Cyber Incident Management and Cyber-Resilience of CCI

Integration of AI/ML & Digital Twins in the Electric Power Ecosystem

Senter for integrert krisehåndtering (CIEM)

Nadia Noori, PhD
Førsteamanuensis i Institutt for IKT
Forsker, Senter for integrert krisehåndtering
Universitetet i Agder

UiA

CIEM er et tverrfaglig forskningssenter ved UiA

Involverer 25 forskere innen teknologi og samfunnsvitenskap, med felles fokus på hvordan beredskap og krisehåndtering kan effektiviseres ved bruk av ny teknologi.

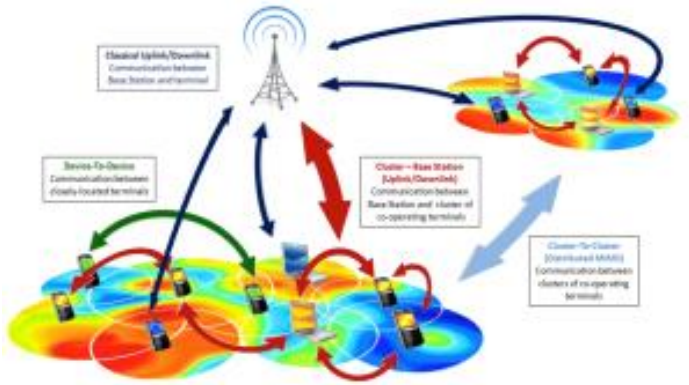
Toppsatsingsområde ved UiA siden 2014

Integrert krisehåndtering:

- Integrasjon av informasjon fra ulike kilder
- Integrasjon mellom fagområder
- Integrasjon mellom forskning og praksis
- Integrasjon av lokal og global kunnskap

Kompetanseområder i CIEM

- Informasjonsdeling og samhandling
- Dataanalyse og beslutningsstøtte
- Cybersikkerhet og kritisk infrastruktur
- Sosiale medier og krisekommunikasjon
- Sensorteknologi og mobil kommunikasjon
- Simulering og kunstig intelligens
- Teknologi-innføring og evaluering



Do we know anything about cyber security responders?

1. Are attacks happening?

2. What might be their origin?

3. What might the attackers be trying to do?

4. What might the attackers do next?

5. Is deception and/or counter-deception involved?

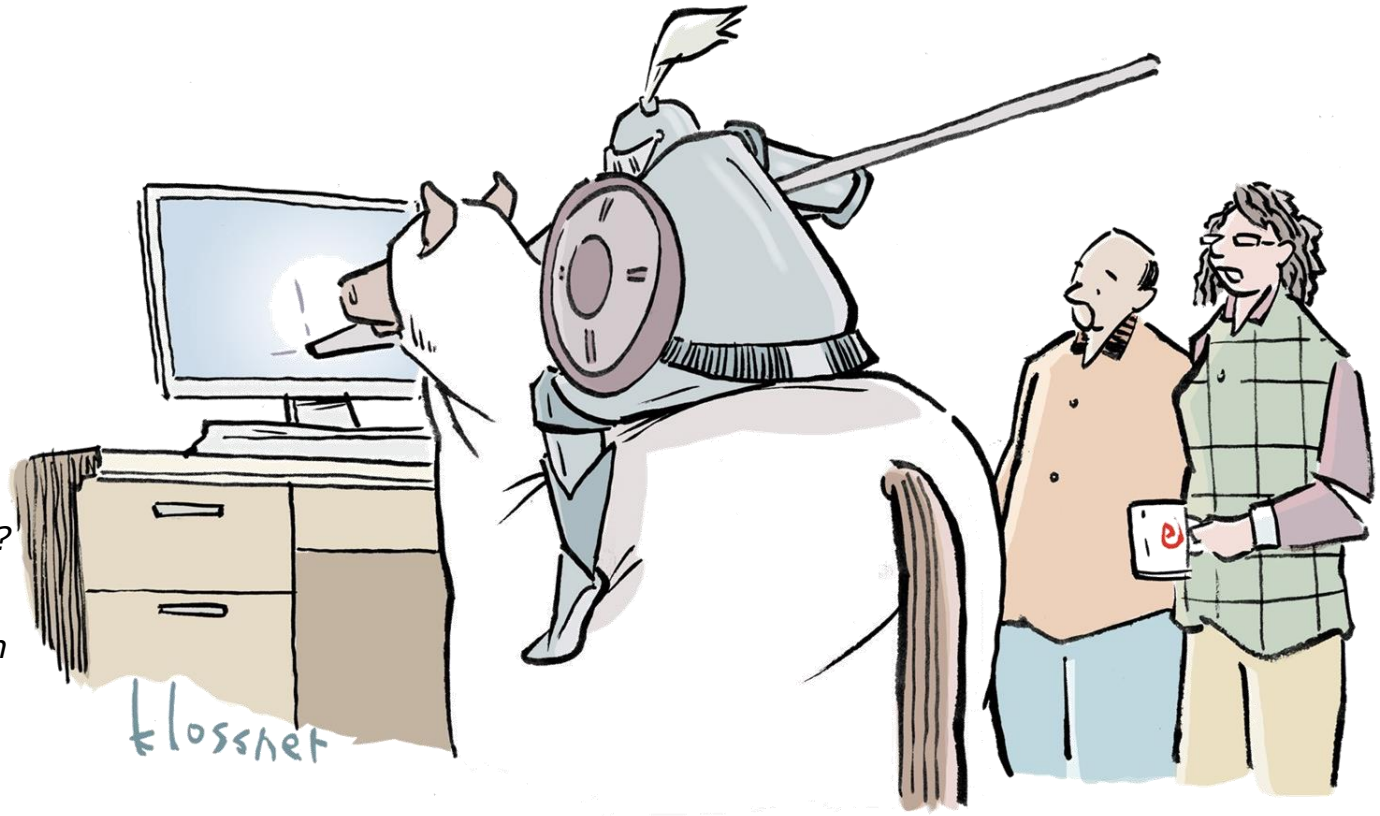
6. How might the attacks affect my mission now, and how might they affect it in the future?

7. What options do I have to defend against these attacks?

8. How effective will a given option be against these attacks, what effect will be exercising it have on my mission, and how is it likely to affect the future actions of allies and adversaries?

9. Might a defensive action "give me away"?

10. How do I prevent or mitigate the impact of such attacks in the future?



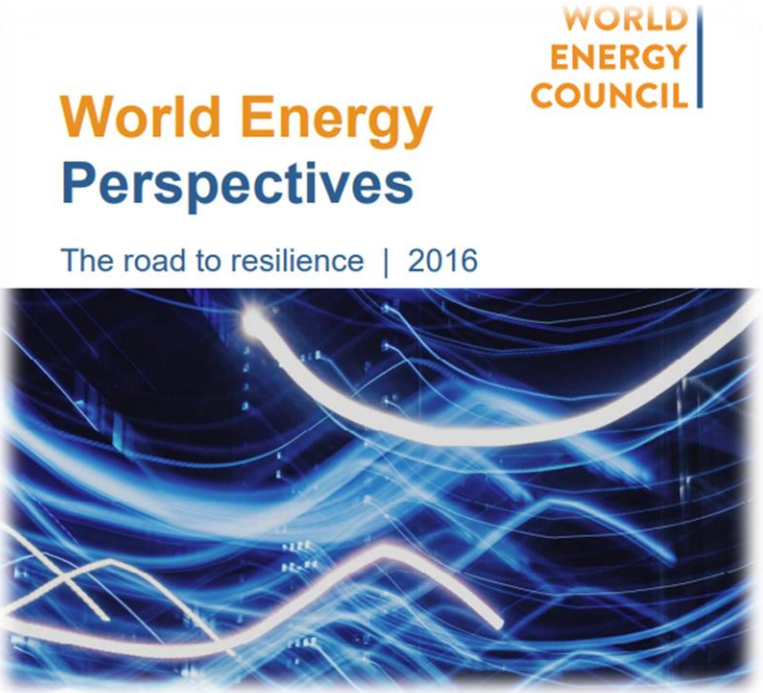
Crisis response, OT systems and sensemaking

"Cyber-attacks in the energy sector have an impact not only on the sector itself, but on the wider economy and the whole fabric of a state."

World Energy Council, "World Energy Perspectives The road to resilience," 2016, p7.

Research on cybersecurity focus on technical and managerial planning (before the threat materializes)

- A series of mechanisms to ensure an effectively balanced incident prevention and response strategy to maximize CCIs resilience.
- Preventive systems for managing predicted threats
- Response systems to diagnose/mitigate unpredicted threats, containing spill-overs
- All the above need to address both technical and business continuity issues by design



Context

A multidisciplinary research teams engaged in a process to design an efficient incident prevention and response system tailored to the needs of the electrical power sector.

- In 2020, CIEM-UiA coordinated the development of an EU project proposal involving nineteen partners including four universities, two research institutes, and six companies managing electrical power transmission and distribution grids
- Goal:
  - Design an incident-centered approach able to bridge between response paradigm and prevention paradigm through a double-loop process of learning.
  - Generate a process model addresses challenges identified by combining concepts from crisis management, information systems security, and advanced technologies (Industry 4.0) .

- Publication in Computers & Security in October 2021, by Andrea Salvia1, Paolo Spagnoletti, Nadia Saad Noori
  - *Department of Business and Management, Luiss University, Rome, Italy*
  - *Center for Integrated Emergency Management, University of Adger, Kristiansand, Norway*

Challenges to the Energy Sector

As identified by the Energy Expert Cyber Security Platform (EECSP) sepert group:

- **Stability** of grids with particular attention to **cross-border** networks.
- **Protection** concepts reflecting **current** threats and risks.
- Handling of **cyber-attacks** within the **EU**.
- **Effects** by **cyber-attacks not fully considered** in the **design rules** of an existing power grid.
- Introduction of new highly **interconnected technologies** and **services**.
- **Outsourcing** of infrastructures and services.
- **Integrity** and **reliability** of components used in energy systems.
- Increased **interdependency** among market players.
- Availability of **human resources** and their **competences**.
- **Constraints** imposed by **cybersecurity** measures in contrast to **real-time/availability** requirements.

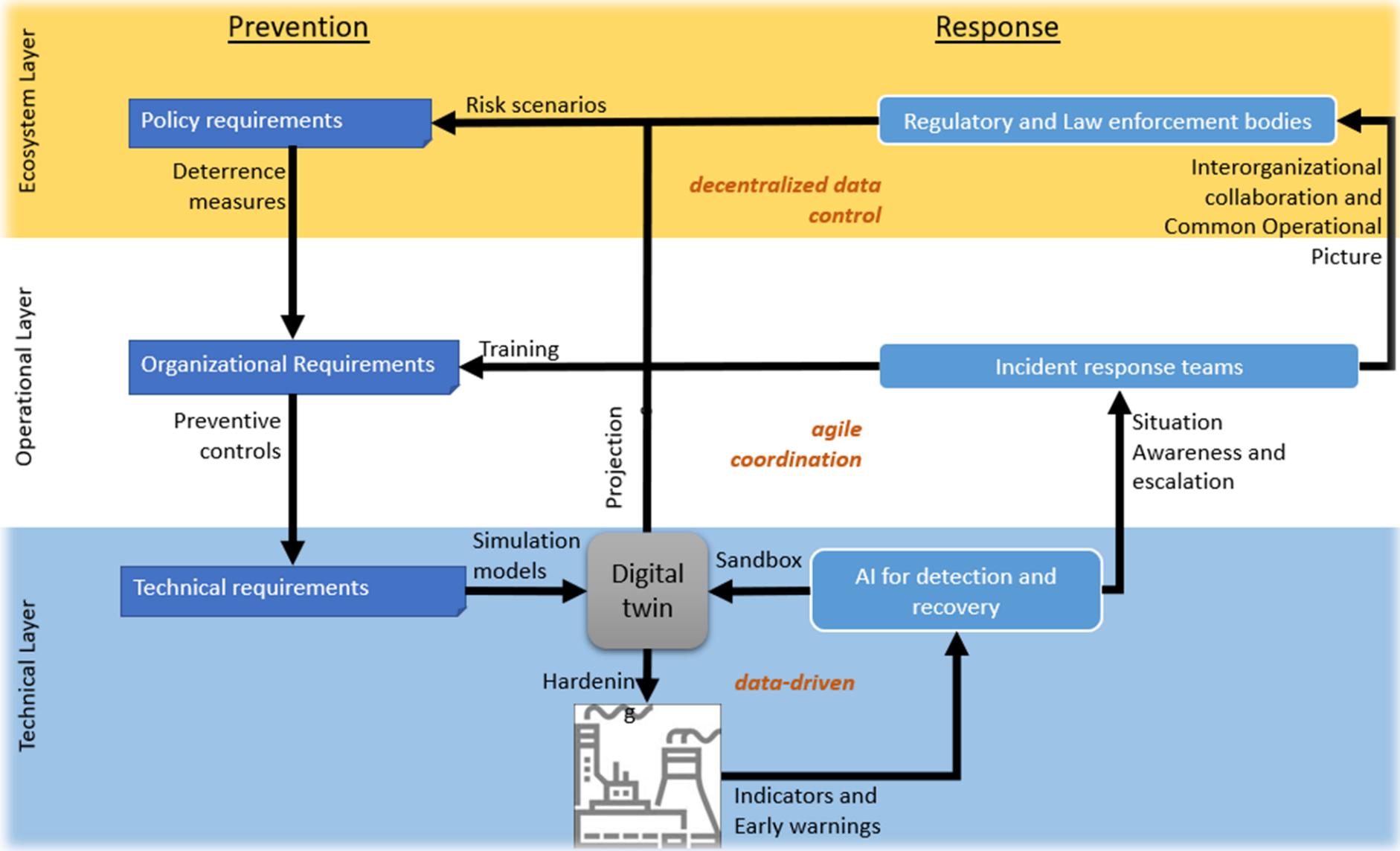
Prevention and Response paradigms matched to electrical CCIs salient issues

Paradigms	Salient Issues	Enablers
Prevention	Develop adequate **capabilities** to **detect** the nature of the threat	Technological artifact (e.g., Threat Intelligence suites)
	Identify the **Threat Agent**	Interorganizational and intraorganizational information sharing
	Identify the **different level** of handling based on **nature and agents of the threat** (Operators, Countries, Transnational Actors)	Preventive Intelligence Training
Response	Develop adequate **Crisis Management Capabilities**	Technological artifact (e.g., anomaly detection suites)
	Develop adequate **Cyber Response Capabilities** through a structured response cycle (preparation, detection and analysis, containment, eradication, and recovery)	Interorganizational and intraorganizational information sharing.
	Post-incident activity with an **interorganizational** two-loop **learning** feedback.	Case-driven containment and remediation training

Requirements derived from the interactions with end-users and operators in the electrical power ecosystem

Requirements	Motivation
Cost-effectiveness **Scalability**	Maximize implementation to a vast host of end-users and operators in the power grid ecosystem
State-of-the-art Technological Artefacts	Increase durability and self-improvement of the system as well as the involvement of the broader cybersecurity community.
Customizable and adaptable to the organizational needs	Given the variety of actors that the model brings in, it needs to be easily adaptable and customizable to match their strategic, operational needs.
Able to support trans-border CCIs	Need to integrate critical trans-border CCIs fostering collaboration between a wide variety of actors (governments, end-users, operators).

Cyber-resilience model for critical cyber infrastructure



Cyber-resilience model key construct

Type of learning	Outcomes	Agents/structures
Data-driven	• Indicators and Early Warnings • Simulation models • Hardening • Sandbox	• **AI/ML, DSS** for detection and recovery • Technical requirements • **Digital twin**
Agile coordination	• Situational Awareness and escalation • Training • Preventive controls • Simulation models	• **AI/ML, DSS** supporting coordination, communication, control & intelligence (C3I) • **Digital twin**/cyber range • Incident response teams • Organizational requirements
Decentralized data control	• Interorganizational collaboration and Common Operational Picture • Risk scenarios • Deterrence measures	• **System dynamics** supporting policy evaluation, maturity models • **Digital twin** • Regulatory bodies • Law enforcement agencies • Policy requirements

Conclusion

- An **incident-centered** approach to cyber-resilience in CCIs needs to consider the **strong ties** between firms and institutions, i.e. an **ecosystems perspective**, describing interdependencies of cyber incident on the three levels: **operational, intra-organizational and ecosystem**.
- Cyber-resilience in CCIs can be improved through **integration** of AI/ML & digital twin supporting prevention and response by fostering **organizational and inter-organizational learning**.
- **Effective** cyber-resilient model in CCIs entails both **organizational and technical** means to **augment Situational Awareness (SA)** and forge an **inter-organizational Common Operational Picture (COP)**.
- A **new role** to the regulatory frameworks, **regulations and norms** are progressively veering to a more "**standard setting role**" as they define the requirements, those norms de facto **absorb inputs** from the **ecosystem** and become more **preventive** in nature.
- CCIs as **complex** cyber-physical systems suggests a **novel and innovative approach** to risk management in digital operations where integration of ML/AI & digital twin would lead to **enhanced preparedness**, **situational awareness** and **agile incident response** by increasing the **data-driven** nature of **cybersecurity operations**
- Best practices and methods **integration** from conventional disaster management into the cybersecurity fields is necessary to develop **procedures** for **information exchange**, **coordination** between **teams and organizations**, and **integrating** new **technologies** for cyber incident management.
- **Summative** evaluation of the **full model** is a **long process**, and requires **extensive research** and development efforts to be carried out by **multidisciplinary teams** from engineering, information management, data science, information, and systems security and finally, simulation and training in the **disaster management context**

Tusen takk!
Thank you!

UiA