Sensors
Converge

IoT and IoB in Safety, Security, and Risk Assessment of Critical Infrastructures

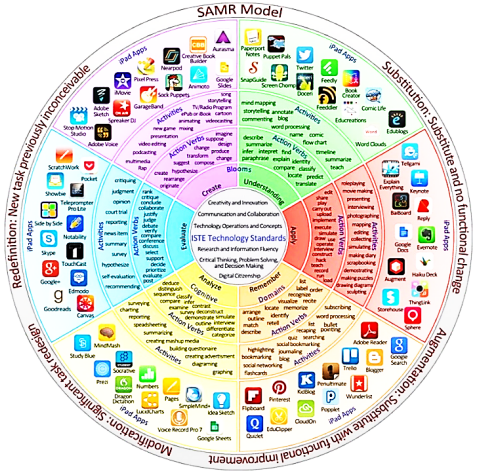
June 20–22, 2023 | Santa Clara, CA

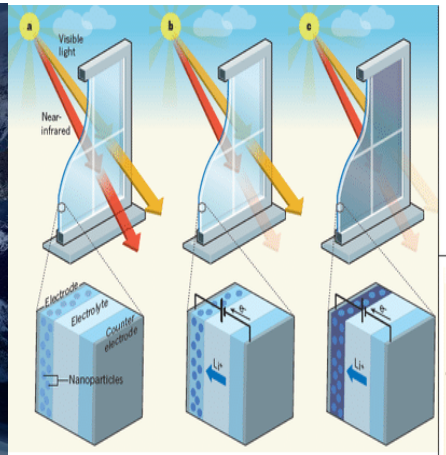
#SensorsConverge

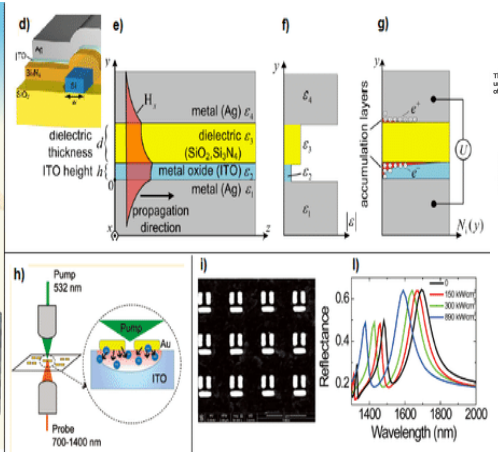
Presentation Outline

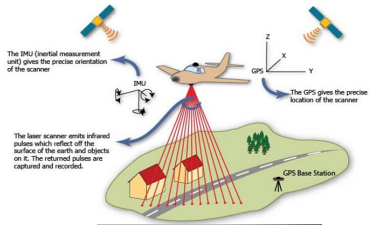
- Connected World
- Exponential Technologies and the Internet of Things (IoTs)
- Cyber Physical Systems
- Small and Connected World and Critical Infrastructure (CIS)
- Internet of Behaviors (IoBs)
- Existing Applications of IoBs
- IoTs and IoBs
- Dual Use Technologies
- Opportunities and Challenges
- Recommendations

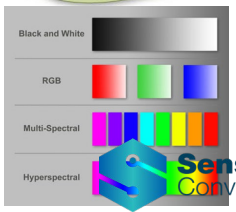
Connected World





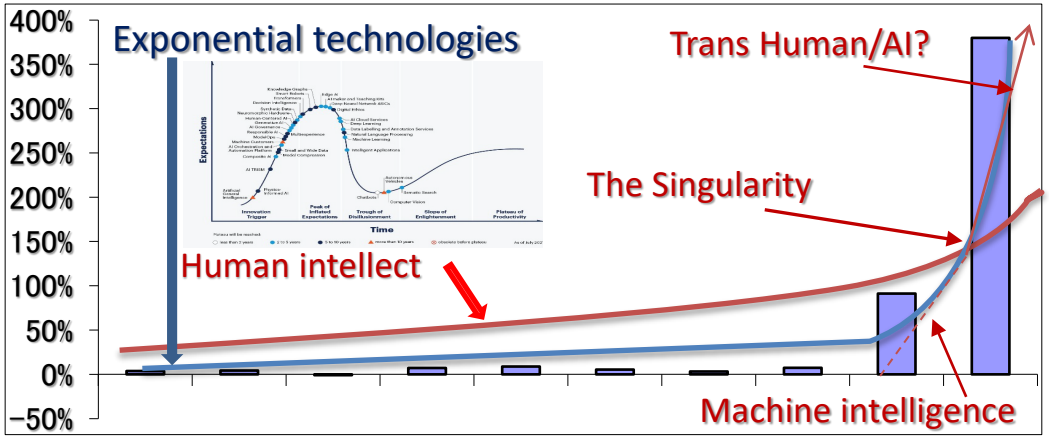


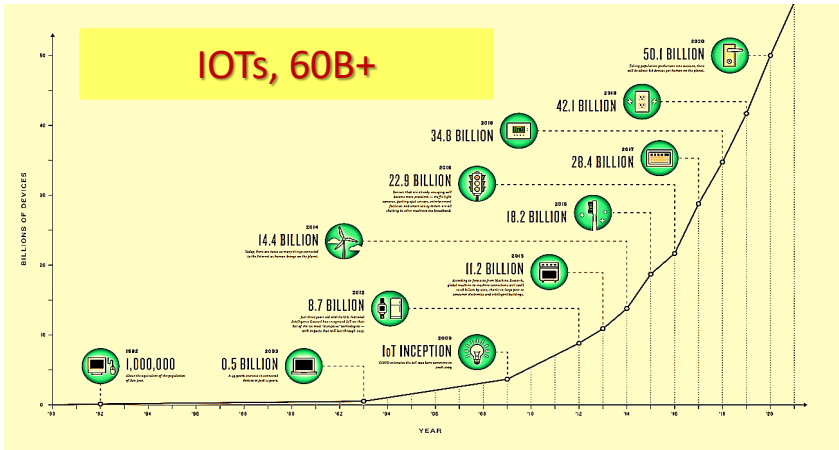




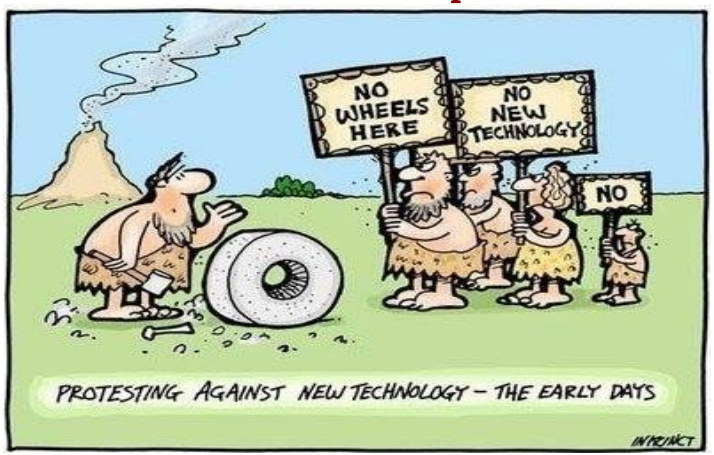
Sensors Converge

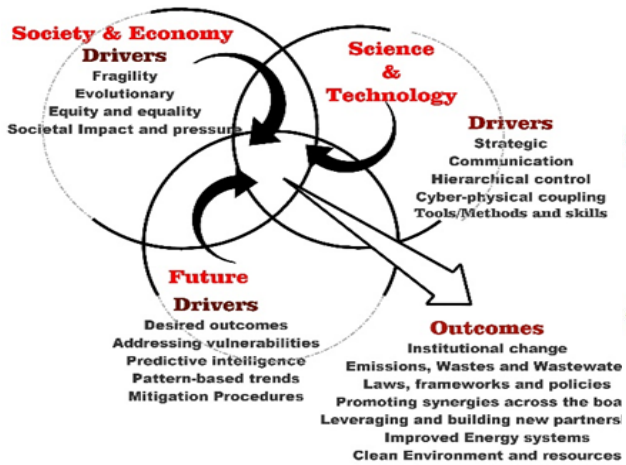
Technology Convergence, Mapping, and Accelerators

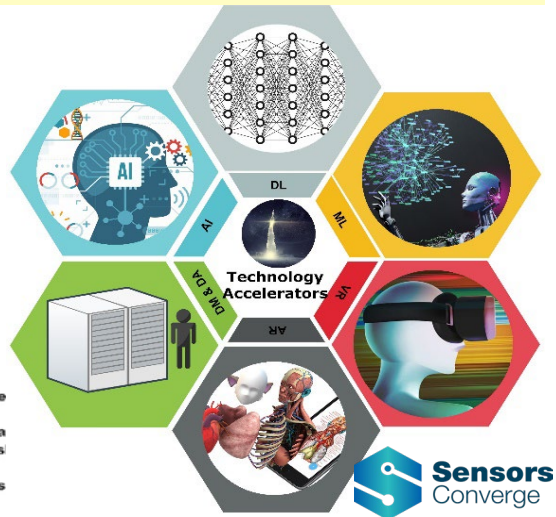




The Maltushian Trap ?



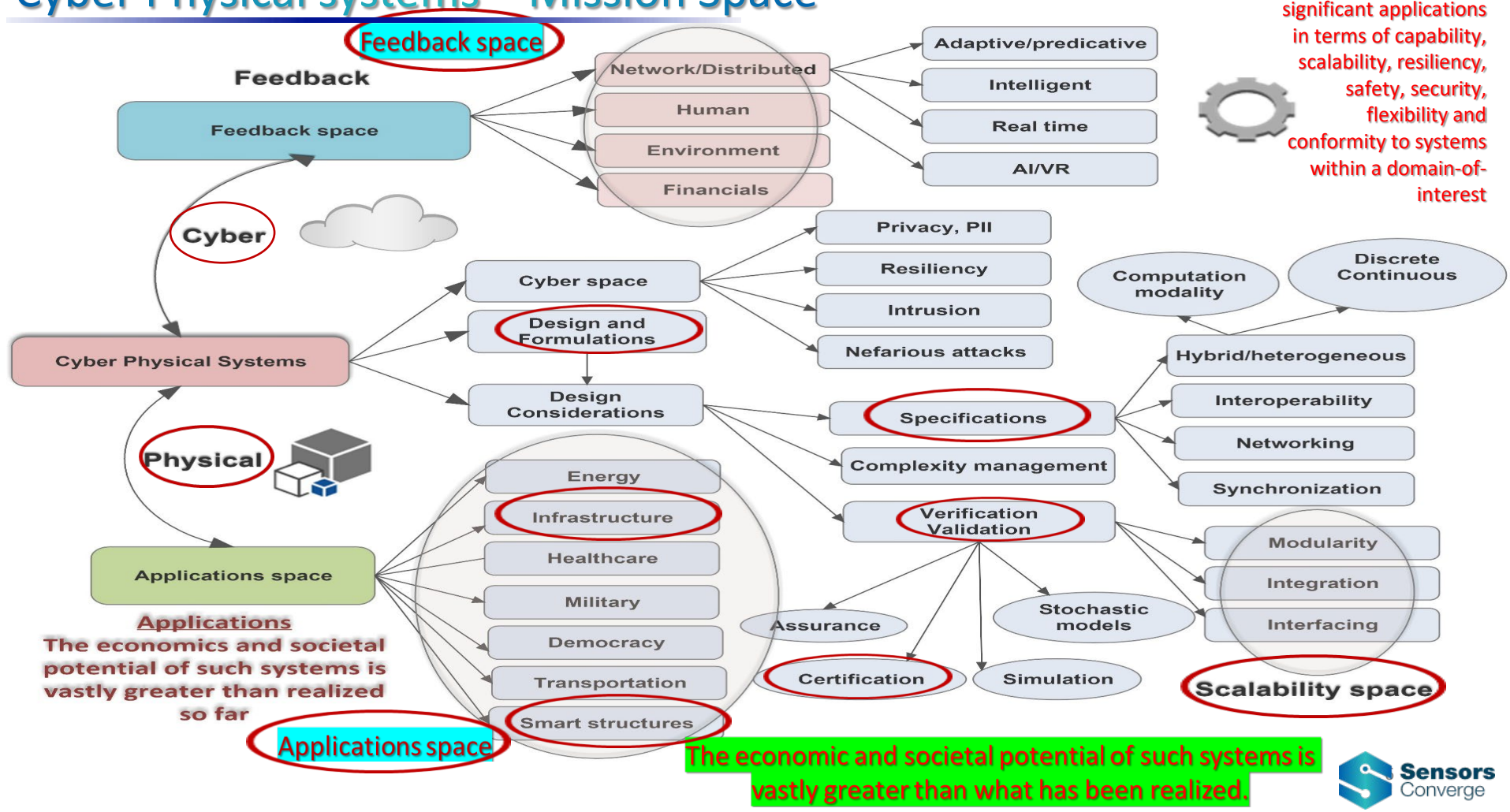




Cyber-physical systems – Concept

- Cyber-Physical systems (CPS) is a multidisciplinary engineering discipline that is focused on technology with a strong foundation in mathematical abstractions.
- CPS integrates the dynamics of the physical processes with the software and networking, providing abstractions and modeling, design, and analysis techniques.
- Cyber-Physical domain consists of integrated and networked system-of-systems where physical processes are controlled or monitored by computer-based algorithms.
- The physical and software components are operating on different spatial and temporal scales, exhibiting multiple, yet distinct behavioral modalities, and interacting with each other in ways that change with context, within a domain of interest (DOI).
- Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa.
- Challenge: is to conjoin abstractions that have evolved over centuries for modeling physical processes (differential equations, stochastic processes, etc.) with abstractions that have evolved over decades in computer science (algorithms and programs, which provide a "procedural epistemology".
- In the Security Arena – in addition to monitoring and surveillance – the use of CPS is to map human behavior by algorithmic estimation of various parameters.

Cyber Physical systems – Mission Space



Advances in CPS have significant applications in terms of capability, scalability, resiliency, safety, security, flexibility and conformity to systems within a domain-of-interest

The economic and societal potential of such systems is vastly greater than what has been realized.

Sensors Converge

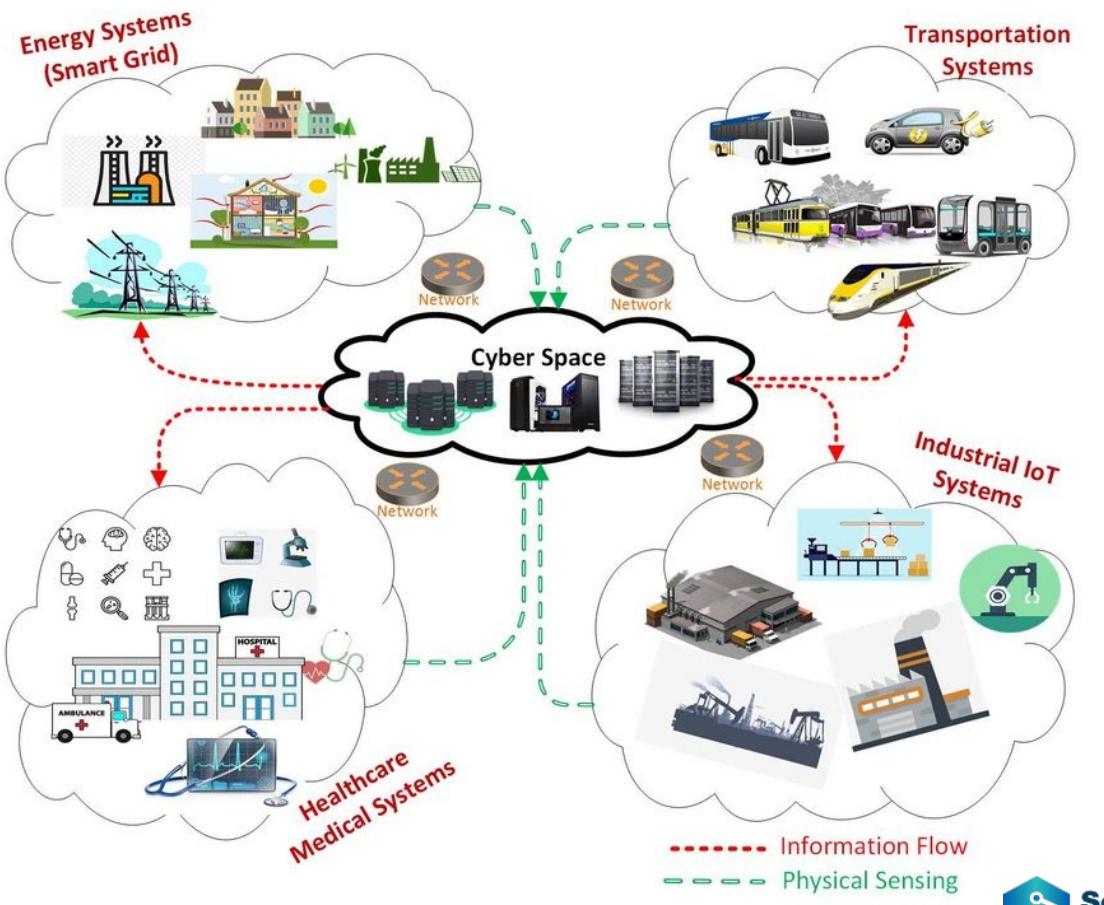
Cyber-Physical Systems – Components and Architectures

Information and Management flows

- SCADA
- Building Control Systems
- Process Control Systems
- Industrial Automation Networks

Physical sensing and control

- PLC
- Smart Controllers
- Industrial IoT
- Remote Terminal Units



Sensors Converge

Cyber-Physical Systems – Vulnerabilities and Mitigation Controls

- Designed around the availability and safety
- Cybersecurity features were not part of the original design
- **"Security by obscurity"**

Top 10 attack vectors

- Zero-Day
- Brute Force
- DDoS
- Compromised Credentials
- Malicious Insiders
- Missing or Poor Encryption
- Misconfiguration
- Ransomware
- Phishing
- Trust Relationships

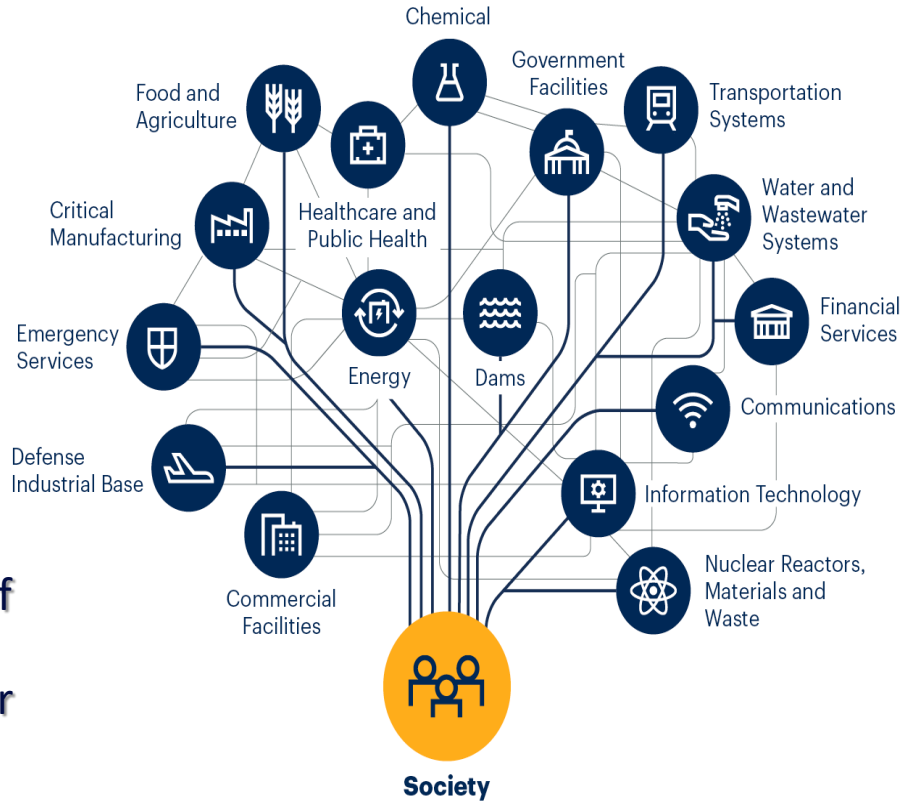
Top 10 Mitigation Controls

Sensors Converge

Critical Infrastructure (CIS)

Critical Infrastructure is the body of systems and networks – physical or virtual assets - that are essential such that their continued operation is required to ensure the security of the state, nation, its economy, and the public's health and/or safety.

Any physical or virtual information system that controls, processes, transmits, receives, or stores electronic information in any form that is vital to the functioning of a society's economy, public health, and safety, security, or any combination of the above, including the food and agriculture sectors, transportation systems, energy and water supply, financial services, telecommunications & broadband internet, defense, and more.



Sensors Converge

CIS Assets, Vulnerabilities, and Resilience

The CIS Assets encompass industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, which are used to automate industrial processes.

The threat of crippling cyberattacks against industrial control systems has severe security, financial, and supply-chain implications as the attackers are increasingly going after CIS and operational technology (OT) while improving their penetration capabilities – as vulnerabilities.

Infrastructure resilience is the ability to withstand, adapt to changing conditions, and recover positively from shocks and stresses. This applies to physical infrastructure assets and the wider system of which these assets are part, including the natural environment, the organizations that own and operate these systems, and the humans who make decisions across the value chains.

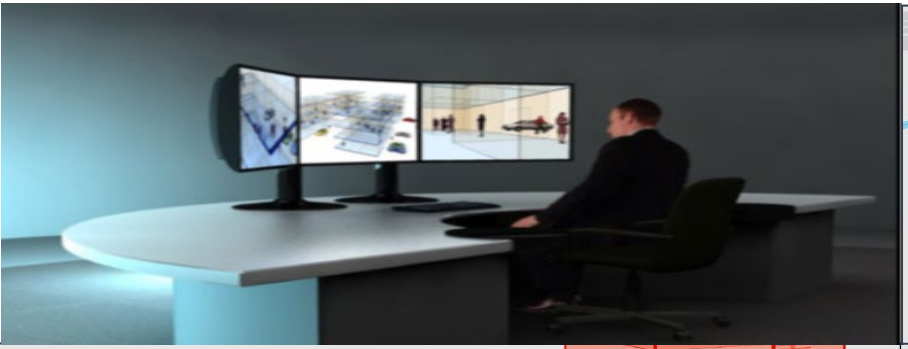
Smart and Connected Communities - Vision

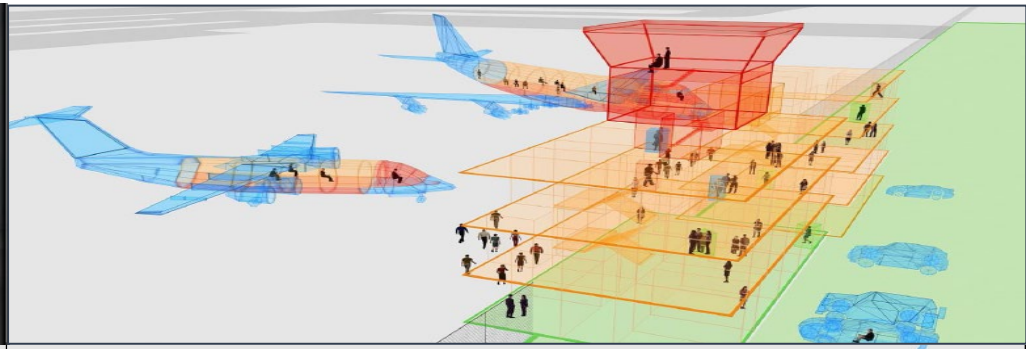
- Communities around the world are entering a new era of transformation in which residents and their surrounding environments are increasingly connected through rapidly changing intelligent technologies.
- This transformation offers great promise for improved well-being and prosperity, however, poses significant challenges at the complex intersection of technology and society.
- The goal of the Smart and Connected Communities program is to accelerate the creation of the scientific and engineering foundations (with Advanced Nanomaterials and nanotechnologies) that will enable connected systems and societies to bring about new levels of;
  - Economic opportunity, prosperity, and growth,
  - Safety and security,
  - Health and wellness, and
  - Improve overall quality of life.

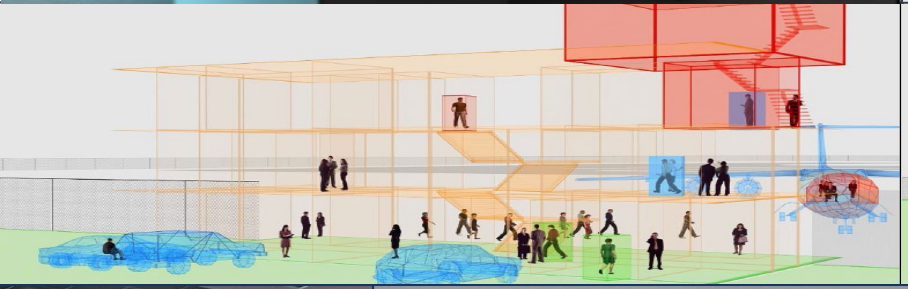
Internet of Behaviors

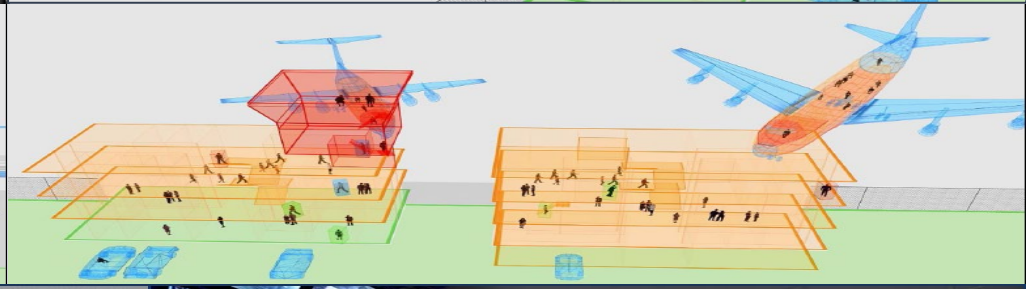
- Internet of Behavior, also known as IoB, refers to the behavioral data analysis gathered from the Internet of Things and other sources and then attempts to make effective use of that data for specific applications. IoB is a relatively new topic when used in the context of IoT. Although in a different context, it has existed for quite some time. (Examples – next slides)
- Due to the ubiquitous nature of IoT, this evolving trend has very useful applications and at the same time poses security risks. This data is amassed through wearable technologies, individual online activities, household electrical devices, and vehicles. When added with biometrics, facial recognition patterns, location tracking, AI, and data analytics – it unleashes a potential that we have not yet considered.
- Studying behavior has been in existence for some time, as most financial institutions use it and so do online retailers – like Amazon. IoB normally refers to personalization, service effectiveness, and adaptability to behaviors. However, accessing behaviors through IoT along with personal physiological data presents challenges.
- We anticipate that almost everyone will likely be exposed to IoB going forward. Examples: Future workforce, lessons from COVID – should we have another pandemic, education, elections, surveys, predictive intelligence tools, and security, … just to name a few.

IoT & IoB and its Implications in CIS Risk Assessment









IoB Examples

- IoB in location tracking
- IoB for the healthcare industry
- IoB in Travel Recommendations
- IoB For E-commerce
- IoB For Logistic Industry
- IoB in Tracking Citizen Behavior For Credit Score
- IoB in improving care insurance pricing

Teachers in Denmark are using apps to audit their students' moods

Companies say the software can help improve well-being, but some experts worry it could have the opposite effect. MIT Tech Review: April 17, 2023

Present objective: Safety and Security of Critical Infrastructures

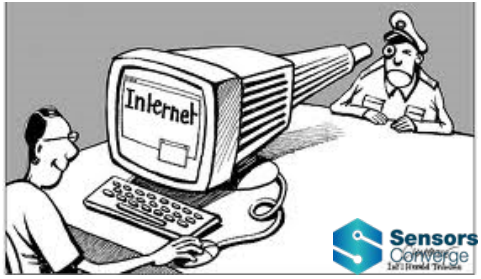
Dual-use Paradigm

The term "dual-use" traditionally has been used to describe technologies that could have both civilian and military usage. Initially used in the context of Nuclear and later in biology (synthetic), the term has, at least, three different dimensions that pose a dilemma for modern technologies and its possible misuse for hostile purposes:

- Ostensibly civilian facilities that are in fact intended for the military – terrorists/bad actors may use;
- Equipment, (information), and agents that could be misappropriated and misused; and
- The generation and dissemination of scientific knowledge that could be misapplied or misused.

Information Technology and Dual Use Paradigm

- Selected aspects
  - Information vs. misinformation/disinformation
  - Social media – Information sharing vs. recruitment by bad actors
  - Enhanced Knowledge vs. distraction
  - Email vs. spam, (Distributed) DoS attacks
  - Cyber security vs. cyber-warfare
  - Critical infrastructure vs. Ransomware (Colonial Pipeline)
  - Automated Health Records vs. Intrusion of Privacy
  - Artificial Intelligence vs. Privacy
  - Machine learning vs. Privacy
  - Foresight vs. Disillusion



Resilience of Critical Infrastructure Systems to Hybrid Threats with Information Disruption
Heimir Thorisson, Fabrizio Baiardi, David G. Angeler, Kuldar Taveter, Ashok Vaseashta, Paul D. Rowe, Wojciech Piotrowicz, Thomas L. Polmateer, James H. Lambert, Igor Linkov.
DOI: 10.3233/NICSP190017

Cyber Risk

- Breach is an uncertain incident (event) created as a result of a system malfunction that severely impacts organizational assets and business objectives.
- Risk - is defined as the potential for harm to an organization's resources when a vulnerability is exploited - loss of privacy, financial loss, legal complications, etc. Hence, the overall risk of the CPS is assessed by analyzing the vulnerability, exposure, and threat of different entities in the critical infrastructure.
- Risk analysis - The process of identifying risks, determining their probability and impact, and identifying areas needing safeguards.
- Risk measurement - A process to determine the likelihood of an adverse event or threat occurring and the potential impact of such an event on the institution. The result of risk measurement leads to the prioritization of potential risks based on severity and likelihood of occurrence.
- Risk assessment - A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact on the institution, its customers, and financial markets, rather than the nature of the threat.

Risk Measures

How to show results?
We need guidelines and scales.

One scale for assessing likelihood
(ex: “Very Likely”, “Likely”, “Possible”, “Unlikely”, “Very Unlikely”)

And

One for severity
(ex: “Severe,” “Significant,” “Moderate,” “Minor,” and “Negligible”)

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

These scales can easily be converted into numbers and plugged into equations for assessing inherent and residual risk.
For example,

“Very Likely” and “Severe” can be assigned as 5
“Very Unlikely” and “Negligible” can be as 1.

Inherent risk

Inherent risk scores represent the level of risk an institution would face if there weren’t controls to mitigate it.

Inherent risk = [Impact of an event] * Probability

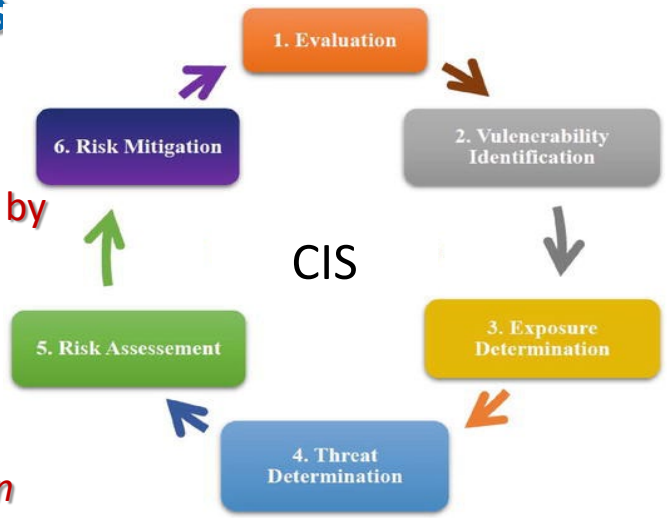
Residual risk

Residual risk is the risk that remains after controls are taken into account.

Residual risk = [Inherent risk] * Control effectiveness

Residual risk is greatest when the inherent risk is high and the controls for mitigating the risk aren’t effective. It decreases when controls are effective.

Risk Assessment in Critical Infrastructures



A risk assessment evaluates both likelihood and impact.

Impact. The impact is an estimate of the harm that could be caused by an event. *For example, a cyber breach could have a catastrophic impact.*

Likelihood. The likelihood of how probable it is that an event will occur. *For example, a cyber breach seems a very likely occurrence when there is no firewalls, endpoint protection software, or intrusion detection software to prevent it.*

The more likely or severe an event, the greater the risk.

- **IoT and IoB** – both are an integral part of many systems around us.
- **Current focus**: IoT and IoB in safety and security in Critical Infrastructures

Sensors Converge

IoT and IoB: Opportunities

Connected home solutions and personal devices

- Security cameras and door locks with face recognition capabilities
- Voice-controlled smart home devices
- Automatic pill dispensers
- Hearing aids
- Indoor navigation systems for the visually impaired
- In-home remote monitoring systems for the elderly and patients with chronic conditions

Fitness devices

- Wearable physical activity trackers, including innovative accessories
- Fitness mirrors with computer vision functionality
- Connected fabrics and apparel
- Training and weight measuring equipment enhanced with sensors

Wellness technology

- Baby tech solutions: camera and sensor-based monitors, smart cribs, intelligent baby formula makers, and connected body temperature thermometers and nebulizers
- Femtech products: smart pads, tampons, and menstruation cups; connected bras and breast cups, hardware-based fertility trackers, pelvic floor training tools
- Vitals monitoring devices: wearables for heart rate, blood pressure, and oxygen monitoring
- Diabetes management systems: smart glucose meters, wearable insulin pumps, and sensor-infused medication storage devices.

IoT and IoB: Opportunities

Smart hospital solutions

- Biometric-based identification systems for patients and hospital staff
- Connected hospital beds with vitals monitoring functionality
- Point-of-care testing equipment
- Stationary medication dispensers
- Integrated IoT systems for inpatient, outpatient, and remote patient care

Implantable and ingestible devices

- Organ systems: heart implants, artificial pancreas systems, smart stents, cochlear implants for individuals with hearing loss, artificial retina implants
- IoT-based prosthetic limb systems
- Neurological IoB solutions: brain-computer interfaces (BCI) with implantable sensors, deep brain stimulation solutions, seizure monitors
- Digital pills for non-invasive diagnostic procedures and medication intake monitoring

Advantages

- 24/7 patient monitoring
- Non-invasive diagnostics
- Improved QoL
- Precision medicine
- Personalized health plans.

IoT and IoB: Challenges

Privacy: collecting, analyzing, and using physiological, behavioral, and biometric data

- IoT devices can track body parameters – walking, working, cardiac, sleep, menstrual cycle, etc. Implication related to accessing these data poses a serious challenge.
- Biometric devices – data from devices such as at the airport, implantable cardiac devices, fingerprint pattern readers, and arm motion trackers (especially for warehouse workers).

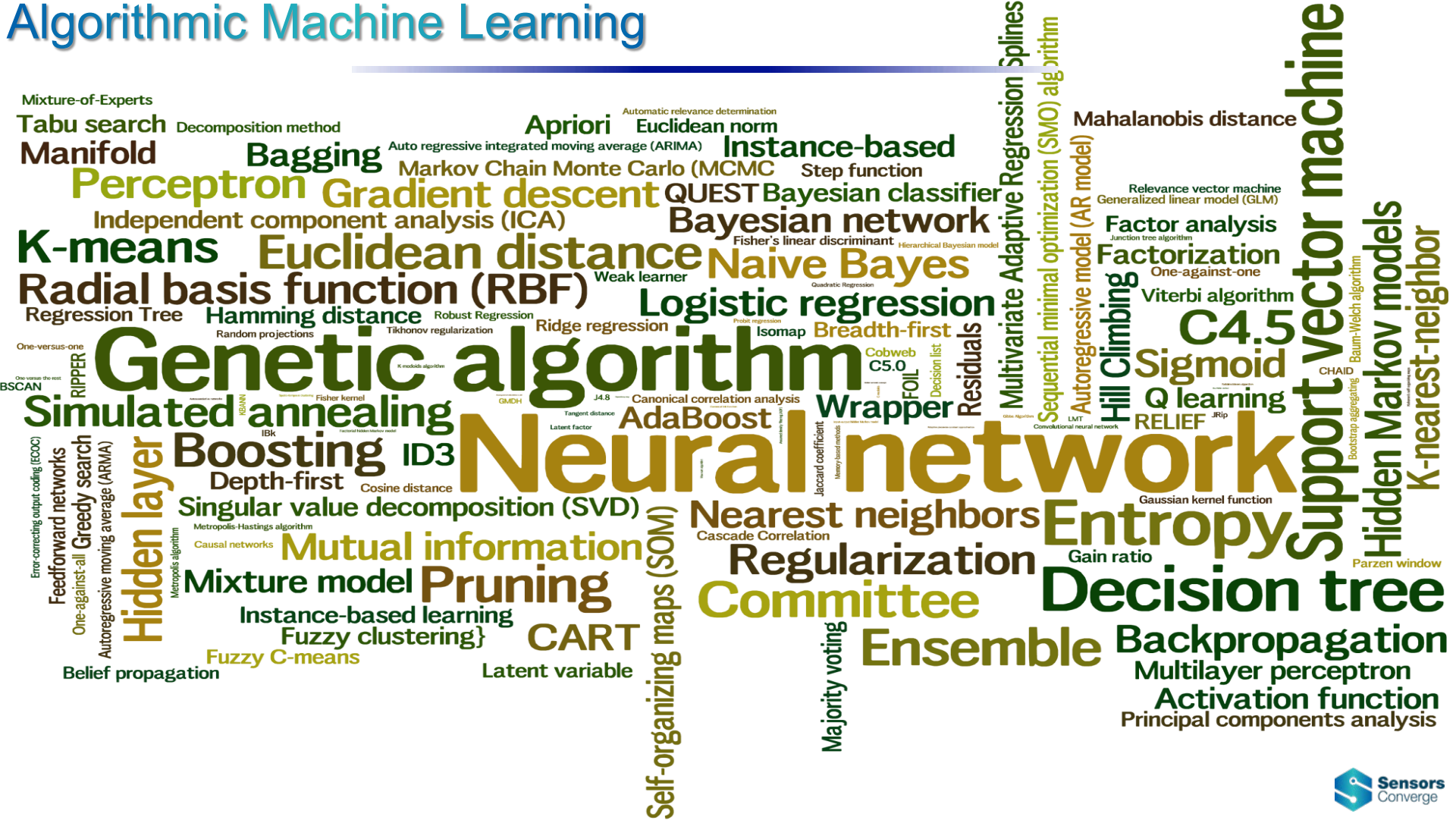
Security

- IoB devices have the same security vulnerability as IoTs. The IP-based cameras have been hacked and have fallen victim to malware attacks. vulnerabilities may span cumbersome software updates installation processes, hard-coded and easy-to-guess passwords, the use of insecure or outdated software and hardware components, and a failure to encrypt data. Personal and biometrics data breach through IoTs needs better security. Also, a comprehensive IoB cybersecurity framework needs to be implemented by NIST and FDA.

Ethics

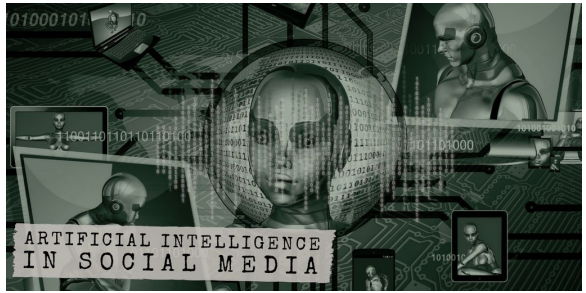
- Without proper regulations, the IoBs might, inadvertently, monitor other people surrounding the user, which violates their privacy. Also, healthcare providers and insurance companies may (or already) incorporate wearable data into treatment plans and health coverage.

Algorithmic Machine Learning



Sensors Converge

Algorithmic Data Analysis and Interpretation – AI, ML, DI, VR

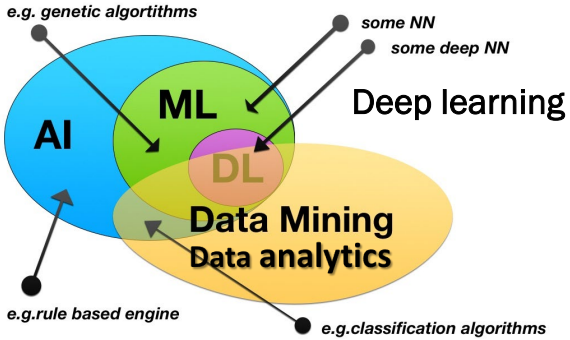


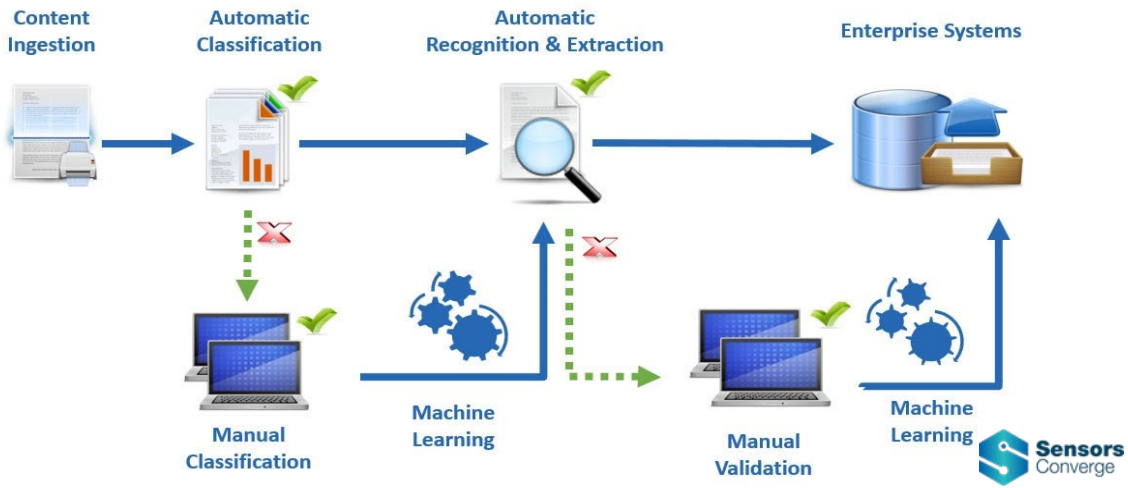
Artificial intelligence holds the potential to transform how brands market their data across networks, such as - Facebook, Instagram, Twitter, and LinkedIn. It can automate many tedious tasks related to social media management, and it can even do social media monitoring at large scale.

Automation – AI takes up the role of delivering your content to your customers. Some of the tasks undertaken are social engagement, scheduling, analytical tracking, etc.

Performance Measurement – AI technology helps marketers review their performances. Be it their social media reach, customer engagement, or social insights, it can collect data to help you review your performance. For example, Hootsuite, an AI technology, allows you to gain insight into your customer preferences.

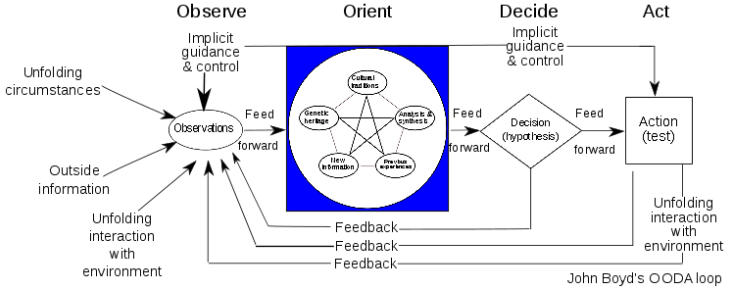
Optimized Content – Since AI technology can optimize social media content with machine learning, it optimizes and displays the content according to your preference pattern.





Application of AI, DL, ML in Defense

- Animal research that translates to operational readiness
- Human performance optimization – predictive intelligence for over-training/overreaching
  - Apps in TBI, muscle failure during endurance (bonking), infection, sleep, nutrition, and behavior
- Use of AI in how outside entities work within secure environments
- AI in surgery in the austere environment
- TBI – use of neuro optometry and neuro radiology – Intrepid emergency center
- Biomarkers/physiological response
- Quantum computing in Data security.
- AI in OODA loop



Notes taken on 09/29/2021

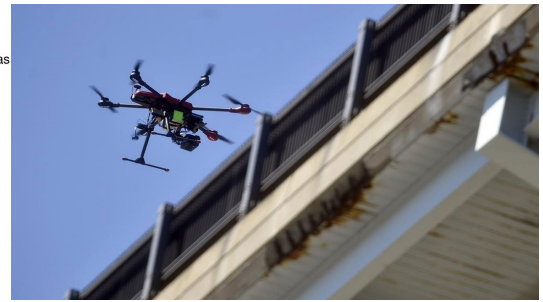
Use of UAVSP in Power Grid, Transport, Hydrology etc.

- ❑ Railroads
  - ➢ Track alignment
  - ➢ Track surface integrity
  - ➢ Track wear and tear
  - ➢ Bridge inspection
  - ➢ Telecommunication antenna
  - ➢ Corridor vegetation encroachment
  - ➢ Physical and mechanical threat security
  - ➢ Air quality monitoring
  - ➢ Spill and Environment monitoring
  - ➢ Facilities management
  - ➢ Construction progress reporting
- ❑ Power Grid
  - ➢ Many examples
- ❑ Hydrology
  - ➢ Many Examples

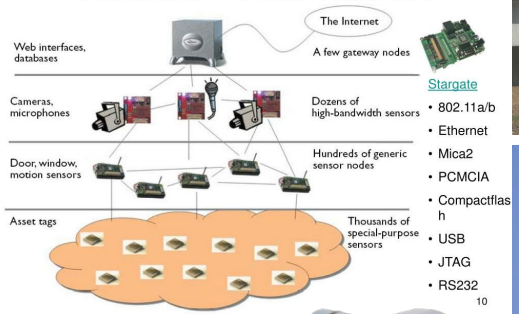
Use of UAVSP in Public Infrastructure

- Cases: Bridges, Dams, Tunnels, Highways, more…
  - Corrosion
  - Roadbed wear
  - Weather and flooding damage
  - Spillway cracks
  - Geologic site conditions
  - Hydrology
  - Emergence Preparedness documentation
  - Structural Stability
  - Vegetation encroachment
- Examples
  - Embedded sensor systems for load testing
  - Surface deflection
  - Environmental parameters
  - License Plate Readers
  - Cell phone tower ping recording
  - IR cameras (thermal imaging)
  - Real-Time Beyond Visual Line-of-Sight (BLOS)
  - Vehicle Reconnaissance System (VRS)
  - Black Hornet Personal Reconnaissance System (PRS

Oblique & NADIR Aerial Imagery



Wireless Sensor Network



Sensors Converge

Rapid Risk Assessment/Verification Research

PC-based rapid risk assessment tool: TechFARM, ADAMS, NESTTS

Verification center

- Online monitoring
- Water treatment
- Decontamination/filtration
- Water Management

ETV

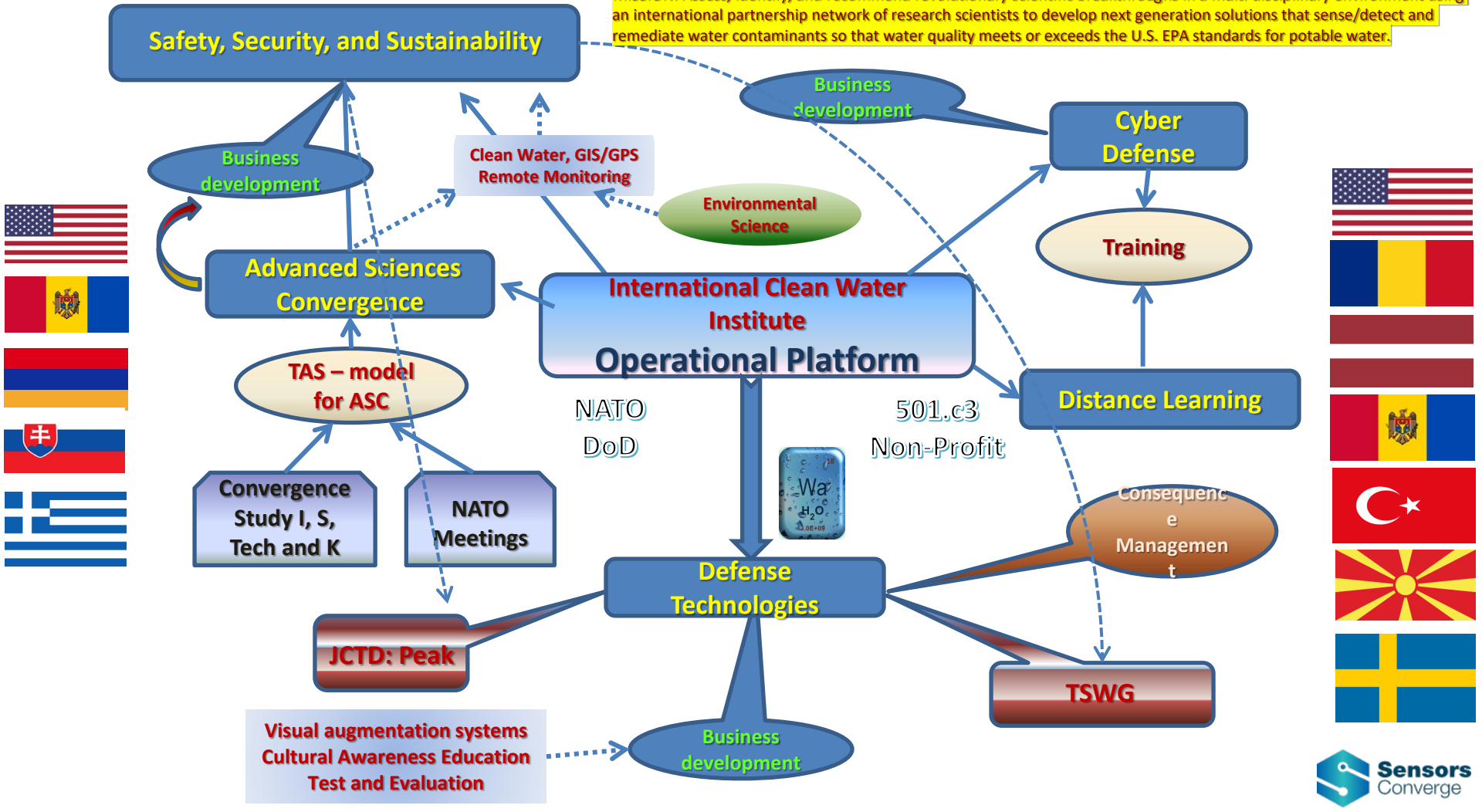
- Threat scenario simulations and screening level risk analyses - TTX/FTX
- Threat Assessment
- Disease surveillance

Sensors Converge

Conclusions and Path Forward

- Paradigm shift using nexus of technological innovations
- Convergence of interdisciplinary fields to monitor risks in the structural integrity
- Smart and Connected Systems to enhance situational awareness
- Integration of new platforms, IoT & IoB
- Creation of new opportunities
- New challenges
  - privacy vs security
  - Licensing requirements – RPIC
  - Bandwidth – needs different frequency bandwidth and its integration with L3, G4, or G5.
  - Weight vs battery lifetime
  - Civil applications vs law enforcement
  - Medical Emergencies - jurisdiction

MISSION: Assess, identify, and recommend revolutionary scientific breakthroughs in a multi-disciplinary environment using an international partnership network of research scientists to develop next generation solutions that sense/detect and remediate water contaminants so that water quality meets or exceeds the U.S. EPA standards for potable water.



Sensors Converge

Contact

Ashok Vaseashta, Prof. Dr. Acad.

International Clean Water Institute, Manassas, VA USA

Transylvania University of Brasov, Brasov, ROMANIA

Ghitu Institute of the Electronic Engineering & Nanotechnologies, Chisinau, MOLDOVA

Email: prof.vaseashta@ieee.org