框架（3）
  - 风险排序平台SAFARI



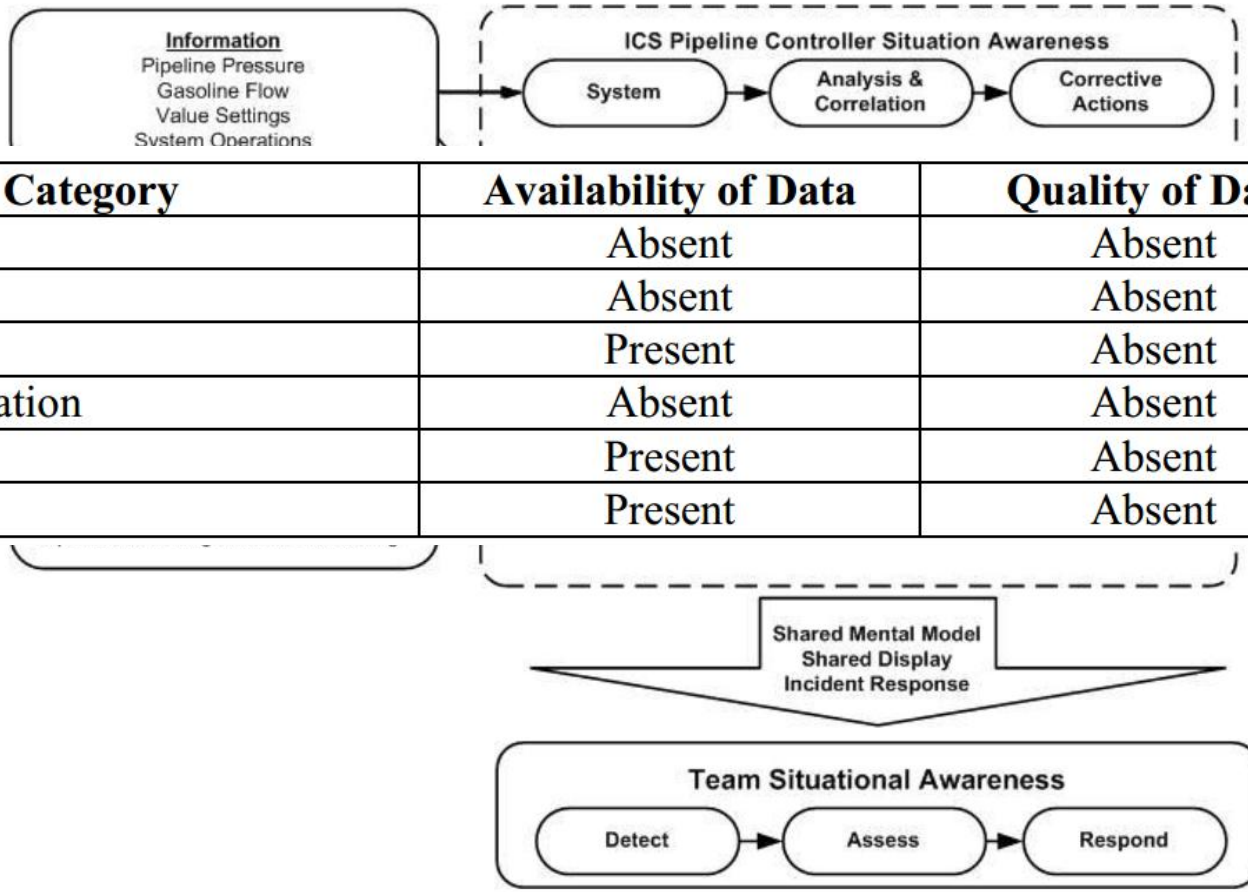
Situat
Sanchez and John R. Williams

Abel

University of Chinese Academy of Sciences

四、新兴领域网络安全态势感知实例

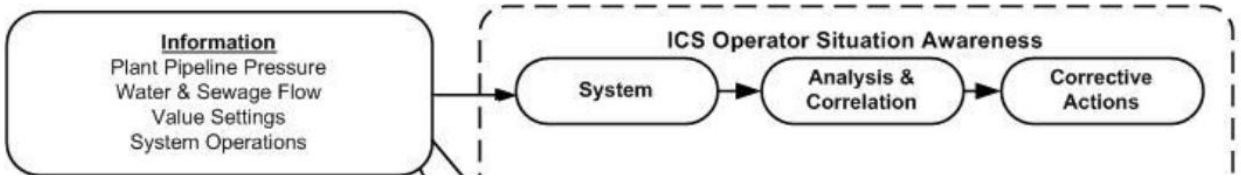
- 工控领域的案例-基于NIST标准的框架（1）
  - Olympic Pipeline Cybersecurity Situation Awareness Model
  - 模型的缸



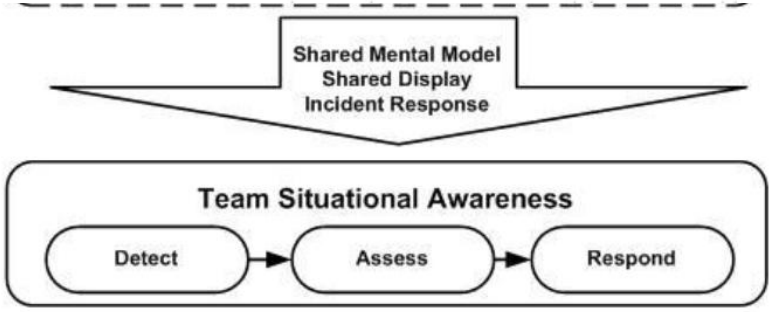
NIST Control Category	Availability of Data	Quality of Data
Access Control	Absent	Absent
Audit and Accountability	Absent	Absent
Configuration Management	Present	Absent
Identification and Authentication	Absent	Absent
Incident Response	Present	Absent
System Integrity	Present	Absent

四、新兴领域网络安全态势感知实例

- 工控领域的案例-基于NIST标准的框架（2）
  - Maroochy Water Plant Cybersecurity Situation Awareness Model
  - 模型的缺点
  - 模型众多，区

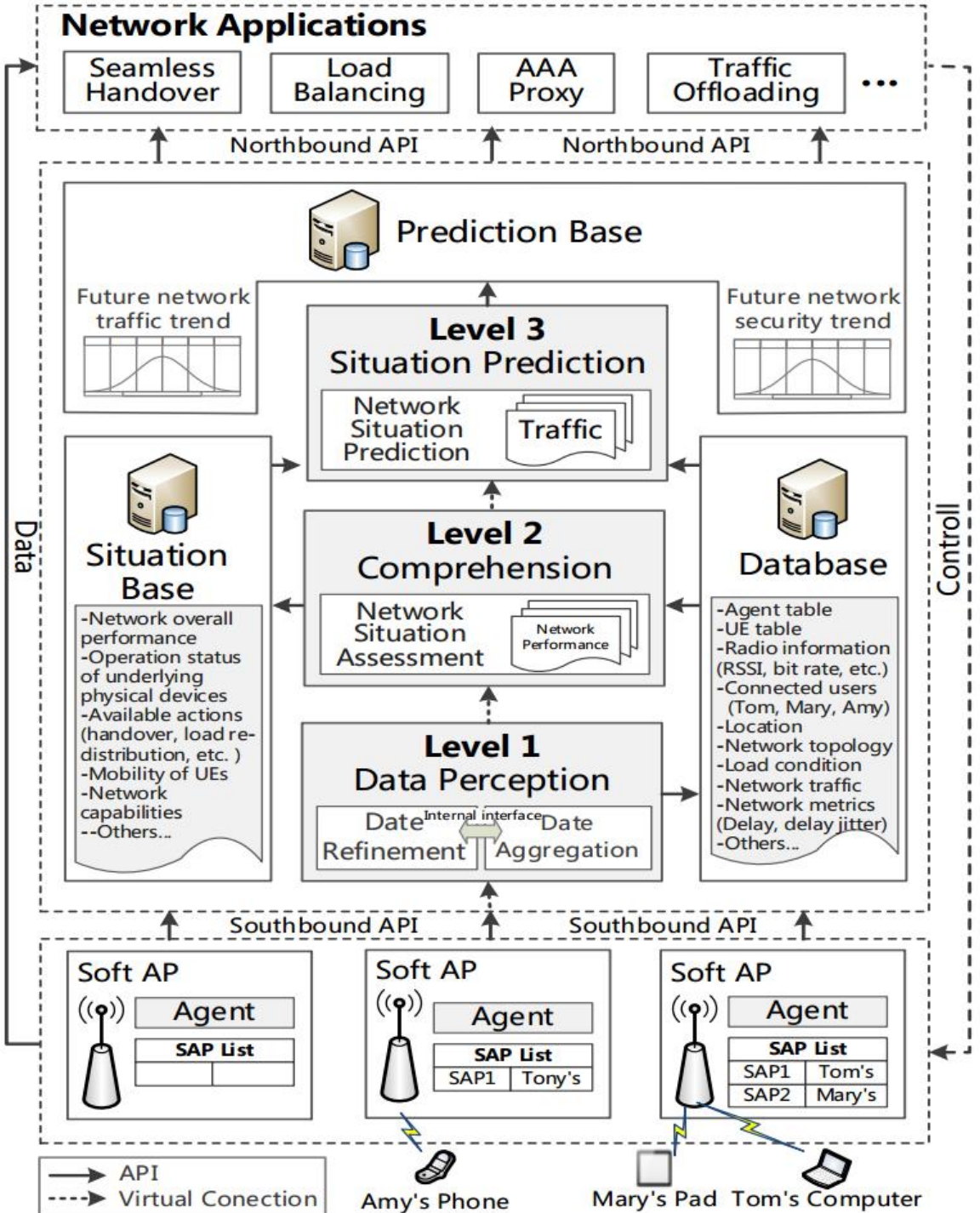


NIST Control Category	Availability of Data	Quality of Data
Access Control	Present	Absent
Audit and Accountability	Present	Absent
Configuration Management	-	-
Identification and Authentication	Present	Absent
Incident Response	Absent	Absent
System Integrity	Present	Absent



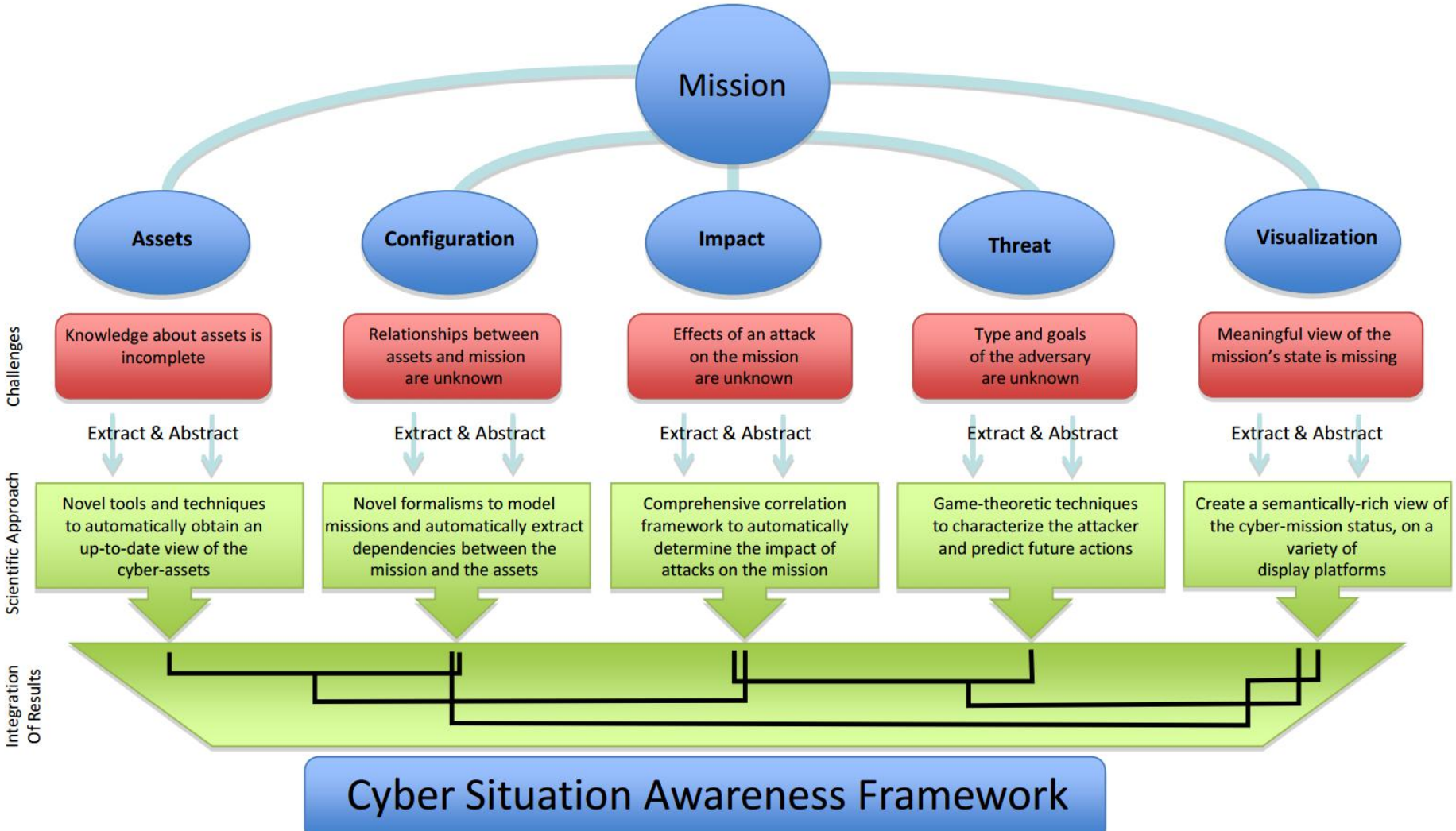
四、 实例

- 软件定



四、新兴领域网络安全态势感知实例

- 加州大学伯克利分校、圣巴巴拉分校佐治亚理工学院的工作



提纲

- 一、新兴领域网络安全态势概述
- 二、面向新兴领域的态势感知
- 三、利用新兴技术的态势感知
- 四、新兴领域安全态势感知实例
- 五、未来的挑战

五、未来的挑战

- 实时环境中海量安全状态数据的处理
  - 万物互联、工业互联网、…
- 封闭式生产系统与开放式安全防护体系之间的矛盾
  - 比如生产系统中如何进行威胁情报共享

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

谢 谢!