CAIS

Cyber Attack Information System

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY

Towards a National Cyber Attack Information System

Cyber Terrorism and Crime Conference CYTER 2012
June 12th - 13th 2012, Prague, Czech Republic

Florian Skopik
Austrian Institute of Technology, Austria
http://www.ait.ac.at/it-security
florian.skopik@ait.ac.at

AIT Austrian Institute of Technology • Bundeskanzleramt Österreich
Bundesministerium für Landesverteidigung und Sport • Bundesministerium für Inneres
FH St. Pölten • OIIP Österreichisches Institut für Internationale Politik
T-Mobile Austria • T-Systems Austria • NIC.AT / CERT.AT

bmvit Bundesministerium für Verkehr, Innovation und Technologie

KIRAS Sicherheitsforschung

FFG

Overview

- Problem Statement and Environment
- Rationale for National Cyber Defence
- What is National Situational Awareness?
- Overall CAIS Approach
- Advanced Incident Response
  - Pro-Active Simulation
  - Re-Active Simulation
- CAIS Architecture
  - Organizational Level
  - National Level
  - Roles and Responsibilities
- Multi National Experiment 7 (MNE7)
- Project CAIS
- Discussion and Conclusion

Problem Statement and Environment

- Our **society** becomes more and more **dependent on ICT**
  - Many critical infrastructures are increasingly closely coupled to the Internet (enabling monitoring, remote control, maintenance)
  - Novel computing areas, such as cloud computing, mobile computing arise
- **Cyber terrorism** (and cyber war) is reality!
  - Stuxnet deployed to sabotage Iran's nuclear research program
  - Large-scale DDos in Estonia 2007
- Several initiatives to foster awareness of vulnerabilities/threats
  - E.g., **Computer Emergency Response Teams (CERTs**)
- **Infrastructure** providers get **increasingly interconnected**, thus also increasing interdependencies and vulnerability → ***novel challenges***
  - Detection of **coordinated attacks** towards multiple organizations
  - **Collaborative protection** against attacks through knowledge sharing
  - Raising awareness of (potential) **consequences of an attack**

→ Need for a **Cyber Attack Information System** on a national level!

Rationale for National Cyber Defence

- **Linking and coordinating** existing initiatives
  - CERTs
  - National initiatives, e.g., crisis management
- Establishing **situational awareness** on a national level
  - Infer risks for society due to interdependent infrastructures
- Facilitating **public-private partnerships**
  - Private organizations delivering public services
- Maintaining **organizational responsibility**
  - Definition of roles, responsibilities, obligations etc.
- Activating **inter-organizational collaboration**
  - Information exchange regarding exploited vulnerabilities
  - Mutual aid in securing systems against current threats

What is National Situational Awareness?

- Understand
  - Structure of networks and interdependencies
  - Availability of services
  - Ongoing business and operations
- Detect and predict
  - Undesired activities and their current or future impact on services, operation, or infrastructure
- Observe and analyze
  - Responsive actions and mitigation strategies and their success
  - Effectiveness of service recovery procedures

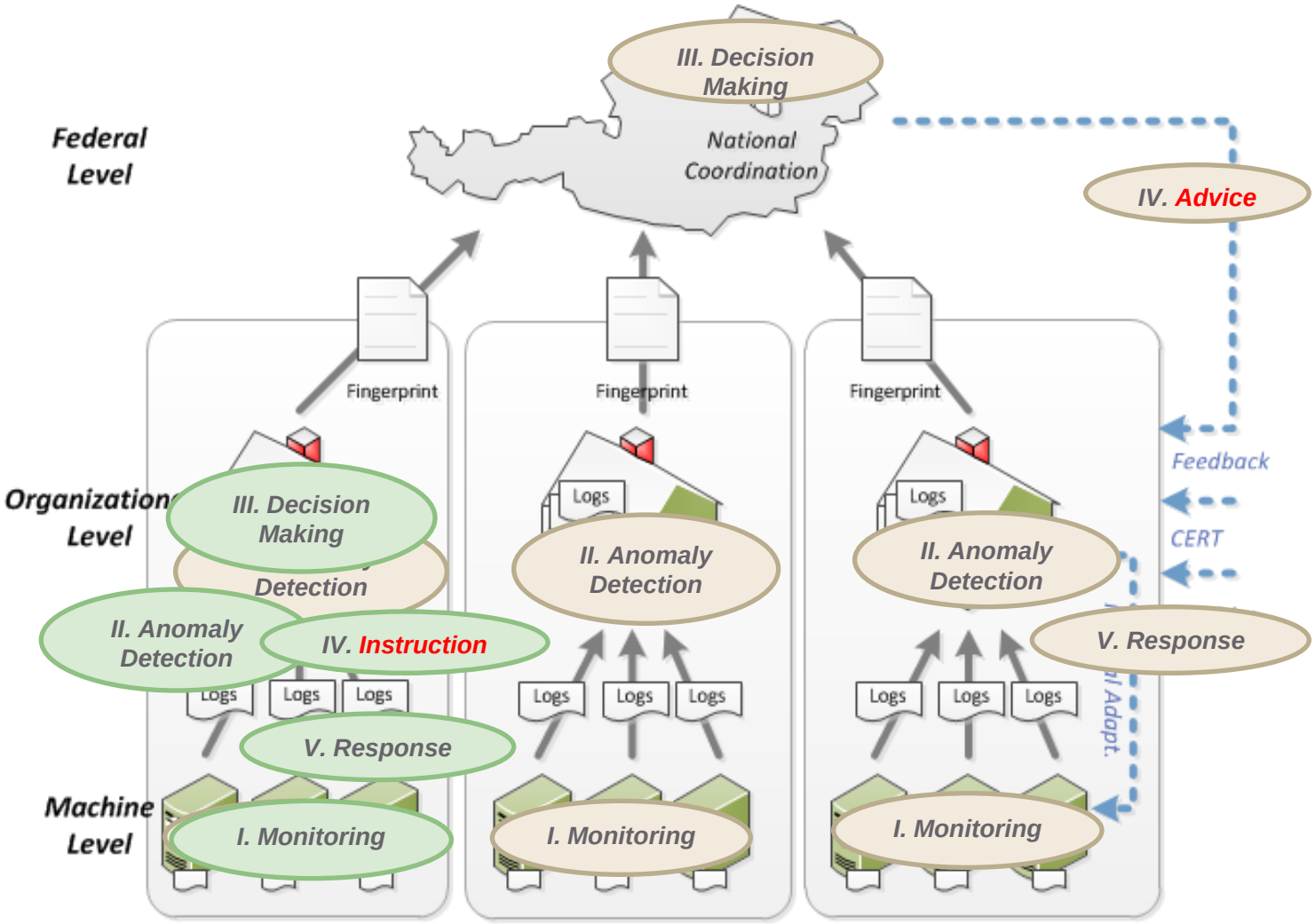
…on an organizational as well as national level!

„gather, filter, process, assess, analyze, interpret, comprehend, visualize, predict, inform, share“

Overall CAIS Approach (1/2)

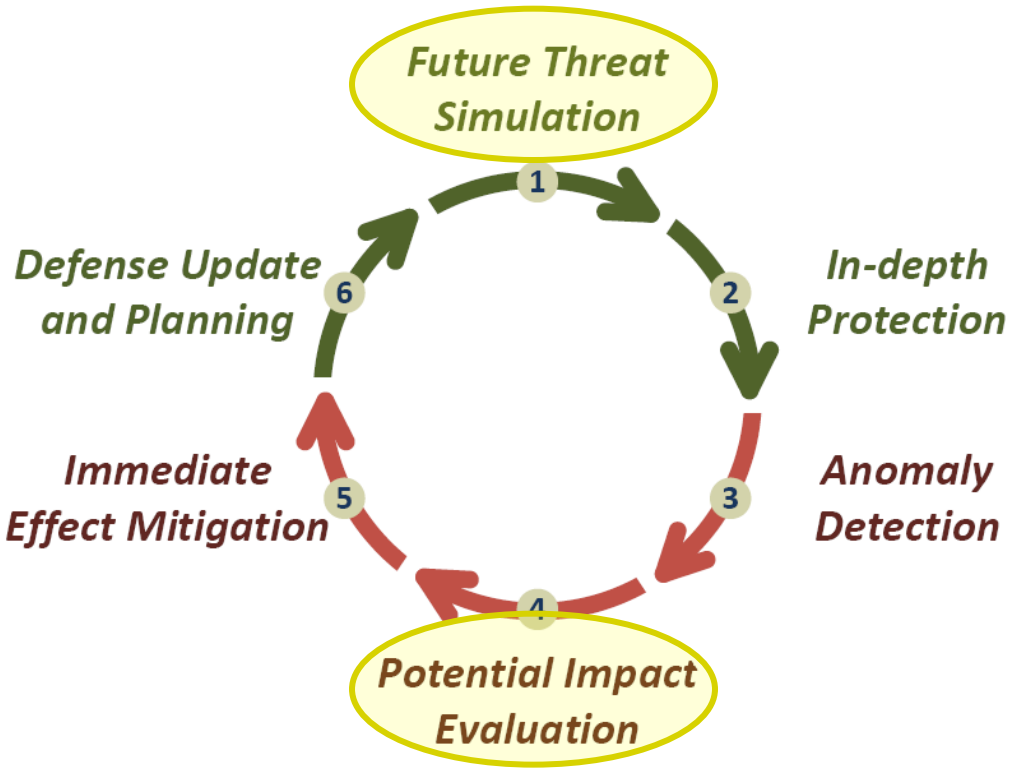
- Cyclic approach – similar to incident response methods
- Hierarchical structure: organizational v.s. national level
- Stepwise Process
  1. *Monitoring*
     - Collect data about status of infrastructure
  2. *Anomaly Detection*
     - Detection of incidents
  3. *Decision Making*
     - Establishing situational awareness, collaborative approach
  4. *Instruction/Advice*
     - Discovery of targeted counter measures
  5. *Response*
     - Mitigation of effects, e.g., through infrastructure adaptation, service patching, etc.

Overall CAIS Approach (2/2)



Advanced Incident Response Cycle

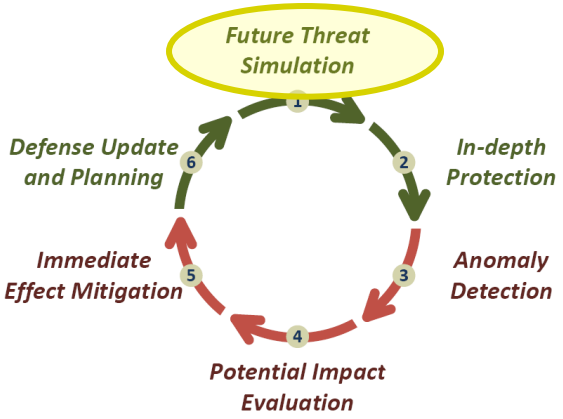
- **Strategic evolution** of an ICT infrastructure (**green**)
  - (**1**) Simulation of future threats and attacks
  - (**2**) Planning and deployment of protection mechanisms
  - (**6**) Periodic updates and maintenance
- **Detection** of on-going **attacks** (**red**)
  - (**3**) Anomaly detection
  - (**4**) Evaluation of potential impact
  - (**5**) Immediate effect mitigation



Application of advanced modeling and simulation techniques.

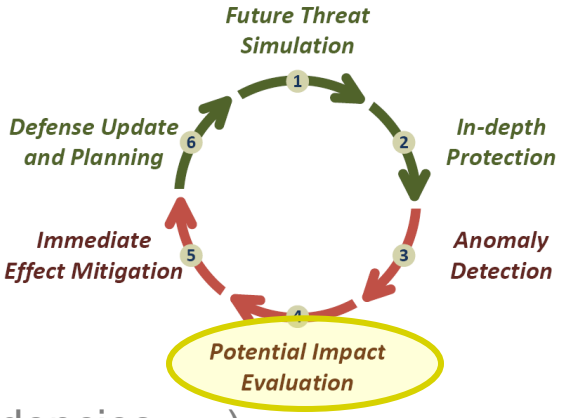
Pro-Active Simulation

- **Evaluation** of the efficiency of deployed **defense mechanisms**
  - Improved monitoring mechanisms
  - Adaptation of infrastructure
  - Update of incident response plans
- Simulation
  - Input
    - Updated (=to be) model of infrastructure
    - Historical contextual data from a verified anomaly/attack or
    - Expected network data of a potential attack
  - Output:
    - Resilience measure of “to-be-model” compared to “as-is-model”
    - Open vulnerabilities
- Ultimate Goal: Learn about the **resilience against potential future attacks** (i.e., create a library of resilience patterns reflecting best practices against specific classes of attacks).



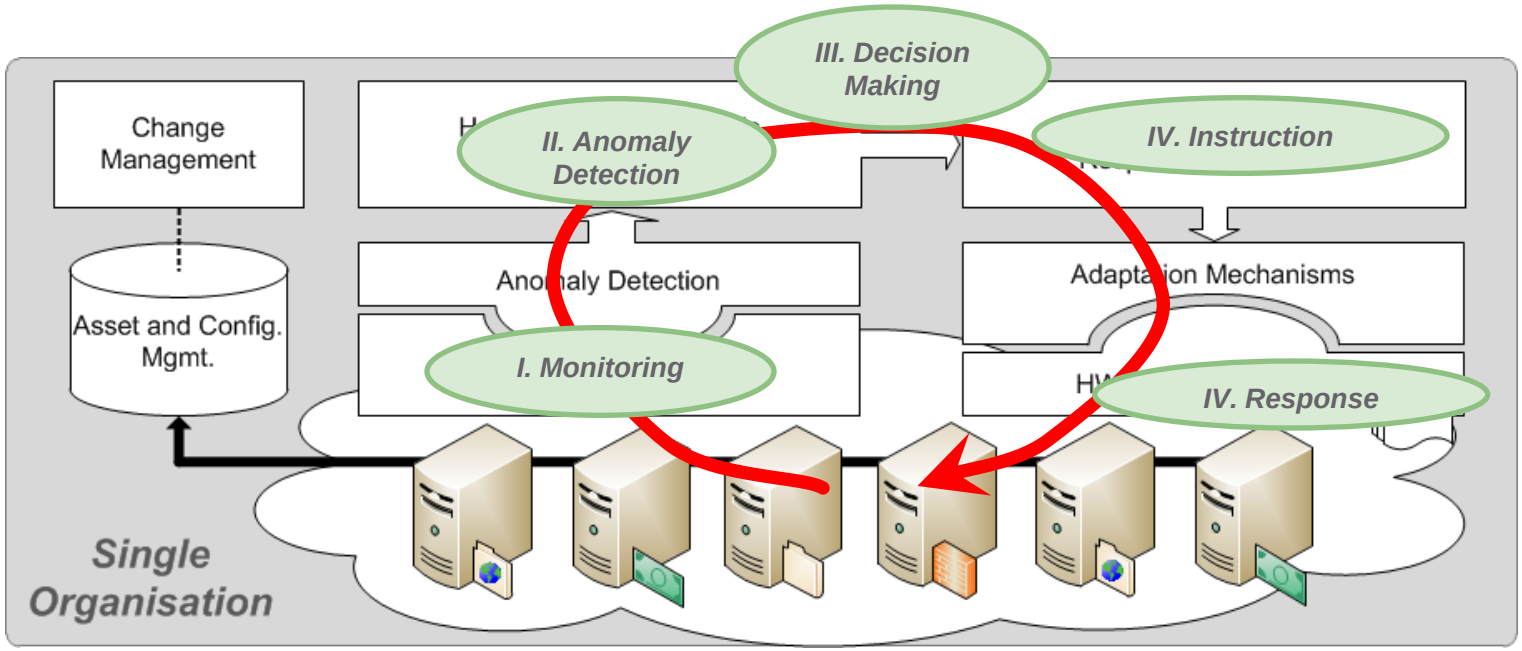
Re-Active Simulation

- **Evaluation** of potential causes and **effects of discovered attacks**
  - Probability that a detected anomaly is actually an attack?
  - Potential effects on the overall national infrastructure?



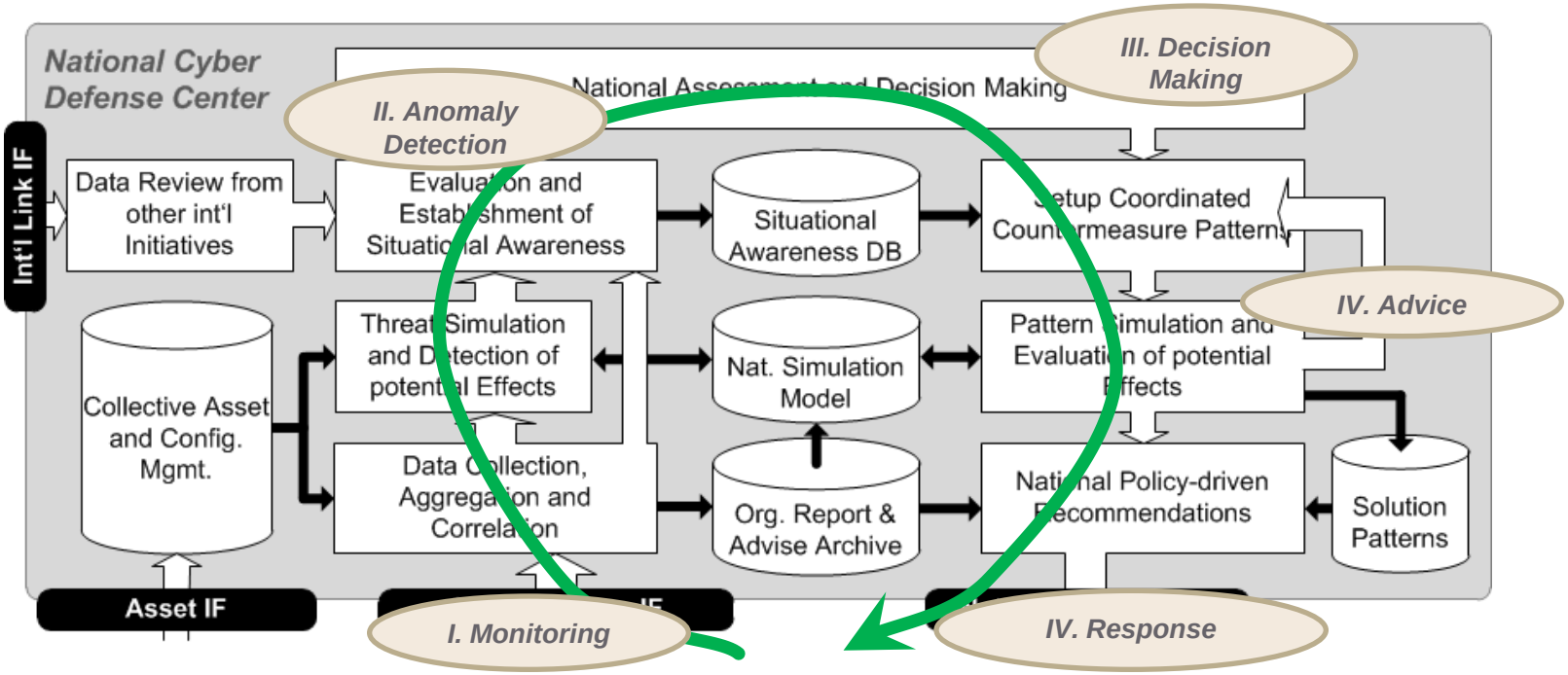
- Simulation
  - Input
    - Current infrastructure models (services, dependencies, …)
    - Current network data (abstract view; including usage of critical services etc.)
    - Explicit information about detected attacks towards a service
  - Output
    - Potential effects on other services (e.g., cascading effects)
    - Support for root cause analysis
- Ultimate Goal: Learn more about **currently ongoing large-scale attacks** to better predict their impact on other services.

CAIS Architecture – Organizational Lvl.



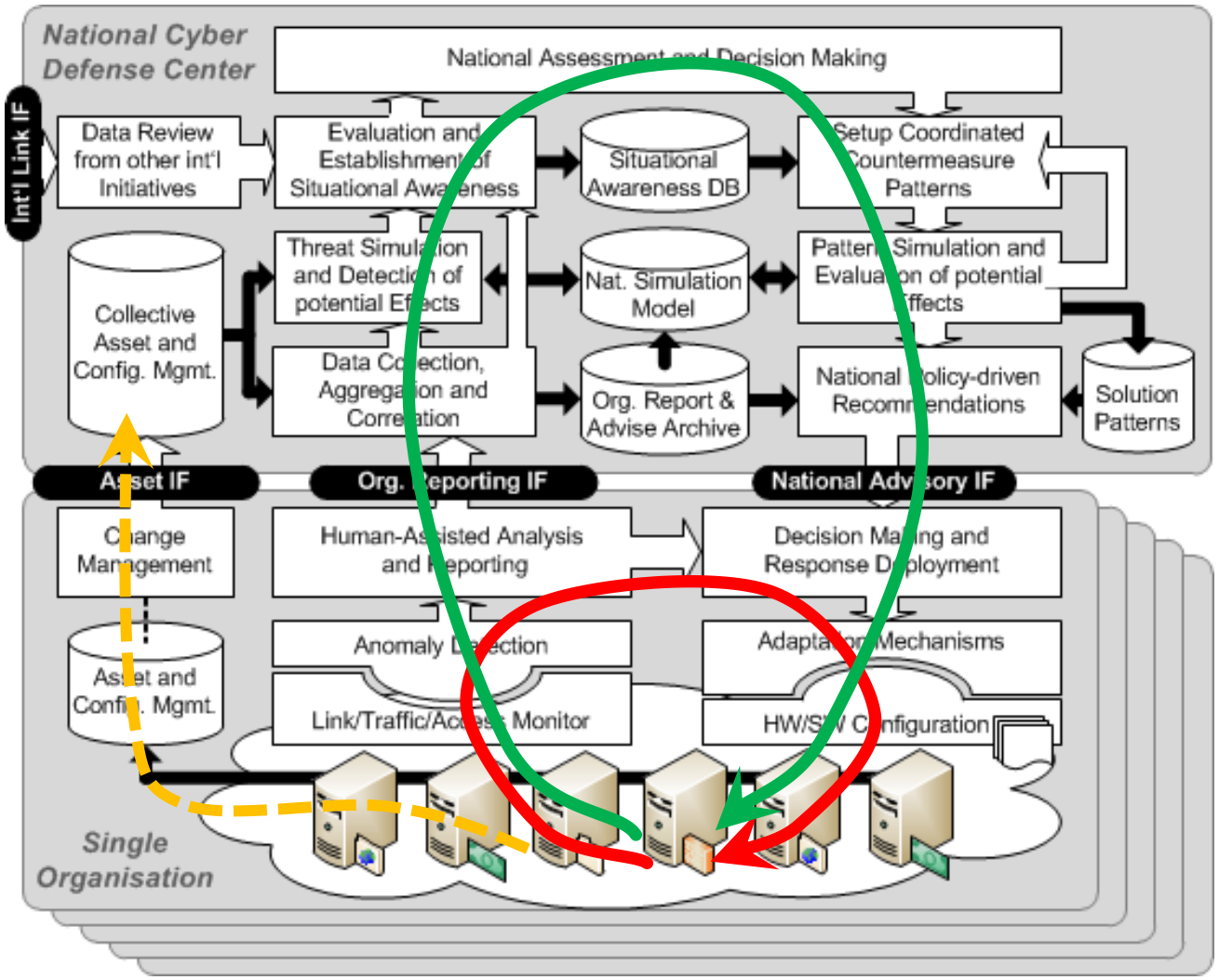
- "Conventional" **incident response** cycle on **organizational** level
- Local **monitoring** of services
- Local **anomaly detection**
- **Fast** (local) **response** based on decisions within org. boundaries
- Local asset management
- Periodic **reporting** to cyber defense center (assets, anomalies, attacks)

CAIS Architecture – National Level



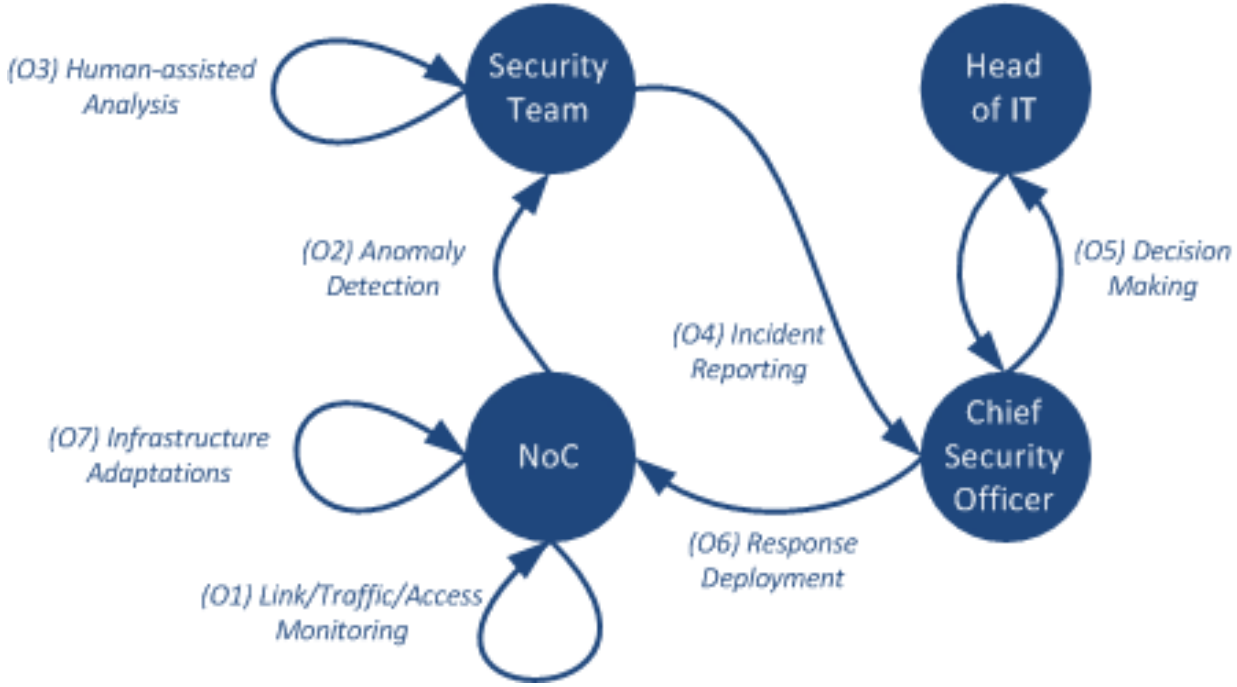
- Collective asset management (abstract level)
- **Holistic simulation** and centralized evaluation → national situational awareness
- **Complex threat analysis** (e.g., distributed attacks) to infer **consequences** of a single attack (e.g., towards a single point of failure)
- **Simulation** of **potential future threats** to prepare countermeasures and emergency plans
- **Planning** coordinated **counter measures** and facilitating **information sharing**

CAIS Architecture – Combined View



CAIS Roles – Organizational Level

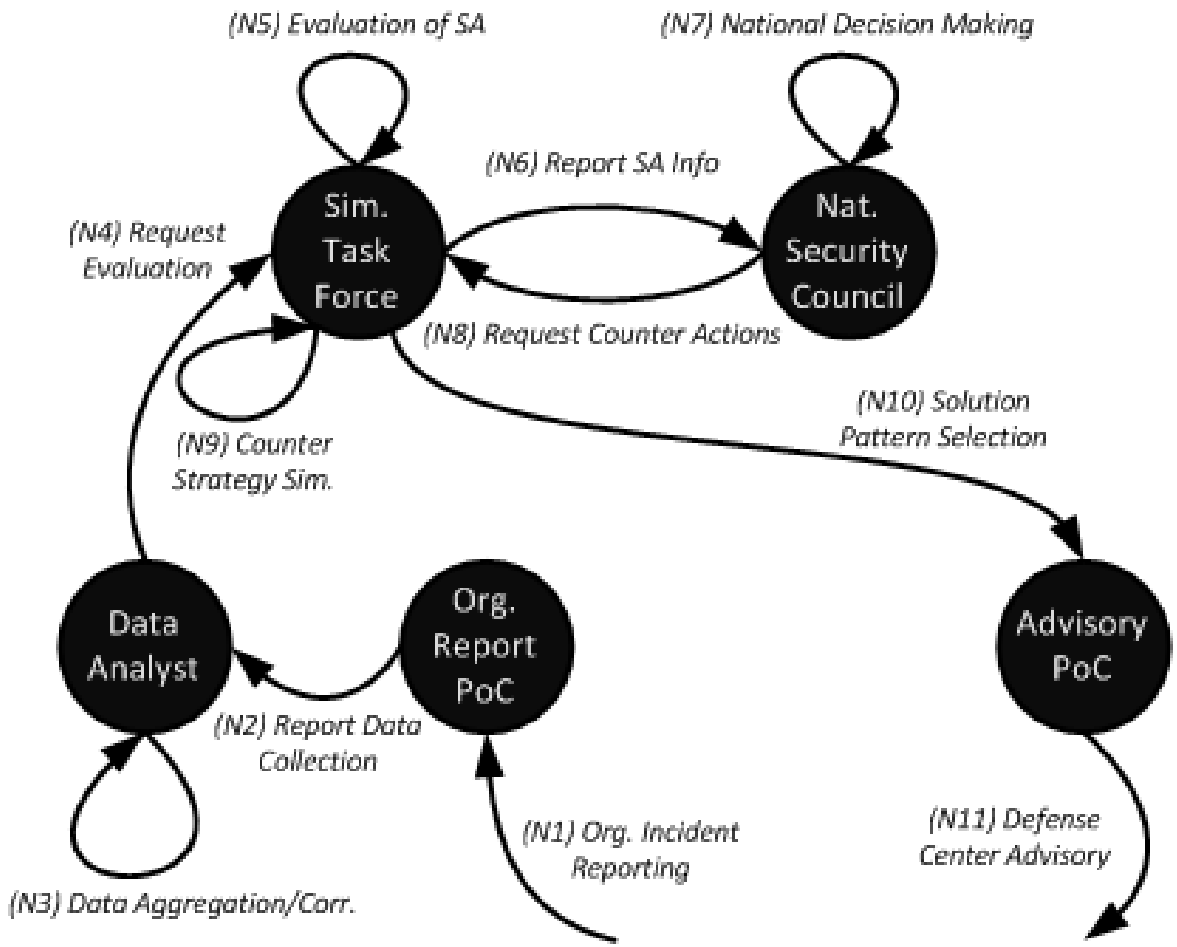
- Involved roles for **fast and effective incident response**
  - Periodically run through O1to O7
- Roles and responsibilities designed to fit into most existing organizational structures
  - Typically there is a 1:n mapping from roles to persons



NoC = Network Operating Center

CAIS Roles – National Level

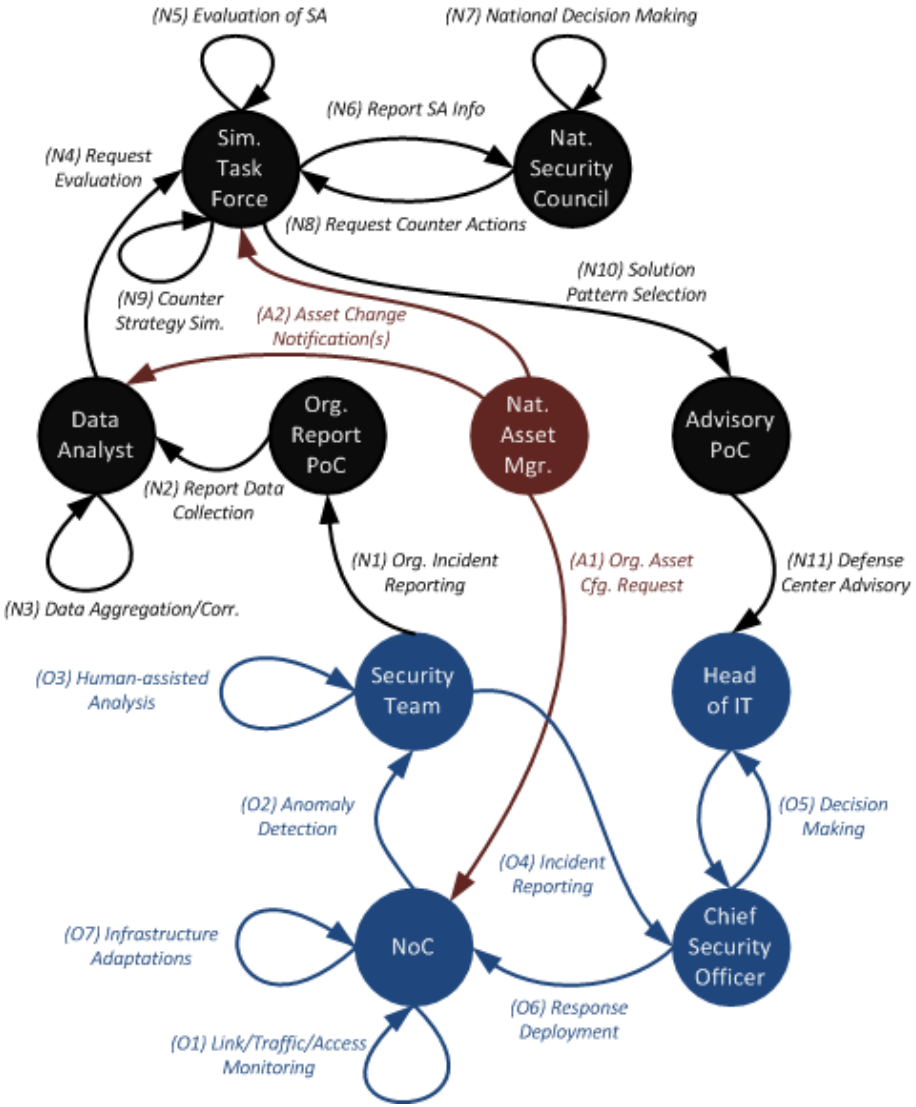
- Involved roles for **long-term strategic evolution of the national ICT infrastructure**
  - Periodically run through N1to N11
  - (N1): reporting from organization
  - (N11): advisory to organization



PoC = Point of Contact

CAIS Roles – Combined View

- Connecting roles on organizational and national level
- Additionally introduce national asset management (red)
  - Requesting information about organizational assets on demand, which are relevant for national data analysis and simulation purposes



Multi National Experiment 7 (MNE7) (1)

- Military Experiment in several dimensions
  - Maritime, Air, Space, **Cyber,** Inter-Domain Understand./Planning
  - Participants: AUT, CAN, CHE, DEU, DNK, ESP, FIN, FRA, GBR, HUN, ITA, KOR, NOR, POL, SGP, SWE, TUR, USA, and NATO
- Each Domain structured in numerous objectives. For the Cyber Domain the objectives are:
  - Threats, Vulnerabilities and Risk Analysis
  - Information Sharing
  - Legal Understanding
  - Enabling Technologies
    - ***Cyber Situational Awareness Standard Operating Procedure (SOP)***
  - Situational Awareness

Multi National Experiment 7 (MNE7) (2)

- Work in context of this **SOP** includes:
  - Cyber Center Roles and Responsibilities
    - Cyber Center SA Element
    - Cyber Center Execution Element
    - System Operator
    - Decision Maker
  - Cyber Center SA Process Model
    - Data Collection Phase
    - Analysis Phase
    - Informing Phase
  - Supporting Technologies
    - Monitoring Techniques
    - Anomaly Detection
    - Simulation and Forecast

Project Cyber Attack Information System

- National research project
  - Partly funded by the Federal Ministry for Transport, Innovation and Technology
- Project duration: 2 years, 2011-2013
- Aim: to study concepts, models and approaches for **setting up a national cyber center** in order to **keep track of ongoing incidents** on a national level and establish/maintain **situational awareness**.
- Partners: from research, industry, and the government
  - AIT Austrian Institute of Technology
  - Bundeskanzleramt Österreich (The Federal Chancellery)
  - Bundesministerium für Landesverteidig. u. Sport (Ministry of Defence and Sports)
  - Bundesministerium für Inneres (Federal Ministry for the Interior)
  - FH St. Pölten (University of Applied Sciences)
  - OIIP Österreichisches Institut für Internationale Politik
  - T-Mobile Austria
  - T-Systems Austria
  - NIC.AT / CERT.AT
- Web: http://www.kiras.at/gefoerderte-projekte/detail/projekt/cais-cyber-attack-information-system/

Discussion and Conclusion

- Since **cyber attacks become** increasingly sophisticated and **coordinated**, there is a strong **need to** also **coordinate defence** mechanisms
- **Situational awareness is key** to even detect attacks
- Infrastructure **modeling and simulation** is a central mechanism to **prepare against future threats**
- **Close collaboration** of all parties in the digital society is mandatory
  - **Private organizations** providing status reports about ongoing activities; in turn, they receive information about others in the same domain or having similar infrastructure assets.
  - **Government** evaluates the “health status” of critical infrastructures on a national level, accounting for interdependencies, and predict possible consequences of detected anomalies.
- Future Work: Currently the implementation of various introduced concepts is on-going. First evaluation results end of 2012. For more information pls. contact me (next slide).

Thank you.

florian.skopik@ait.ac.at

Dr. Florian Skopik
Future Networks and Services
Safety & Security Department
Austrian Institute of Technology

florian.skopik@ait.ac.at | +43 664 8251495 | www.ait.ac.at/it-security