KTH VETENSKAP OCH KONST

sp network Safe Places

Preventing crime in hyperspaces

digital futures

pixabay

In this seminar...

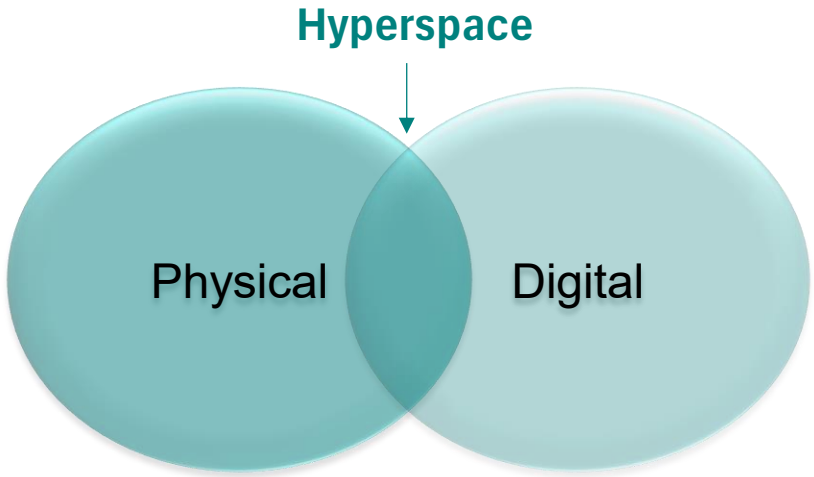
We begin by introducing the concept of hyperspaces and examining the unique cybersecurity risks arising from interactions between online and physical environments.

In this seminar, we focus on **transportation systems** and on integrating the concepts of hyperspace into urban planning and policy-making.

What is hyperspace?

Hyperspaces intersect the online and physical worlds (Brantingham & Brantingham, 2015; Bichler, 2019).

They are ‘places’ where threats are not only spatial but networked and systemic.
They may also be associated with online environments, such as the dark web or social media, where identity, location, and legality are fluid.
They can mean attacks on transportation systems



Social interactions

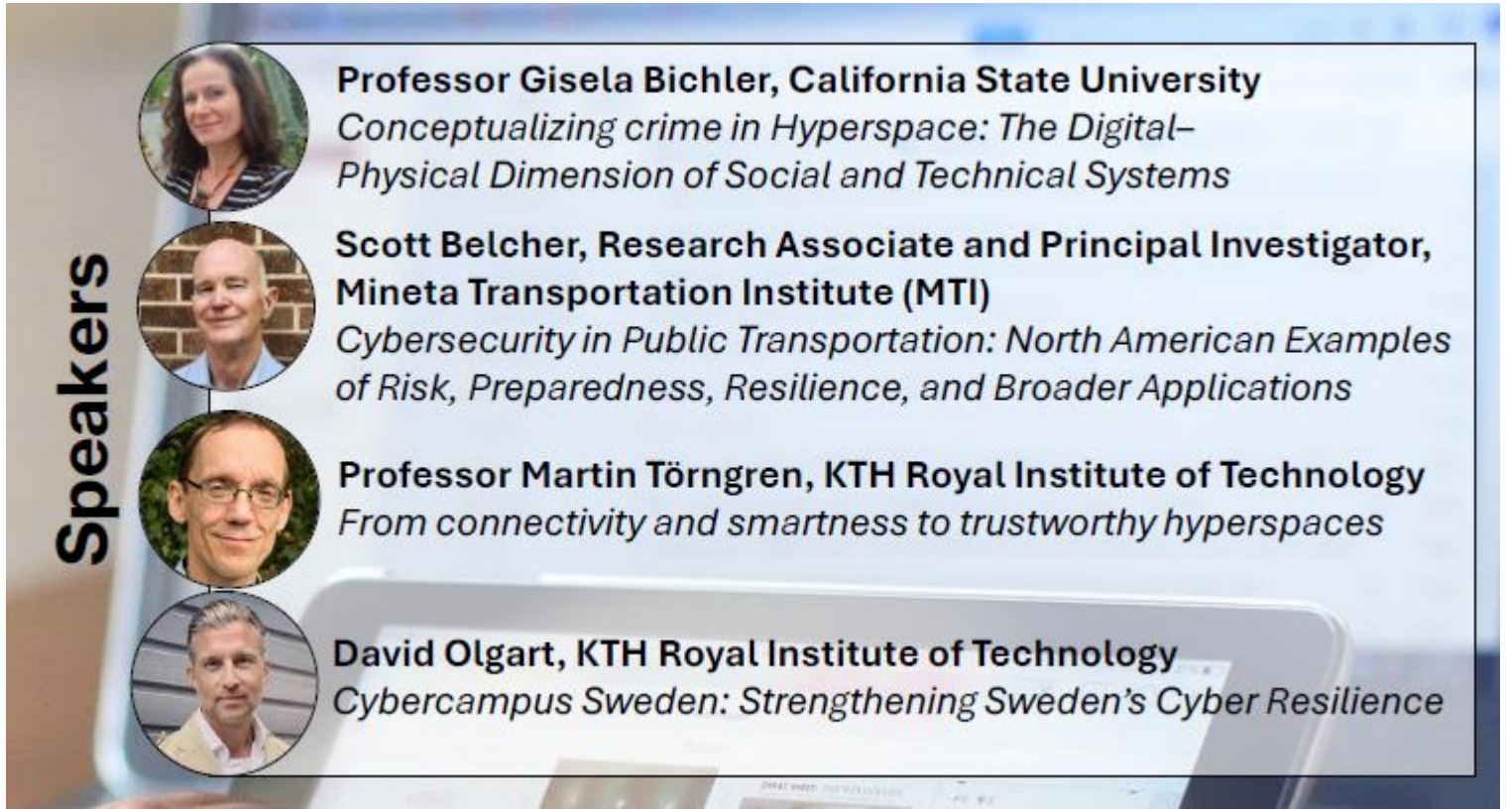
Including illegal activities

Crime = an action or omission which constitutes an offence and is punishable by law.

Crime and crime prevention

- What new forms of crime are made possible by the digital-physical system?
- Who holds responsibility for prevention in these blended environments?
- How prepared are we to deal with these crimes?

Speakers and program



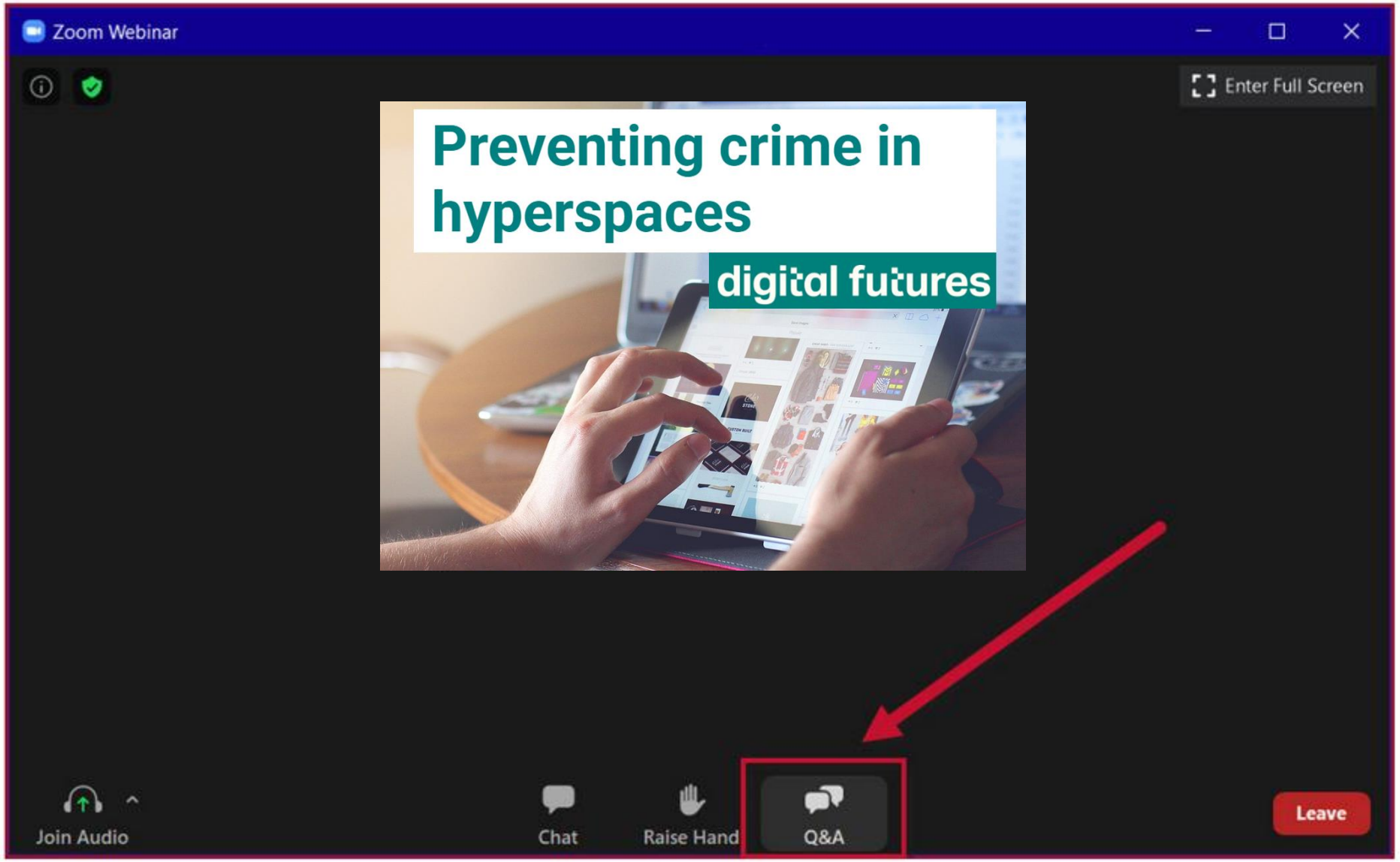
Discussant: Alpay Aksoy,
Stockholm region

20 min break

Discussant: Emre Süren,
Royal Hacking Lab at KTH

Final discussion

Enter your question using Q&A function



Organisers/sponsors

nätverket

Prof Vania Ceccato, KTH, ABE
Network Safe Places
vace@kth.se

Organisation team:

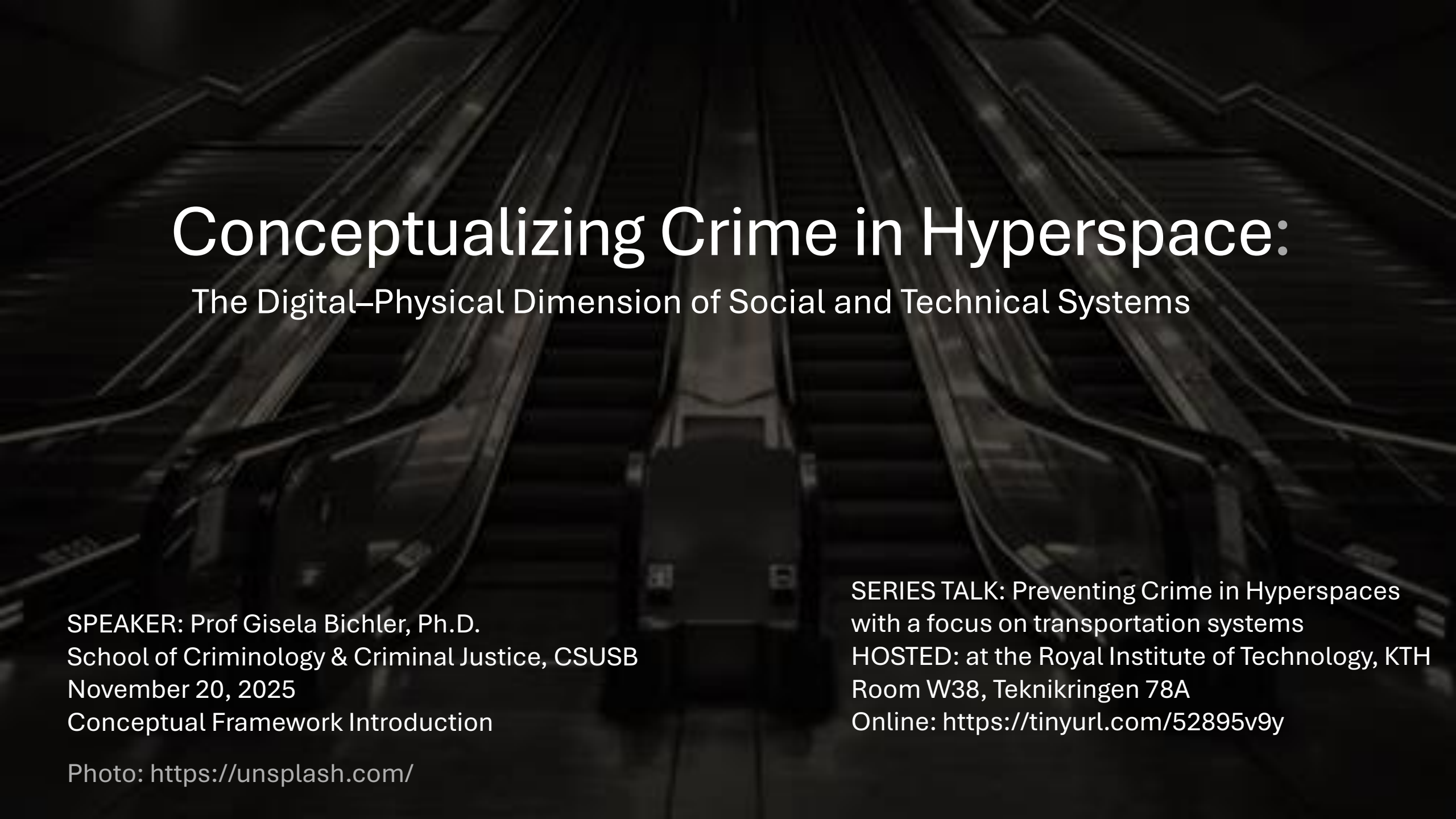
Dr Ioannis Ioannidis
Dr Jonatan Abraham
Gabriel Gliori
Alvar Almgren
Lisa Josefsson

digital futures

Vendela Hasselberg

Professor Gisela Bichler, California State University

Conceptualizing crime in Hyperspace: The Digital–Physical Dimension of Social and Technical Systems



Conceptualizing Crime in Hyperspace:

The Digital–Physical Dimension of Social and Technical Systems

SPEAKER: Prof Gisela Bichler, Ph.D.
School of Criminology & Criminal Justice, CSUSB
November 20, 2025
Conceptual Framework Introduction

SERIES TALK: Preventing Crime in Hyperspaces
with a focus on transportation systems
HOSTED: at the Royal Institute of Technology, KTH
Room W38, Teknikringen 78A
Online: https://tinyurl.com/52895v9y

Photo: https://unsplash.com/

Cybersecurity in Public Transportation: U.S Examples of Preparedness, Resilience, and Broader Applications

Scott Belcher
Research Associate and Principal Investigator,
Mineta Transportation Institute, and
Co-Founder, Cybrbase

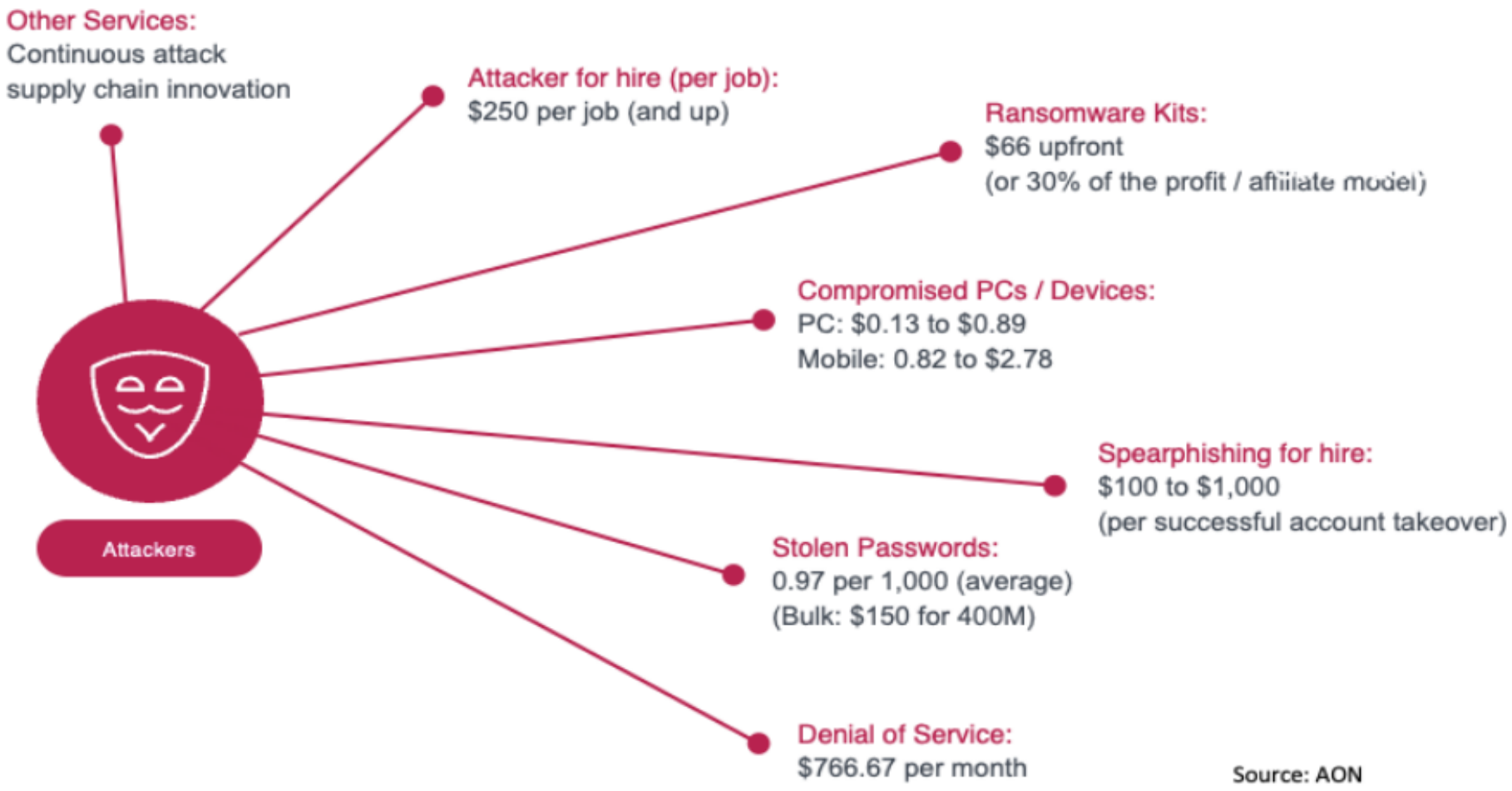
What Does the U.S. Transportation Cybersecurity Landscape Look Like?

- U.S. Department of Transportation is the major federal agency overseeing all modes of transportation ($145B a year; 56,000 employees). There are multiple other federal agencies that have a direct impact on transportation operations
- There are 50 State Departments of Transportations($213B; 300,000 employees)
- There are roughly 19,000 cities; 6,800 transit agencies; 3,000 counties; and 400 metropolitan planning organizations all with transportation responsibilities in the U.S.
- There are over 62 federal agencies as well as thousands of local agencies with cybersecurity responsibilities

Changes in U.S. Approach to Cybersecurity: Uncertainty, Decentralization and Focus on Private Sector

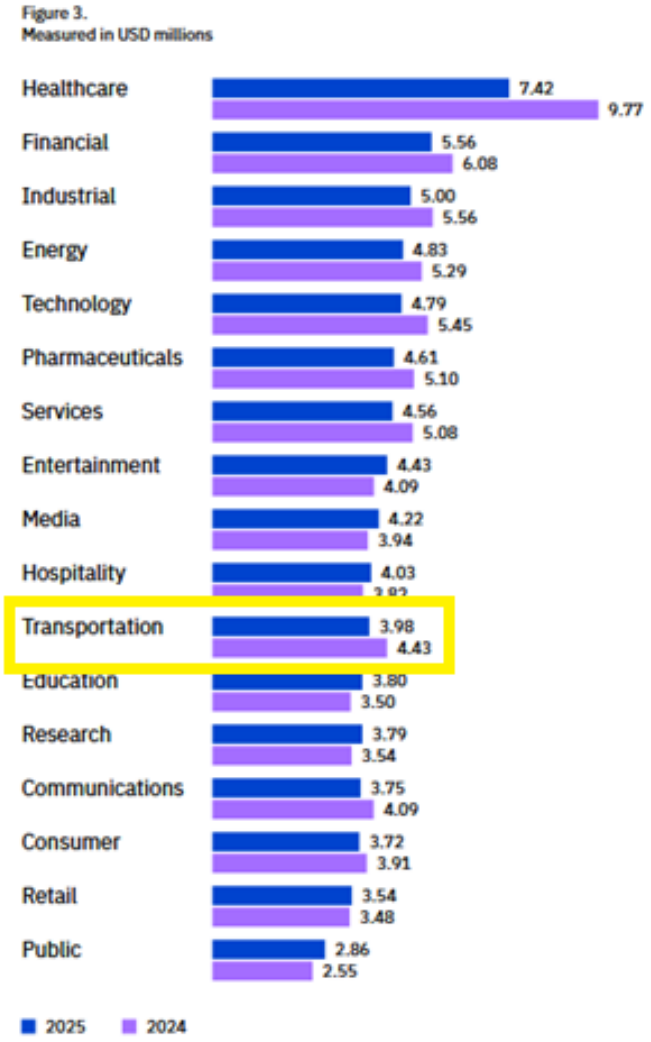
- New Executive Orders focusing on Artificial Intelligence vulnerability management and a rollback of previous Administration priorities
- Decentralization of responsibilities from Federal Government to State and Local Governments
- Reduction in domestic corporate cybersecurity obligations
- Greater focus on national security
- Greater focus on secure software development, security, and operations practices
- Major leadership, organizational, and funding changes

Changing Cybersecurity Threat Landscape



Source: AON

What is at Stake for Transportation?



Source: IBM 2025 Cost of a Data Breach Report

Public Transportation remains a high target. The average cost of a breach between 2024 and 2025?

$4.2 Million

Since the 2020 MTI study, there have been numerous publicly disclosed cyber incidents in transit, resulting in public distrust, service disruption, and substantial financial loss.

At an average cost of $4.2 million per breach, this eclipses a small, rural transit agency's **entire annual operating budget**.

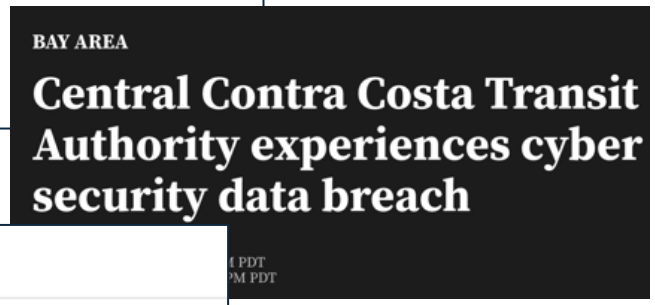
Cybersecurity Attacks Are on the Rise

METRO (WMATA)

A cyberattack took down Metro's website for two hours. Here's what a cybersecurity expert says

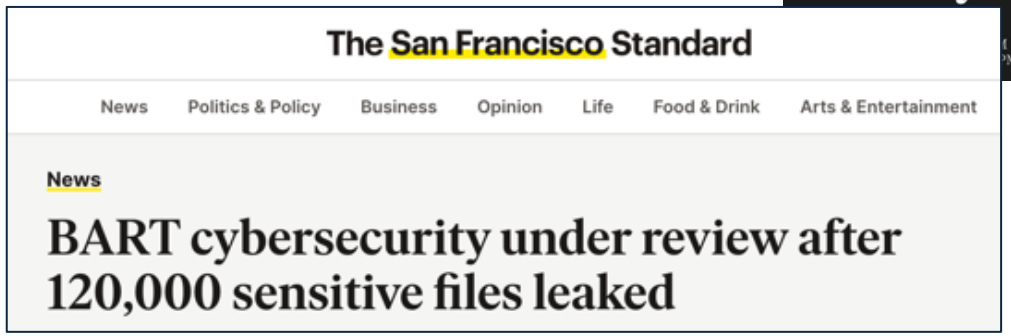
"So what they're trying to do is, hackers are trying to flood your network so you can't operate," cybersecurity expert Steve McKeon told us

By Adam Tuss, News4 Anchor & Transportation Reporter • Published May 14, 2024 • Updated on May 14, 2024 at 7:54 pm



BAY AREA

Central Contra Costa Transit Authority experiences cyber security data breach

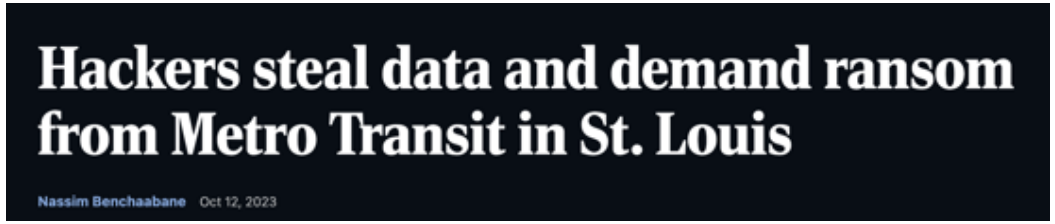


The San Francisco Standard

News Politics & Policy Business Opinion Life Food & Drink Arts & Entertainment

News

BART cybersecurity under review after 120,000 sensitive files leaked



Hackers steal data and demand ransom from Metro Transit in St. Louis

Nassim Benchaabane Oct 12, 2023

RIPTA
RHODE ISLAND PUBLIC TRANSIT AUTHORITY

valley regional transit

MTA

SEPTA

TheBus
HEA

TORONTO TRANSIT COMMISSION

TheRide
Ann Arbor Area Transportation Authority

metro

Maryland Transit Administration

- Maryland Transit Administration (MTA), a subdivision of the Maryland Department of Transportation, is the one of the 20 largest transit agency in the U.S. and provides almost 100M unlinked trips per year.
- In 2025, the MTA suffered a ransomware attack by a criminal group called Rhysida who stole resident's sensitive personal data and threatened to place it on the dark web.
- Rhysida demanded 30 Bitcoin (@$3.3M) which the state refused to pay.
- The state is still working with the affected individuals.
- The attack also disrupted real-time bus tracking systems; temporarily impacted paratransit operations (forced to rely on a manual work around), and affected their service operations, information systems, including real-time information and call centers, thus their ability to communicate with their customers.
- MTA is still dealing with the fall-out of this attack.

Texas Department of Transportation

- TxDOT is the largest state DOT in the U.S. in terms of lane miles and among the largest in terms of budget.
- In 2025, TxDOT experienced a data breach where hackers accessed 300,000 crash reports resulting in the improper disclosure of sensitive personal information.
- Likely compromised through phishing or credential reusem and part of a ransomware attack.
- The compromised account was immediately blocked, and an internal and external forensic investigation began.
- Was the catalyst for the creation of the Texas Cyber Command.

Bay Area Rapid Transit (BART)

- BART is one of the 20 largest transit agency in the U.S. and provides about 130M unlinked trips a year.
- During final review of a 2018 metro extension, BART's cybersecurity team identify over 1,000 corrupted Cisco devices.
- Cisco has a cradle to grave tracking system for its devices and the the BART team determined that the devices in question had been decommissioned by a hostile nation, rebuilt with hidden back doors to the devices, and resold on the internet.
- Because of their relationship, BART and Cisco were able to replace the compromised devices quickly.
- Resulted in an on-going international criminal investigation impacting more than 20 transit agencies.

“We are the good guys, and we have nothing. Why would they hack us?”

- A Community Action Agency (CAA) is a small, local organization in the U.S. that provides services to low-income people. Service can include transit.
- In 2021, the transit operation of a CAA was compromised by a phishing attack and subject to a ransomware demand. The state in which the CAA was located did not allow the payment of ransom.
- The transit operations was a total of five people, with two servers, one that housed their customer date. The transit agency lost all their customer data and was forced to rely on historic paper documents and the personal information was put on the dark web.

Mineta Transportation Institute Research: Transit Agencies Are Not Cyber Resilient

- **Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness**, S. Belcher, T. Belcher, Greenwald & Thomas, Mineta Transportation Institute Publications, September 2020.
- **Implications of the Sunburst Cybersecurity Attack on the Transit Industry**, Belcher & Thomas, Mineta Transportation Institute Publications, January 2021.
- **Will the Biden Administration's 'Made in America' Executive Order Present Significant New Cybersecurity Obligations for Transit Operators?,** S. Belcher, H. Belcher, Seckman & Thomas, Mineta Transportation Institute Publications, June 2021.
- **Personal Data Protection as a Driver for Improved Cybersecurity Practices in U.S. Public Transit,** Seckman, Thomas, H Belcher & S Belcher, Mineta Transportation Institute Publications, December 2021.
- **Aligning the Transit Industry and Their Vendors in the Face of Increasing Cyber Risk: Recommendations for Identifying and Addressing Cybersecurity Challenges,** Belcher, Belcher, Seckman, Thomas & Yaqub, Mineta Transportation Institute Publications, July 2022.
- **Is There a Light at the End of the Tunnel? The Outlook for Cybersecurity Insurance and Transit in 2024**, Belcher & Chollet, Mineta Transportation Institute Publications, April 2024.
- ➢ **Does the Transit Industry Understand the Risks of Cybersecurity and are the Risks Being Appropriately Prioritized?,** S. Belcher, T. Belcher, J. Grimes, L. Holmstrom, A. Souders, Mineta Transportation Institute Publications, May 2025.

The Problem in 2020

44%

Did not have a cybersecurity program in place

59%

Did not conduct cybersecurity assessments at least annually

43%

Did not provide annual cybersecurity training

Source: Mineta Transportation Institute 2020 Study

After the 2020 Study, the Authors Became Evangelists

- Testified before Congress multiple times
- Worked with multiple government agencies and trade associations
- Spoke at every transportation conference that would have us
- Created the Cybersecurity Assessment Tool for Transit (CATT) for the FTA
- Urged U.S. DOT and Congress to establish cybersecurity requirements for transportation
- Founded Cybrbase, Inc., where we developed a repeatable, web-based, cybersecurity assessment tool based on NIST CRR
- Helped dozens of transit agencies of all sizes with their cybersecurity challenges
- Continued to conduct research in the space

The Result . . . Four Years Later

	2020	2024	2024 <$5M
Have a cybersecurity policy	50%	55%	25%
Believe they have the resources to respond to an attack	47%	76%	N/A
Conduct annual security audit or assessment	50%	60%	15%
Either do not have/do not know if they have cybersecurity clauses in their vendor contracts	60%	54%	75%
Provide annual cybersecurity training	47%	55%	<10%

Source: Mineta Transportation Institute 2020 and 2025 Studies

Recommendations from 2025 Study

- Dedicate funding tor transportation cybersecurity programs
- Establish a statutory or regulatory mandate that transportation agencies have a cybersecurity program in place
- Establish a CEO attestation requirement
- Establish procurement language clarifying vendor cybersecurity obligations and liability
- Educate Executives and Boards about their fiduciary responsibility
- Educate transportation agencies about available resources

Cybersecurity Regulatory Requirements

- Transportation Security Administration (TSA) Security Directive 1580/82-2022-01: Rail Cybersecurity Mitigation Actions and Testing
- TSA Information Circular 2021-01, Enhancing Surface Transportation Cybersecurity
- New, standard discretionary grant Language
- Update of the Triennial Grant Manual
- Cybersecurity insurance market

Examples of Available Resources

Examples of Funding Resources

- Federal Transportation Administration (FTA) Formula Grant programs and Discretionary Grant programs
- Fund through State DOTs
- TSA Transit Security Grant Program
- Cybersecurity and Infrastructure Security Agency (CISA) State and Local Cybersecurity Grant Program

Examples of Free Resources

- FTA: Cybersecurity Resources for Transit Agencies
- TSA: Surface Transportation Cybersecurity Tool Kit
- CISA: Cyber Resource Hub
- American Public Transportation Association: Cybersecurity Resources
- State sponsored programs

Basic Recommendations for Transportation Agencies

- Develop an individualized cybersecurity plan and update it at least annually
- Conduct a cybersecurity assessment at least annually and address the shortcomings identified in that assessment in a timely manner
- Ensure that there are documented cybersecurity policies and procedures in place and that the organization is following them
- Ensure that there is at least one person on staff that is qualified to oversee the overall cybersecurity program and/or cybersecurity vendors
- These do not include technology solutions (e.g., penetration testing, threat monitoring, network segmentation)

After the 2025 MTI Study, Authors Were Again Challenged Again by the FTA and MTI

- Working with Illinois DOT and six of its partners, Cybrbase developed a Cohort-Based approach to conducting cybersecurity assessments
- Replicable, group-based cybersecurity assessment methodology
- Scalable across industry
- Drives down cost
- Fosters shared learning and best practices

How Does it Work?

State groups agencies into smaller cohorts that work together (6-10)

Initial policies and procedures workshop

Facilitated cohort assessment on replicable platform

Post-assessment workshop to identify common problems and actions

Follow-on support

Second facilitated assessment to determine progress

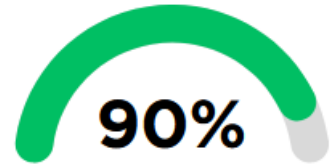
Referrals to technical support

Participants Have Seen Great Value

- Peer engagement and collaboration
- Strong buy-in from management
- Eliminates many excuses
- Heightened cybersecurity awareness within agencies
- Agency silos broken down
- Insurance milestone

Strong Impressions Thus Far

Of attendees found these sessions **beneficial**.



Found in-person assessment and common solutions workshop **very beneficial**.

Have begun discussions with internal/external teams to **tackle risks**.

Questions?

Scott Belcher
scottfbelcher@gmail.com
(703) 447-0263

MINETA TRANSPORTATION INSTITUTE

CYBRBASE

From connectivity and smartness to trustworthy (cyber-physical) hyperspaces

Martin Törngren, Professor in Embedded control systems
martint@kth.se; www.kth.se/profile/martint
Mechatronics and Embedded Control Systems,
Machine Design, KTH - Royal Institute of Technology

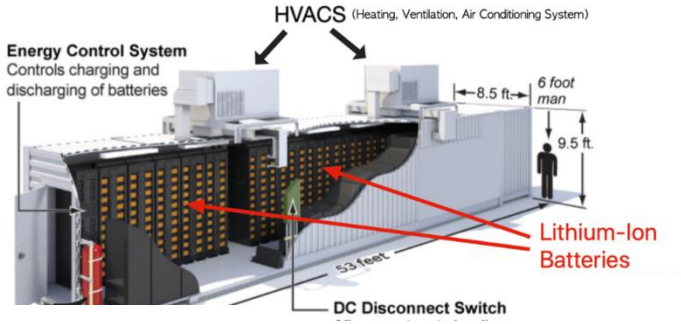
Towards smart and sustainable cities

Cyber Physical Systems (~2006)

Integration of computation, networking and physical processes where CPS range from minuscule (pacemakers) to large-scale (e.g. national power-grid).

Not new but with an increasing scale and new capabilities!

Cyber-physical systems - examples



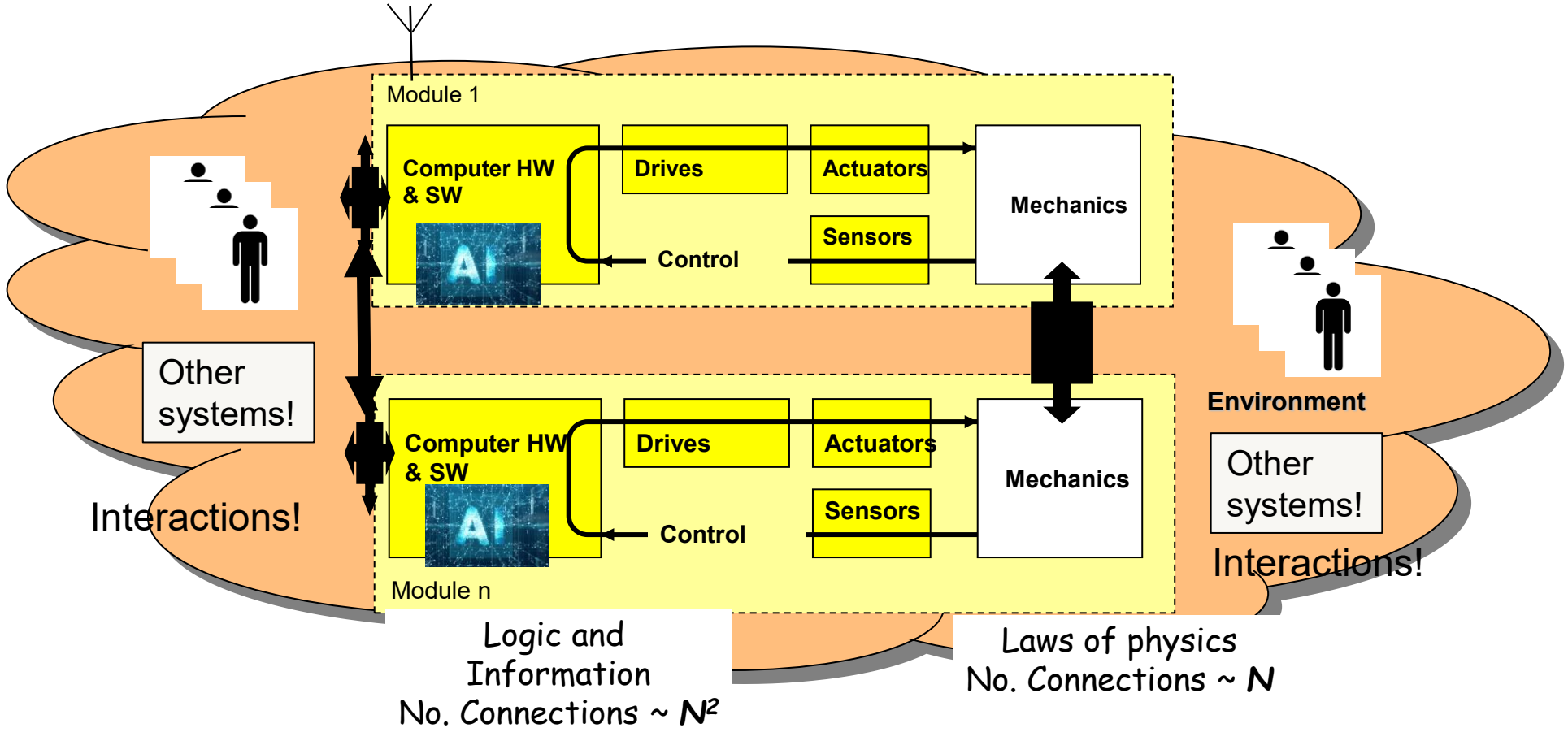
Energy storage

Industrial robot

Automated vehicle

From mechanics to CPS

- adding flexible information processing and flow

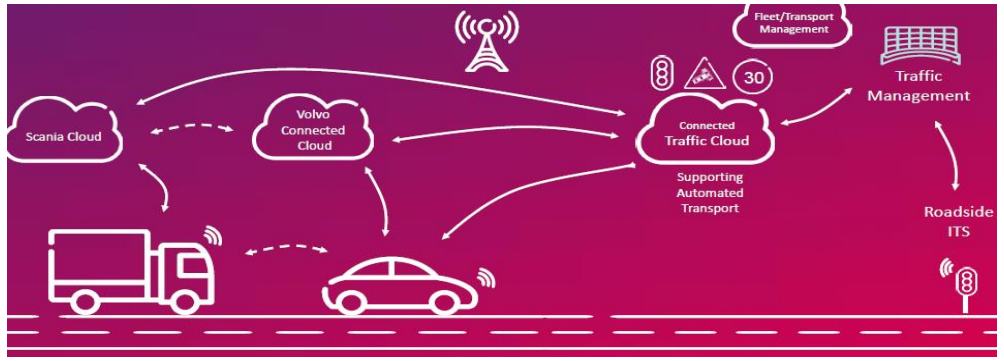


Digital infrastructure and connectivity

Telecommunication: …3G, 4G, 5G, … and edge computing!
Smart phones/pads
Wireless and wired communication
Internet and cloud
Satelite communication and navigation
Industrial computing
Smart devices and embedded systems

The world as a connected and SW defined distributed system

But really as a collaborative CPS

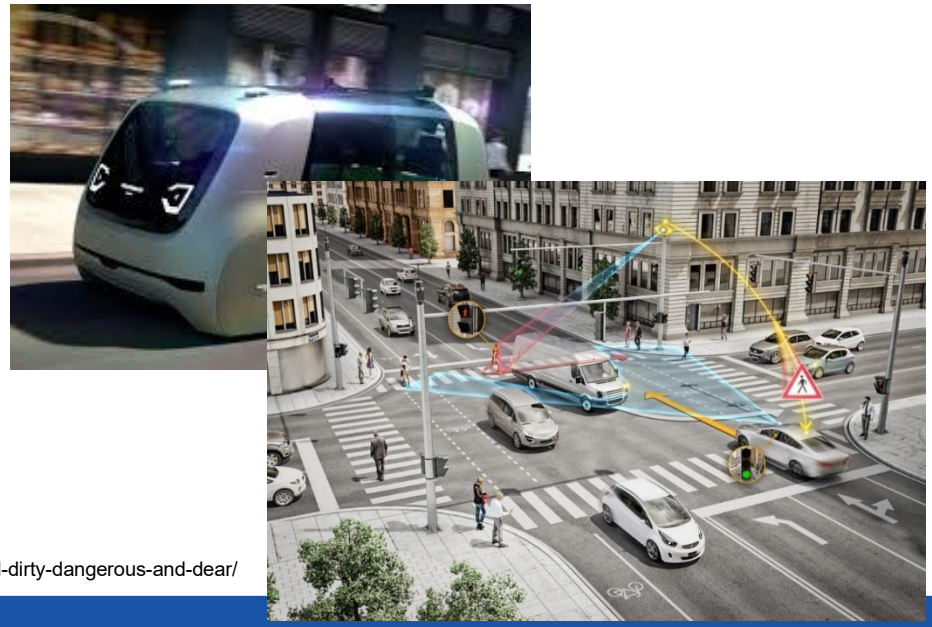


Courtesy of Ericsson

Free the robots!

Beyond ”dirty, dull and dangerous”: 4 D’s of robotization (*)

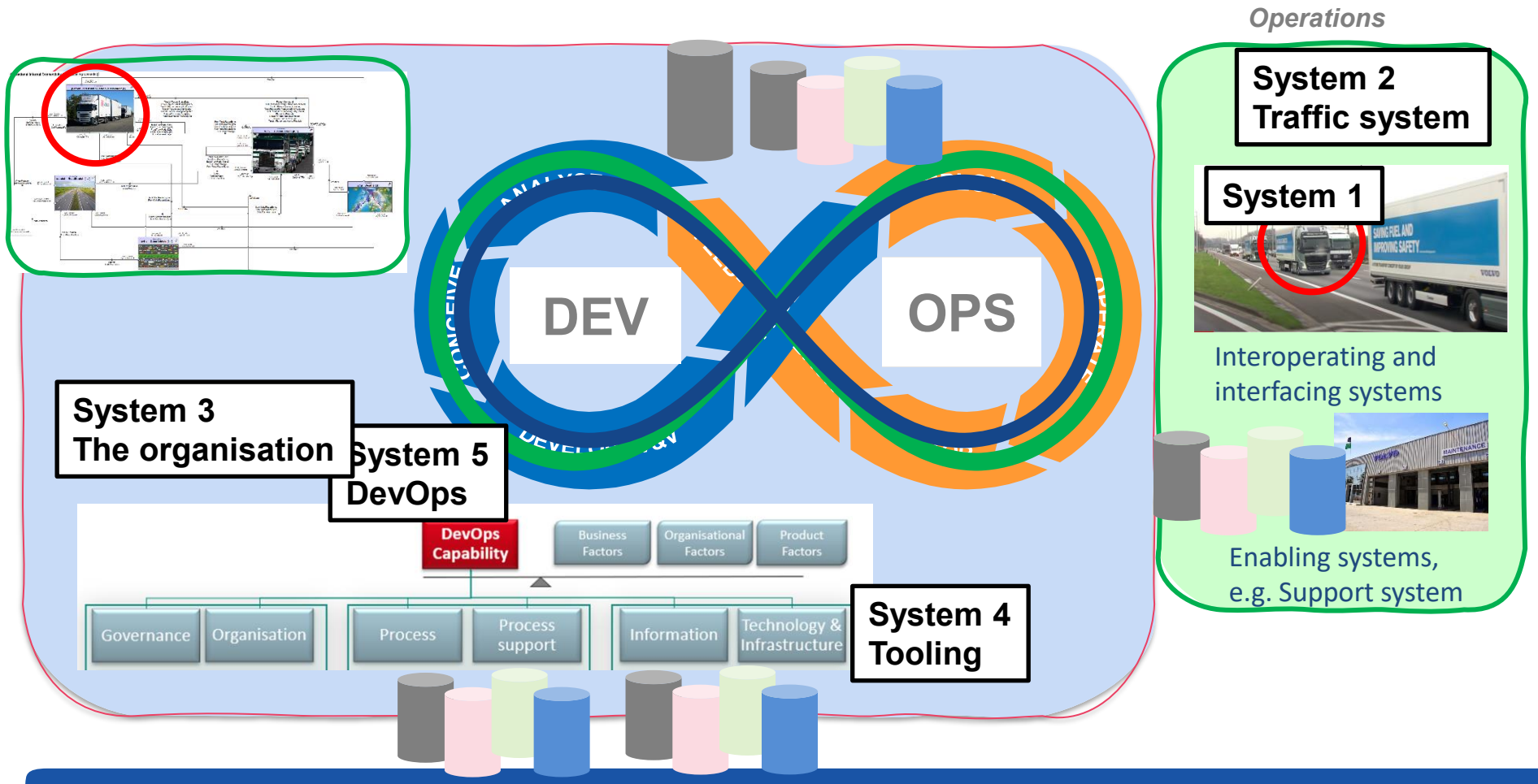
Higher levels of automation - CPS in open environments



(*) McAfee and Brynjolfsson, 2017
Machine, Platform, Crowd:
Harnessing Our Digital Future

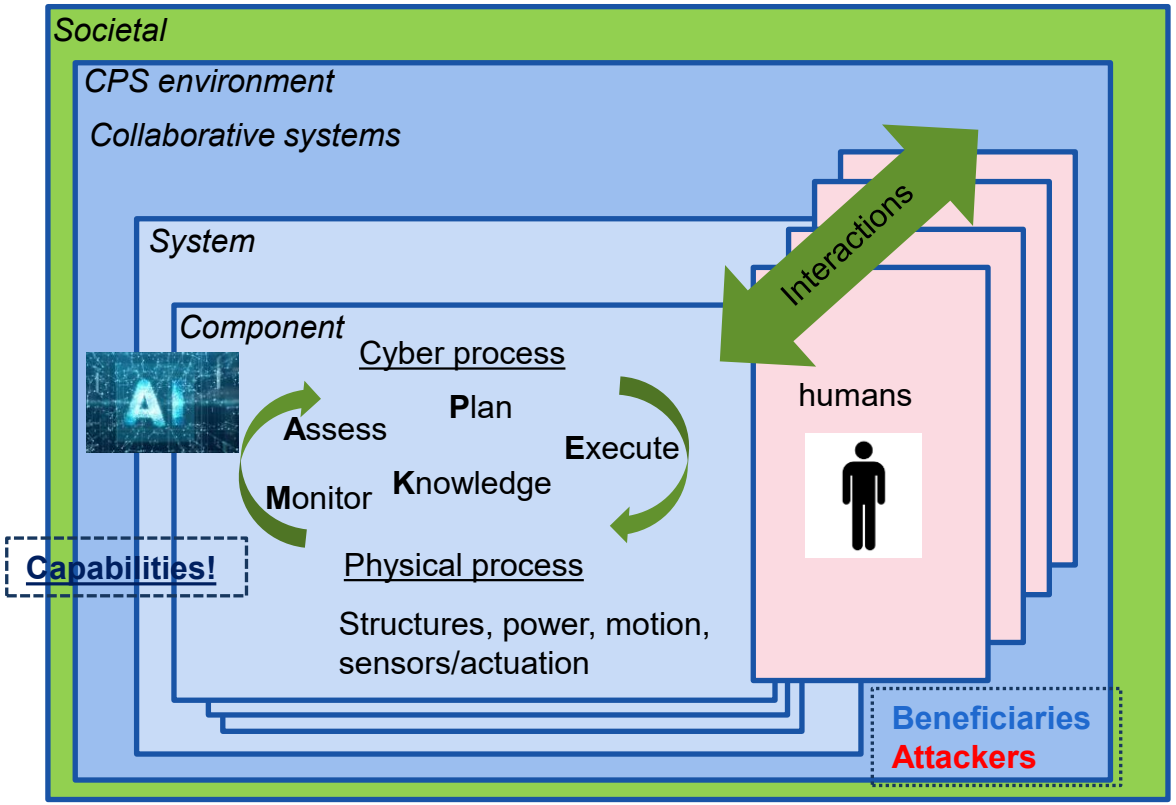
Beyond DDD => 4Ds: https://www.forbes.com/sites/bernardmarr/2017/10/16/the-4-ds-of-robotization-dull-dirty-dangerous-and-dear/

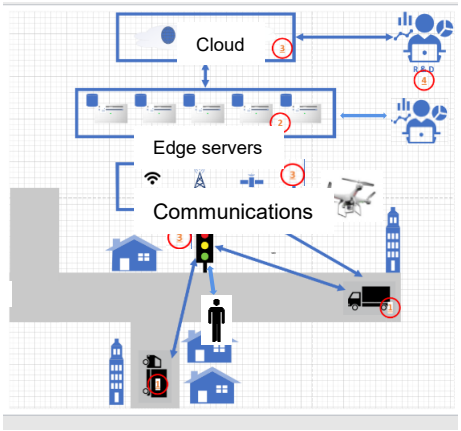
Towards software-defined systems and data spaces



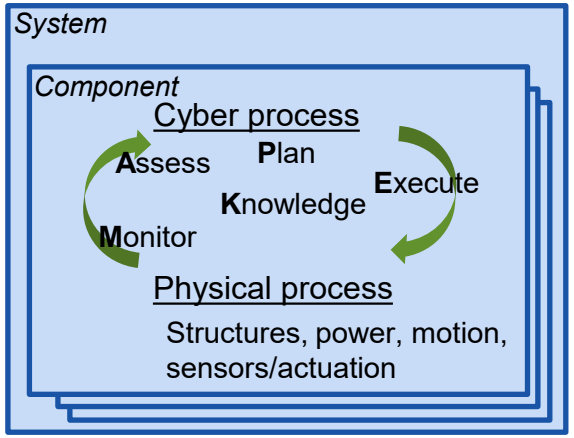
Cyber-physical systems: benefits, risks, and levels!

Regulations, culture, ”what is safe enough”





CPS capabilities



Gather, store and process data

Awareness and prediction

Plan and make decisions

Generate and control energy

Affect and create physical / software systems

Collaborate - exchange information, visualization, AR/VR

Capabilities with various time and system perspectives

➔ Reinforced by multiple progressing technological fronts

➔ Human capability augmentation – collaboration!

How can CPS support a circular economy?

Facilitating

- Identification, tracing, monitoring, prediction
- Reuse, recycling, upgrading, downgrading, maintenance
- Supporting a service based business model
- Individualized production of spare parts

A circular economy concept needs to address the CPS itself!

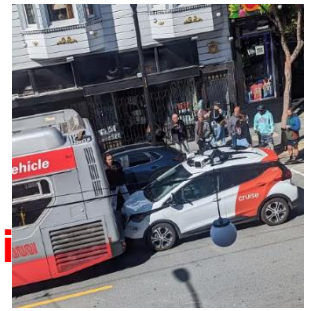
A CPS does not drive drunk, so what could ever go

Complexity

- Billions of transistors, LOC's and 100's of billions of (DL) parameters

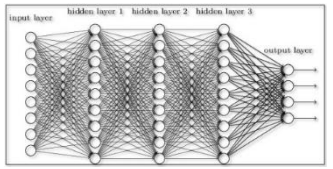
The world of software and bugs

- Industry average code ~ 15– 50 errors /KLOC
- Safety critical systems ~ 0.1 error/KLOC at very high cost
- Single event upsets (transient HW errors, bit-flips)



Deep learning: breakthroughs but brittleness & explainabili

- Limited contextualization beyond training data
- An emerging discipline (M. Jordan, UC Berkeley)



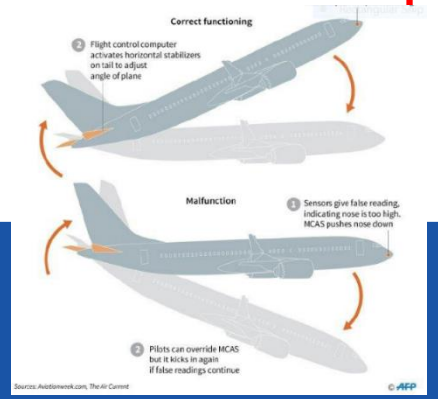
Cyber-security threats and attacks

- Dynamic threat landscape

Verification & val. challenges - environment & interaction complexity

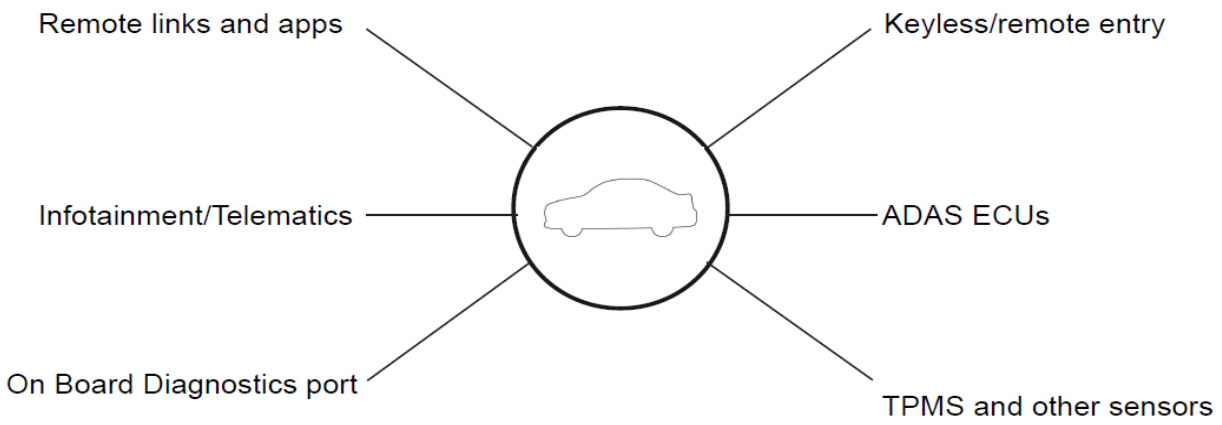
Automation surprises and pitfalls

- Humans in- and on- the loop



Lisanne Bainbridge, 1983: Ironies of automation

Cyber security – evolving attack surfaces



Exemples of attack surfaces in a modern car:

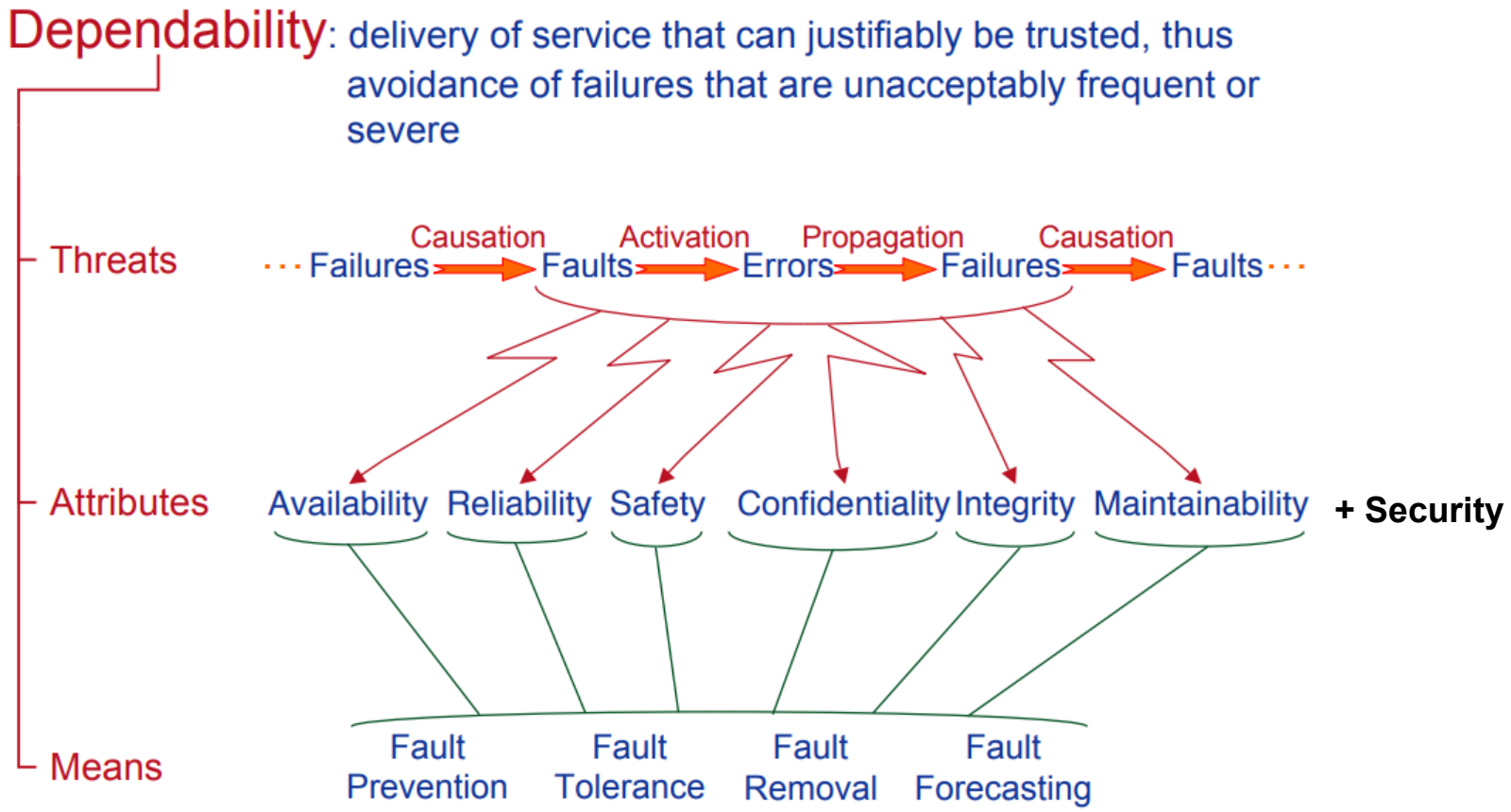
Examples:

- Malicious access to cyber- or physical services (autentification, authorization)
- Denial of service (availability)
- Theft of things (e.g. a car) or intellectual property (data)
- Corrupted/wrong service (e.g. commissioned braking)

Towards smart and sustainable cities

Trustworthiness and Dependability

Dependability



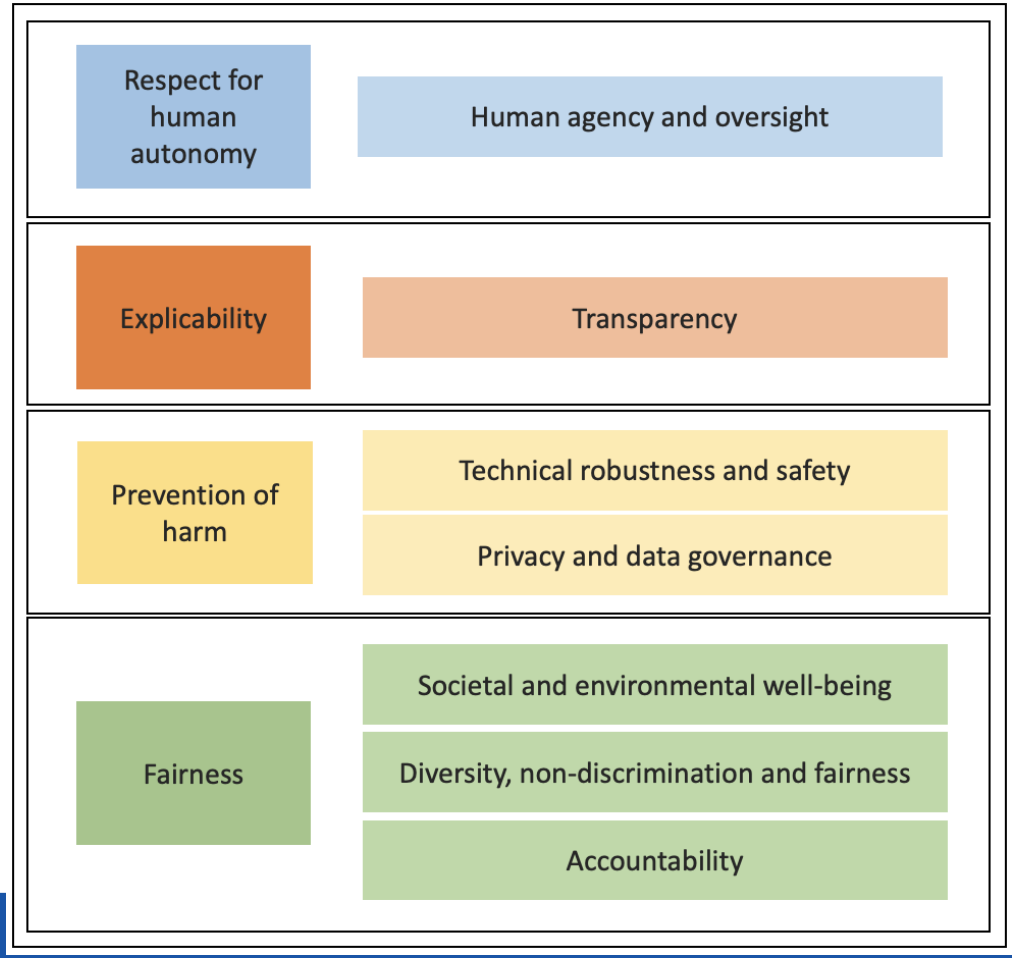
A. Avizienis, et al. Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Tr. Dependable and Secure Computing, 2004''

Trustworthy AI - as an umbrella concept

EU guidelines from 2021 – permeating the AI act

Key aspects of trustworthy AI:

- Ethical
- Lawful
- Robust



Resilience

- "The … ability of a system to adjust its functioning prior to, during, or following changes and disturbances, to sustain required operations" (in both expected & unexpected conditions)
  - 4th ed. Resilience Engineering in Practice, 2010"
- Origins in ecology
  - Resilience and Stability of Ecological systems (1973), C.S. Holling
  - "Principles for Building Resilience - Sustaining Ecosystem Services in Social-Ecological Systems" (2015)
- Increasingly adopted in many areas
  - "100 Resilient Cities" - (100RC) – non-profit organisation
  - CRO: Chief Resilience Officer – new role in cities

CPS Trustworthiness and Dependability

Multiattribute

Cross-cutting and **trade-offs**

Assurance cases

Socio-technical

Evolution and emergence

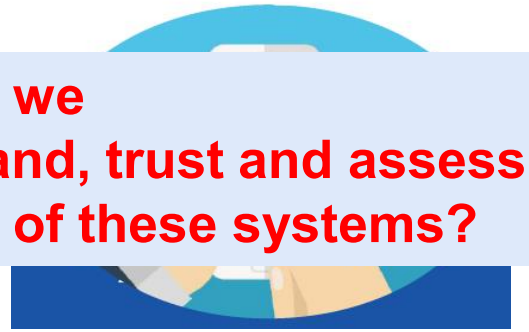
ATTRIBUTES

Fairness Ethics
Transparency
Auditability
Security
Safety
Availability
Reliability

Humans – Cyber – Physical – Infrastructure – Devices
Compute continuum – Connectivity - Automation/Smartness

Human-centered Cyber-physical systems?

Arthur C. Clarke:
Any sufficiently advanced technology is indistinguishable from magic



How can we
Understand, trust and assess
the risks of these systems?

Needs when going into the “complex domain”

Cynefin model (Snowden, 1999)

Learning and creating new foundations, methodologies and architectures

- Sharing of data, incidents, failures, …
- Research, testbeds and controlled experiments!

New sociotechnical frameworks

New knowledge and innovation eco-systems

Precautionary vs. innovation principle $$$

Cyber-security management – a NIST framework

RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security event.

IDENTIFY

Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.

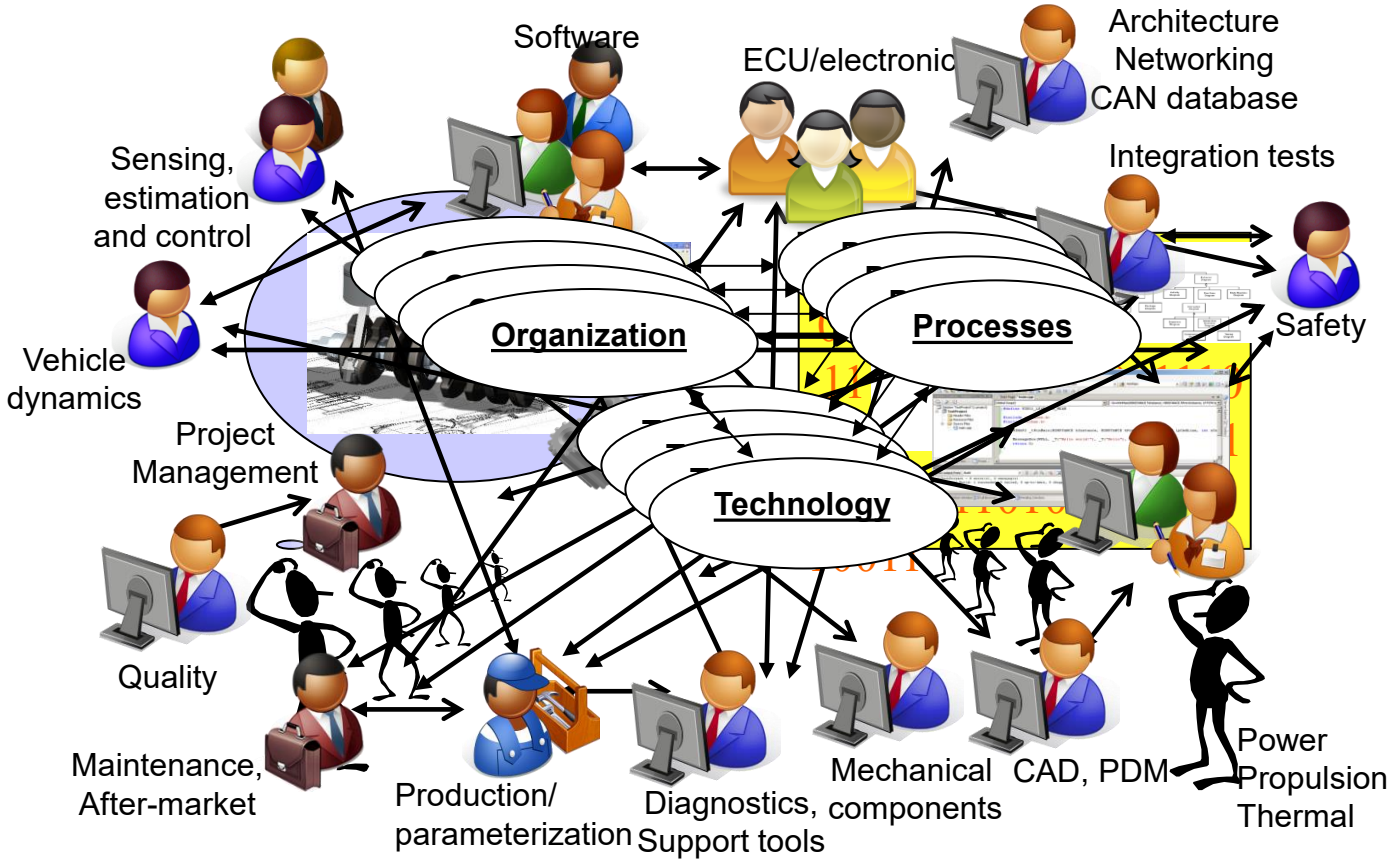
PROTECT

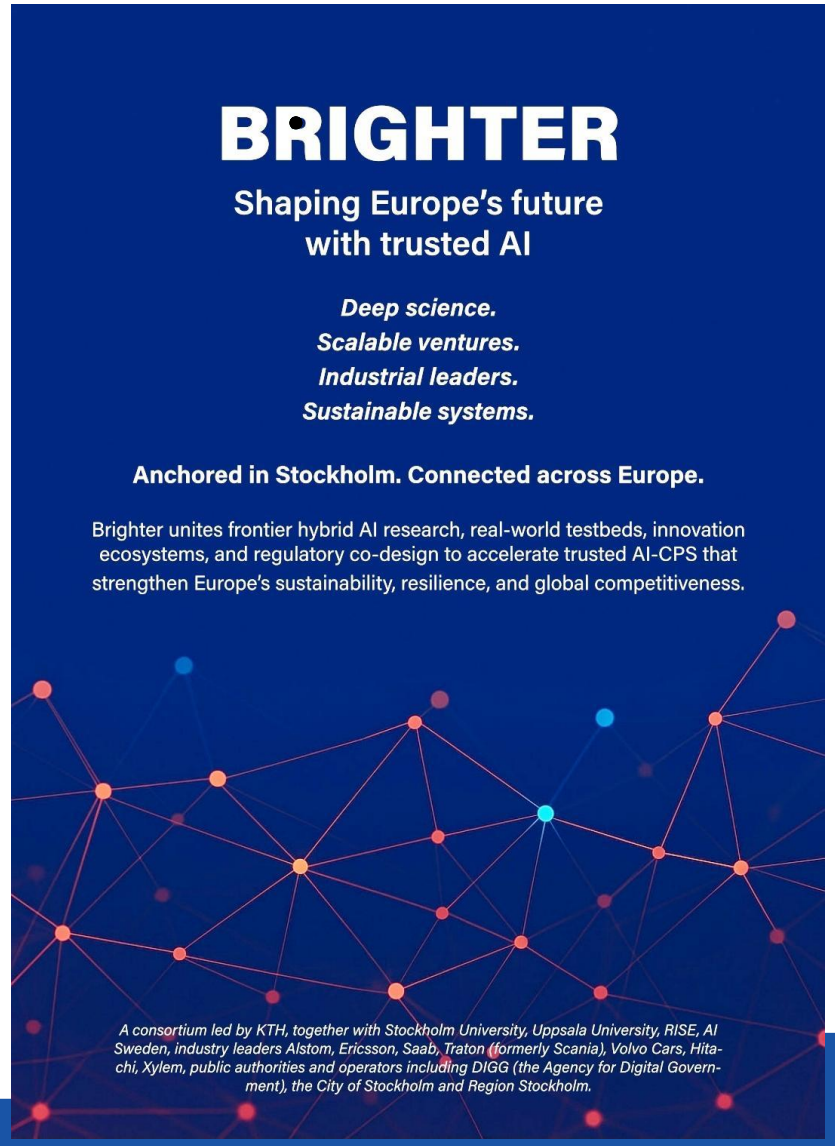
Develop and implement the appropriate safeguards to ensure delivery of services.

DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Complexity, viewpoints and integration pasta





Vinnova Excellence cluster - AI and automation:

- Principles and focus/balancing – towards a Research&Innovation cluster
- Connecting/relation to other initiatives including benchmarking
- In-depth investigations/assessments of
  - AI-CPS Research
  - R&I Infrastructure
  - Regulatory Frameworks
  - Innovation Ecosystem

Way forward towards trustworthy transportation – CPS and hyperspace

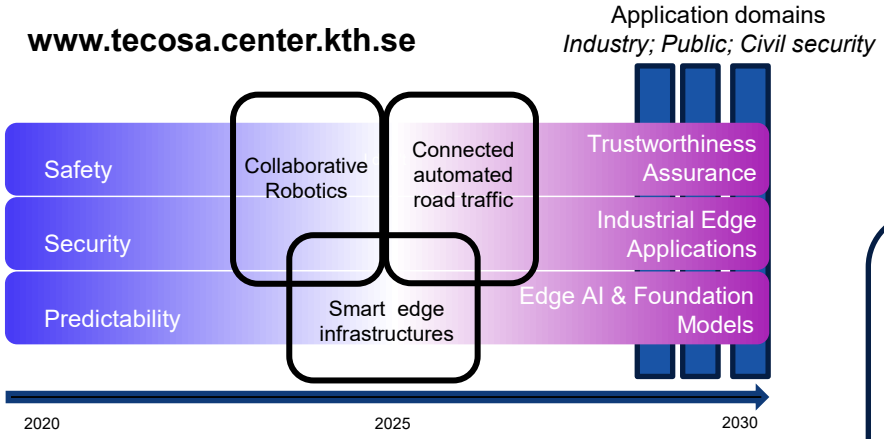
- The multiple facets of trustworthiness
- Competence and awareness in risks
- Roles in industry and society (CDO, CRO, CISO, …)
- New research and innovation arenas
- Trustworthiness
  - From design for trustworthiness to Trustworthy DevOps
- Trustworthiness management systems
  - Monitoring, leading indicators
  - Anomaly detection, OoD

Spares on research and testbeds

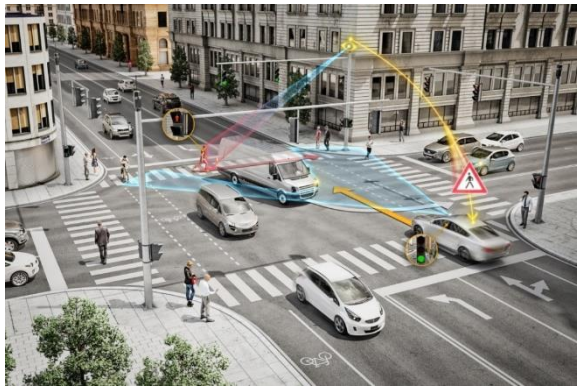
Related research

TECoSA research center on digital infrastructure supported CPS; trustworthiness assurance and edge AI as two main directions.
18 industrial partners, 9 KTH research groups, 5 + 5 year funding

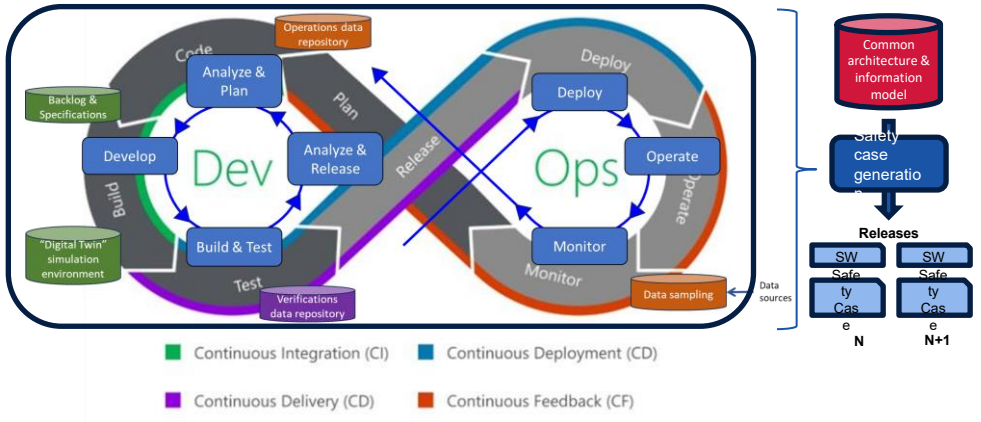
www.tecosa.center.kth.se



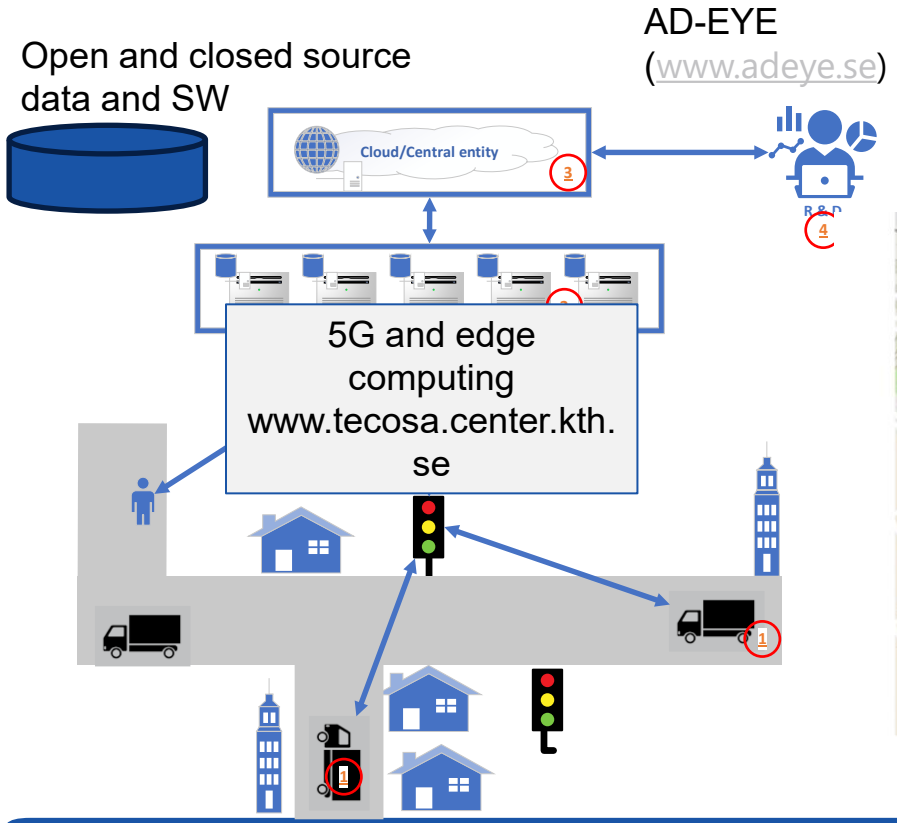
Connected traffic – e.g. Entice project

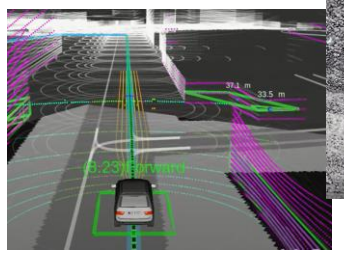


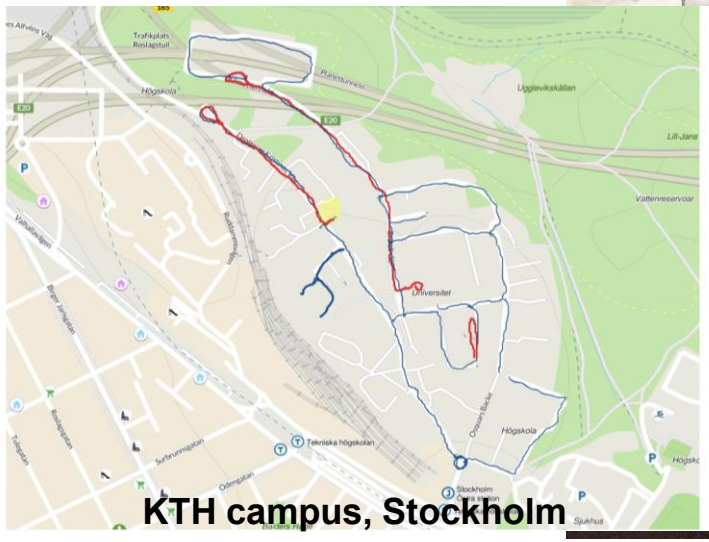
DevOps adapted to safety – TADDO2 project

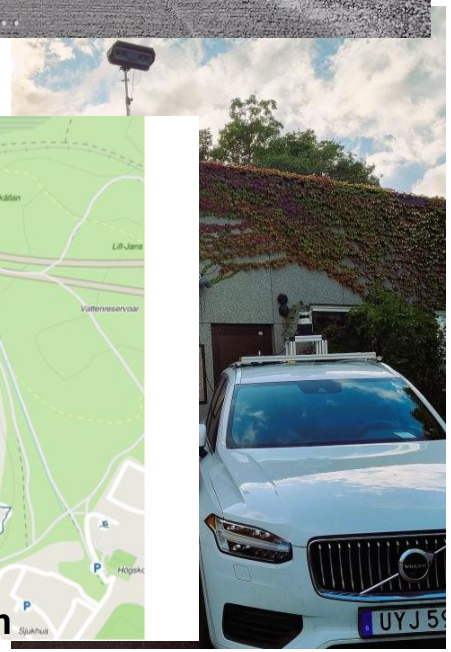


AD-EYE/TECoSA open research testbeds

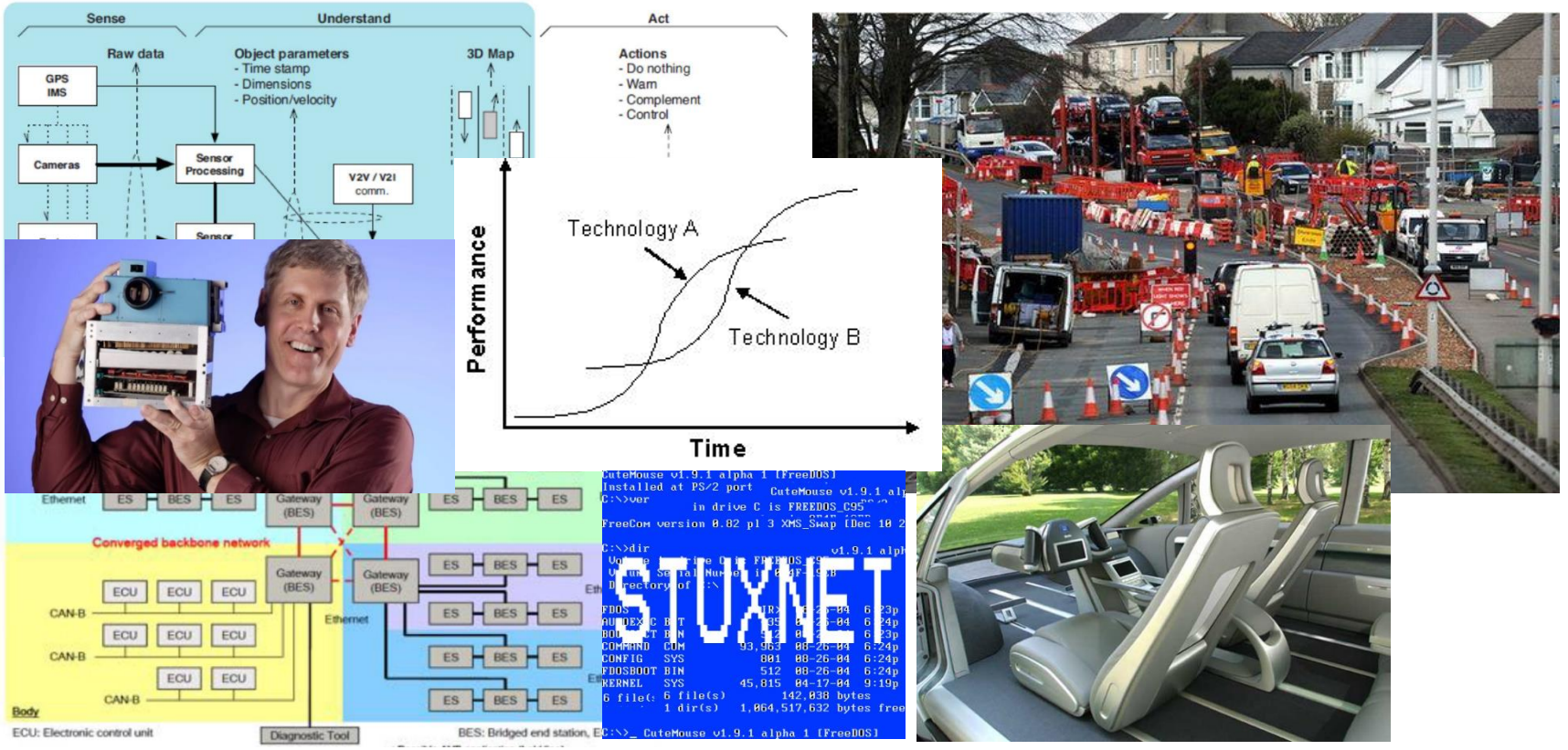




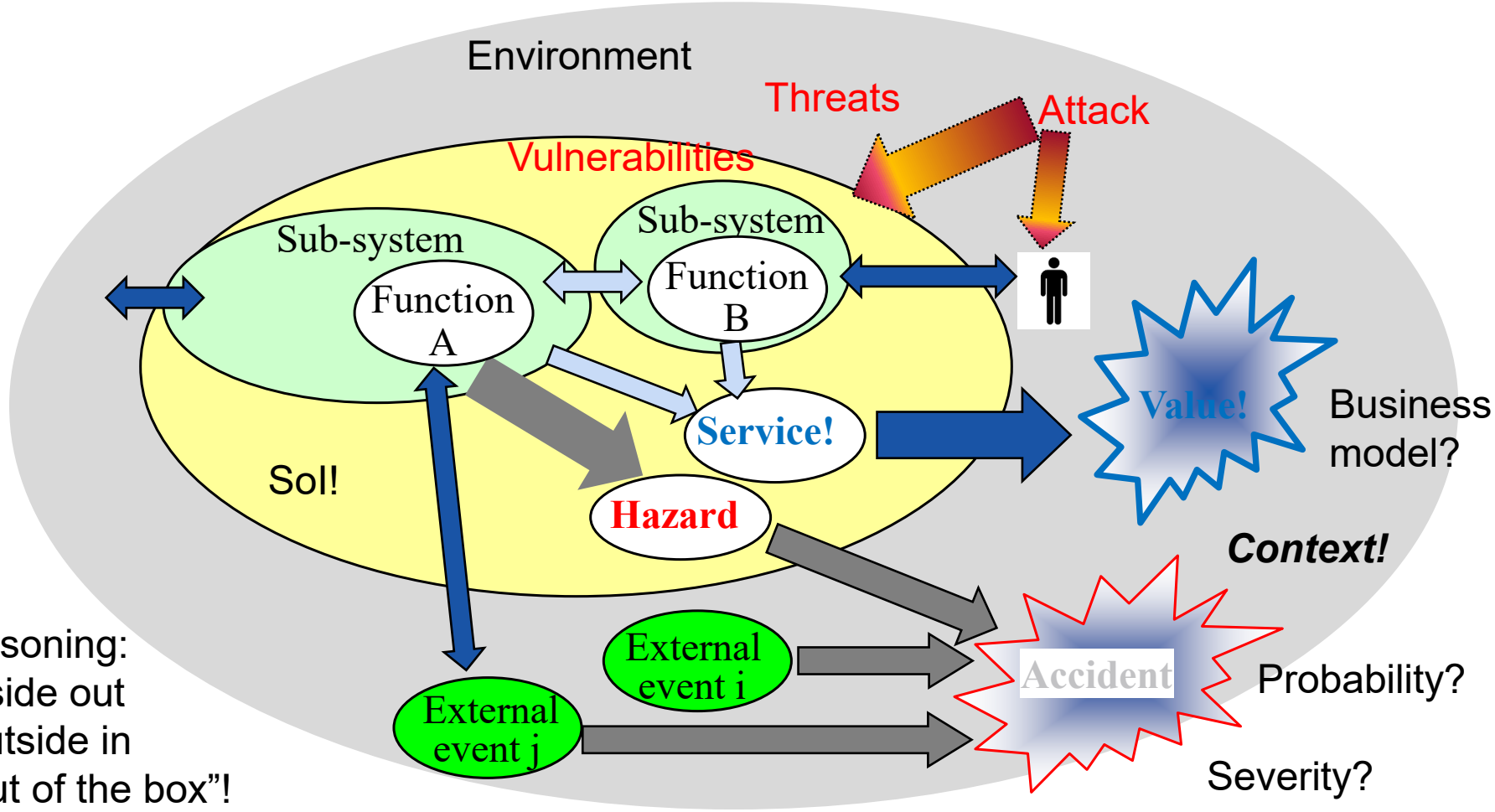




Indications on a technical paradigm shift



CPS views, effects and analysis



Reasoning:
- Inside out
- Outside in
- ”out of the box”!

Resilience principles from social-ecological systems

Maintain diversity and redundancy

Manage connectivity

Manage slow variables and feedbacks

Foster complex adaptive systems thinking

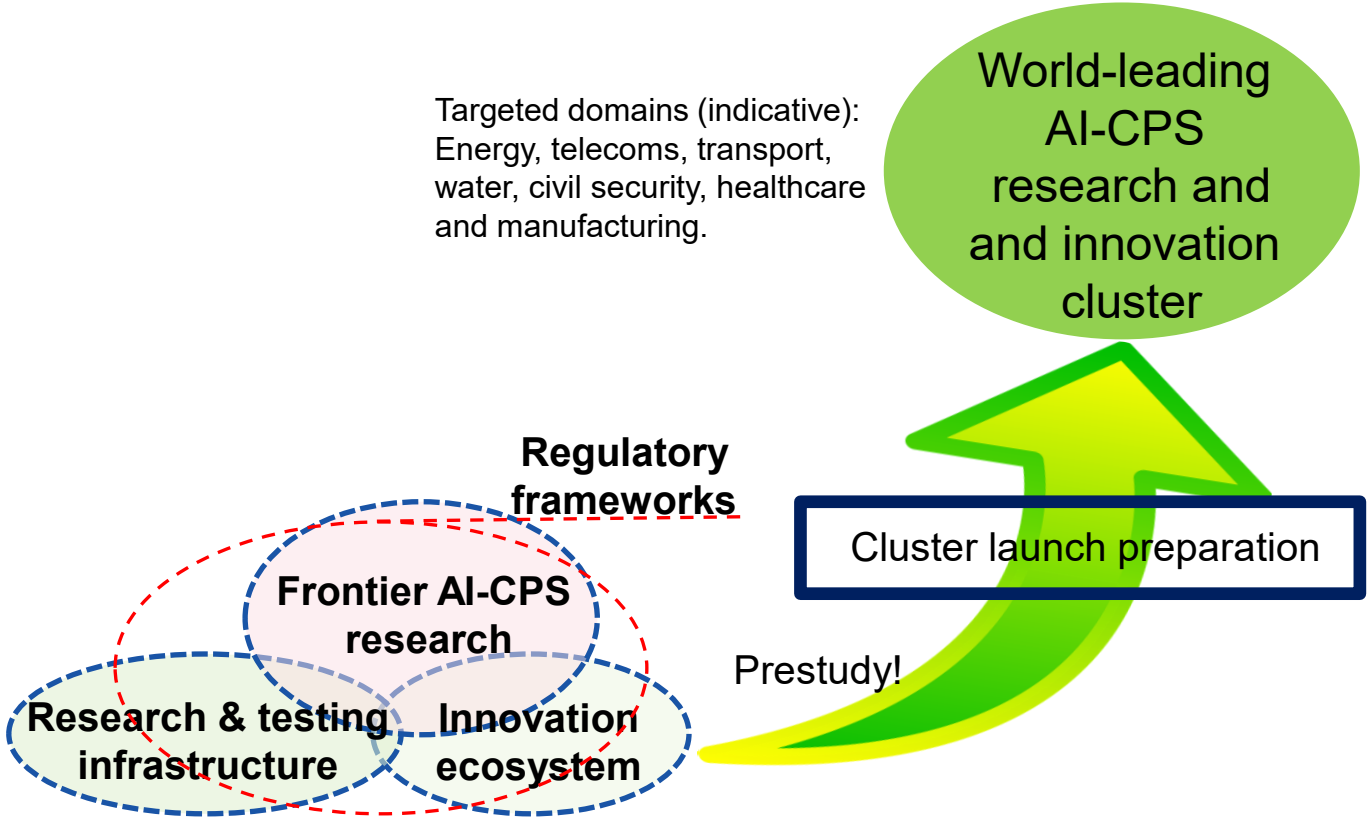
Encourage learning

Broaden participation

Promote polycentric governance systems

Book: Principles for Building Resilience - Sustaining Ecosystem Services in Social-Ecological Systems, 2015 (Stockholm Resilience Center, SU)

BRIGHTER - We lead the way with trusted AI for a sustainable society



CYBERCAMPUS SVERIGE

Preventing Crime in Hyperspaces
With focus on transportation systems
digital futures

Together, towards a robust and cybersecure digitalized Sweden

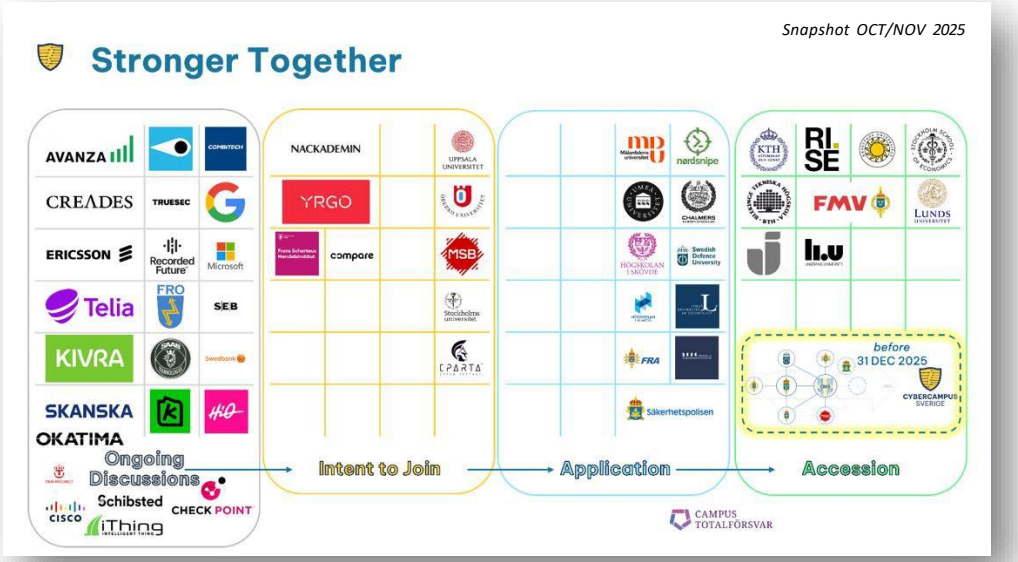
David Olgart
Director

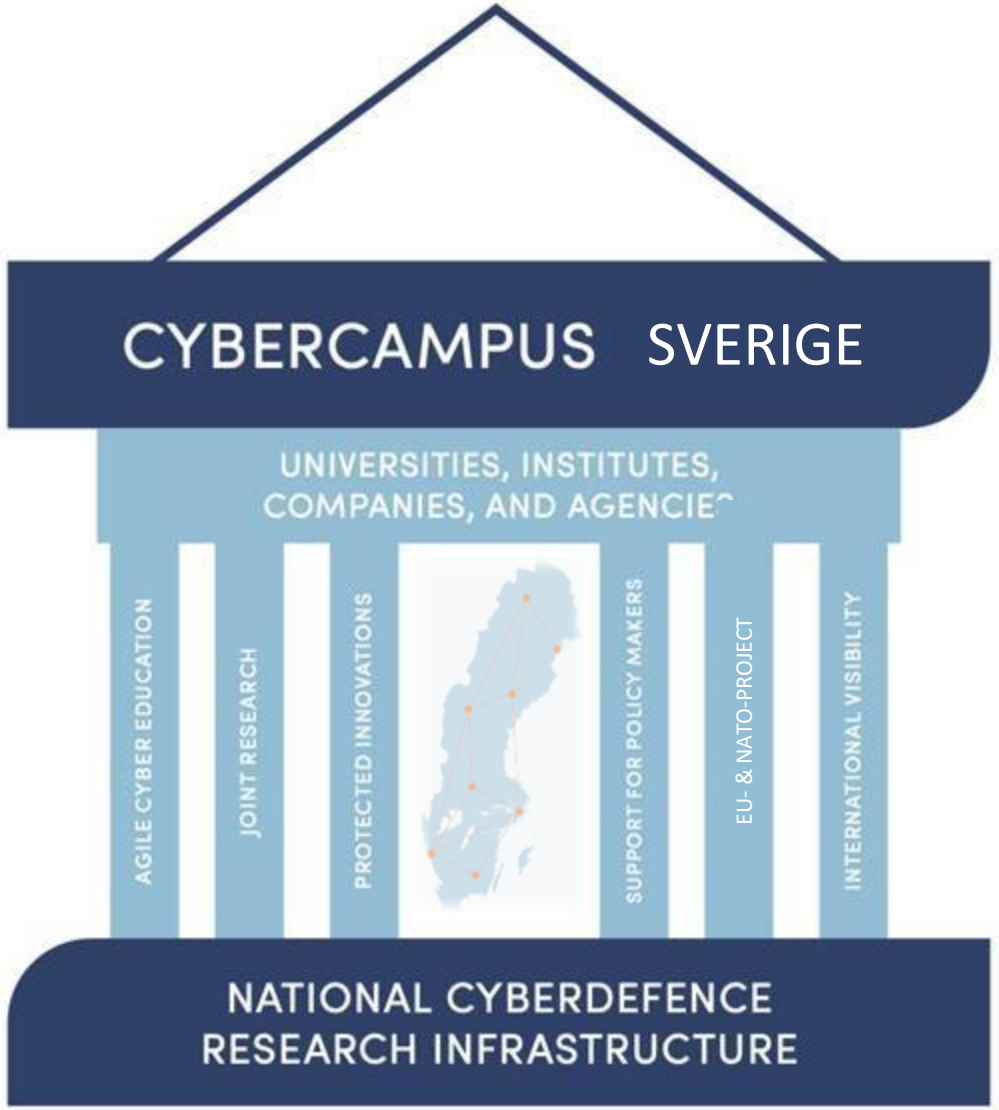
20 NOV 2025

Mission – National Collaboration

Agile and cutting-edge research, innovation, and **education** for cybersecurity and cyberdefense **beyond what is possible for a single** university, institute, company, or agency

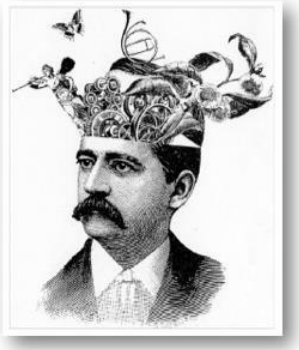
A Physical, Neutral & Inclusive Space



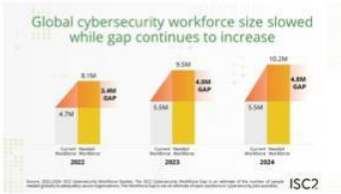


The Cybersecurity Challenge is Closely Linked to the ongoing Digitalization of our Interconnected World

The Never Ending Flow of Vulnerabilities

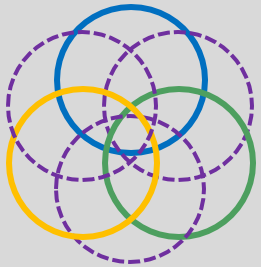


It's too Complex
(not complicated)



Lack of Competences
The Workforce Gap

Background | Outlook

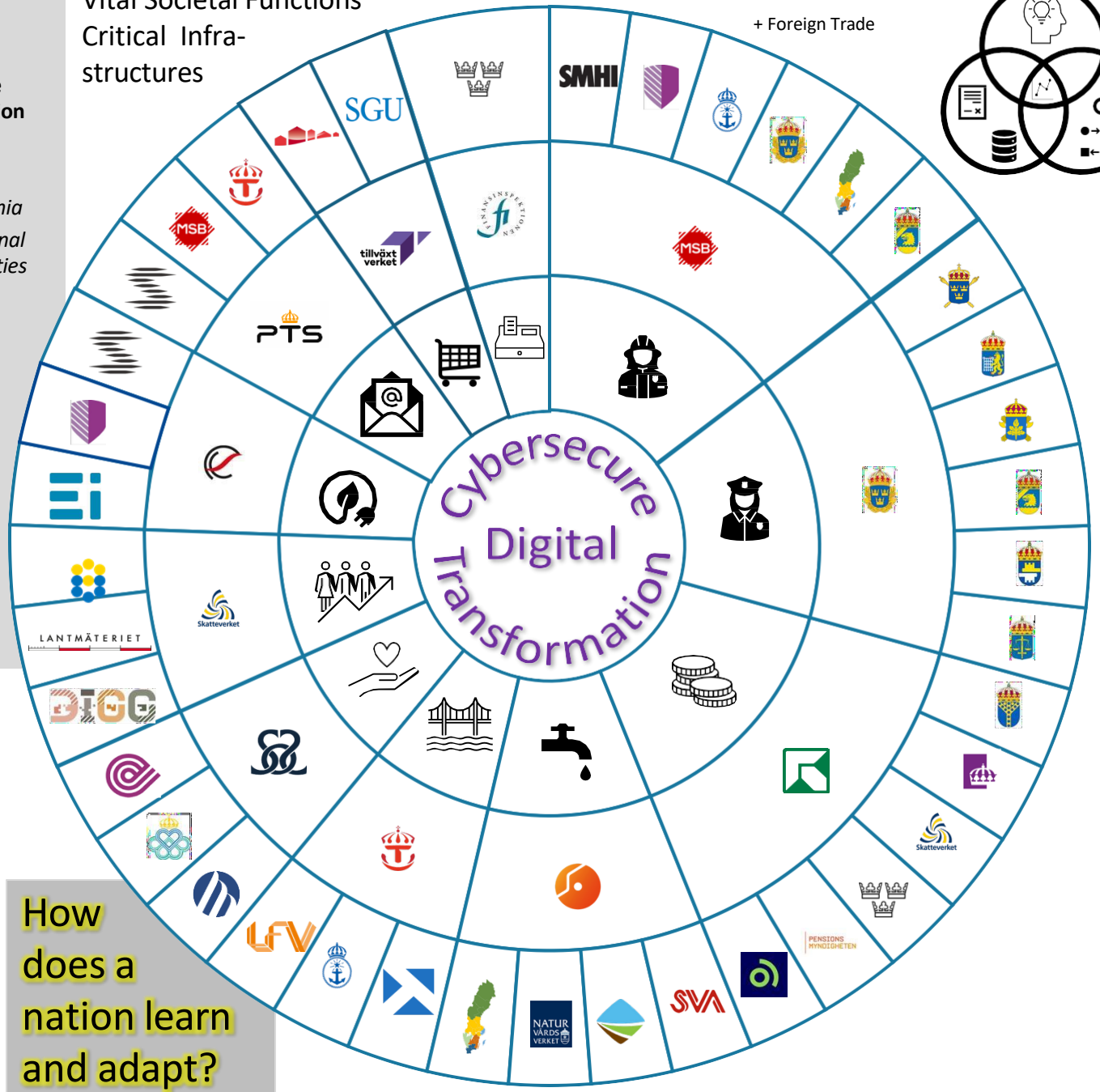


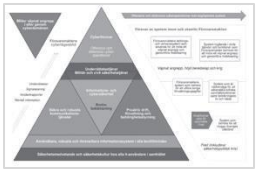
”Deliver on needs that are not addressed by any other stakeholder in the cybersecurity ecosystem.”

Research
Innovation
Education

Vital Societal Functions
Critical Infra-structures

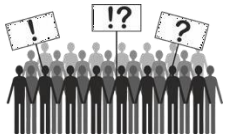
+ Foreign Trade





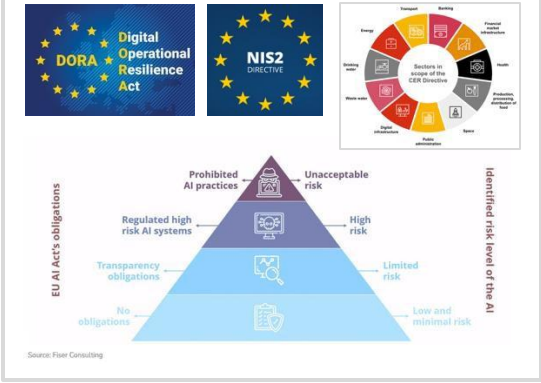
Cyber Threats & Incidents

Develop and strengthen the capability to prevent, identify, and handle cyber threats and large-scale incidents.



III & V

How does a nation learn and adapt?

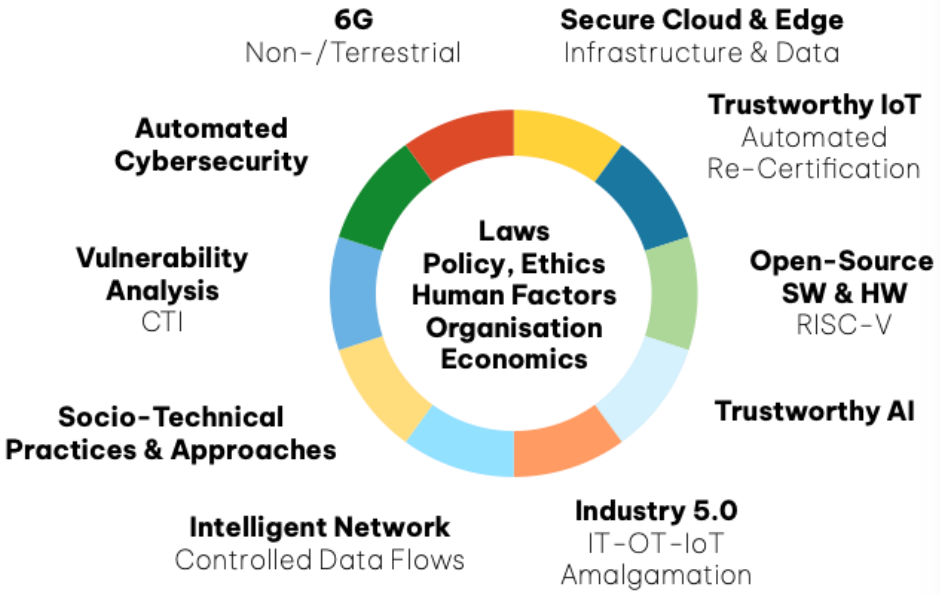


National Collaboration and Mobilisation

Joint Research

Mission-Oriented - **Interdisciplinary**
Research Pairs – **Graduate School**

The sum of all conditions for actual cybersecurity, including the ability to withstand and manage incidents and cyberattacks.



Continuous Education

Introductory – Intermediate – Experts
Professionals – Specialists – **Decision-makers**

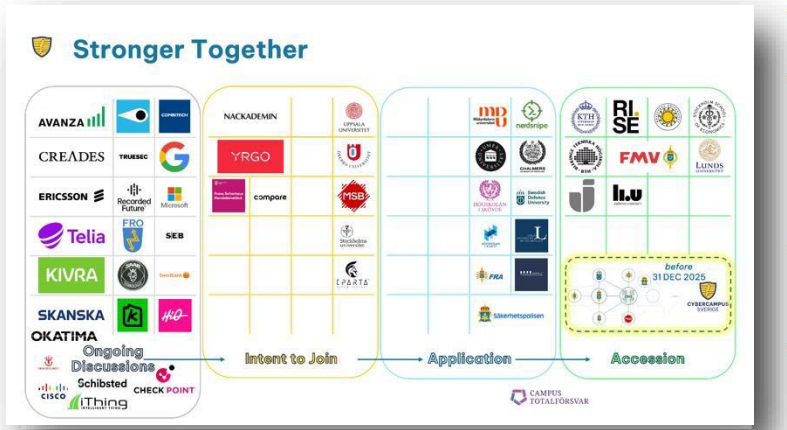
Innovation

Research- / Theme- / Partnership-Based
Challenge-Driven / **National Arena**

Cybercampus Sverige

The road ahead

Planning & Execution



Interdisciplinary Activities

- Joint & Cutting-Edge Research
  - Ethical Hacking Lab; Bug Bounty
- Agile Education – Continuous / Lifelong
  - Cybersecurity for ...
    - All ↔ Specialists / Experts ↔ Decision Makers
  - Graduate School – Co-Supervised PhD Projects
  - Ethical Hacking
  - Certificates – Validation
  - Training – Exercises
- Defence Innovation
  - Ethical Hacking; Bug Bounty; Hackathons
  - Co-creation Events
- Collaboration
  - National Entities – NCC-SE
  - Co-Organizer of Activities
  - Co-Sponsor of the SE National Hacking Team
  - International, Similar Entities

CYCERONE

Co-funded by the European Union

I'M CYBER VACCINATED CYVAC

Cyber Sweden Conference 2025

CYBERCAMPUS SVERIGE

David Olgart

Director

olgart @ kth.se

https://www.cybercampus.se/

KTH VETENSKAP OCH KONST

sPnetwork Safe Places

digital futures

Discussion

pixabay