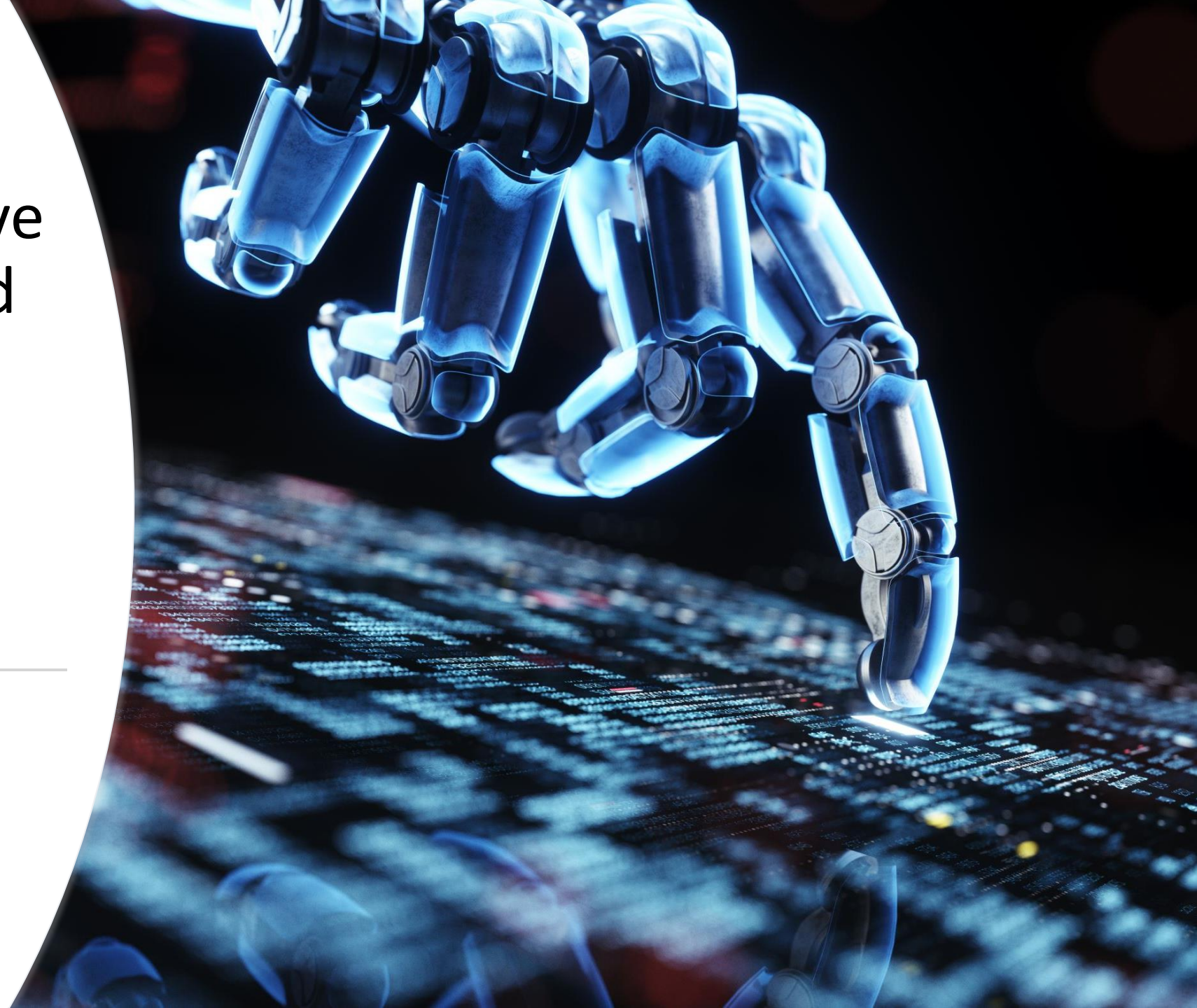
# Integrated Adaptive Cyber Defense and the Importance of Knowledge Representation & Reasoning

Shawn P. Riley

Chief Cybersecurity Scientist

Cybersecurity Science with Shawn Riley



# About Me

- 30+ years in Information Security
  - 13 years in applied AI for cybersecurity
- U.S. Navy Veteran
  - Cryptology Community
- Cat Dad

- Location: Las Vegas, NV, USA
- LinkedIn: https://www.linkedin.com/in/shawnriley71/
- Blog: https://cybersecurityscience.blogspot.com/

# Agenda

- How today's talk aligns with Cybersecurity Science
- Overview of Cybersecurity to frame the talk
- Overview of Integrated Adaptive Cyber Defense (IACD)
- Overview of Knowledge Representation & Reasoning (KR&R)
- Overview of the 4 Levels of Interoperability
- Practical Examples that pull it all together

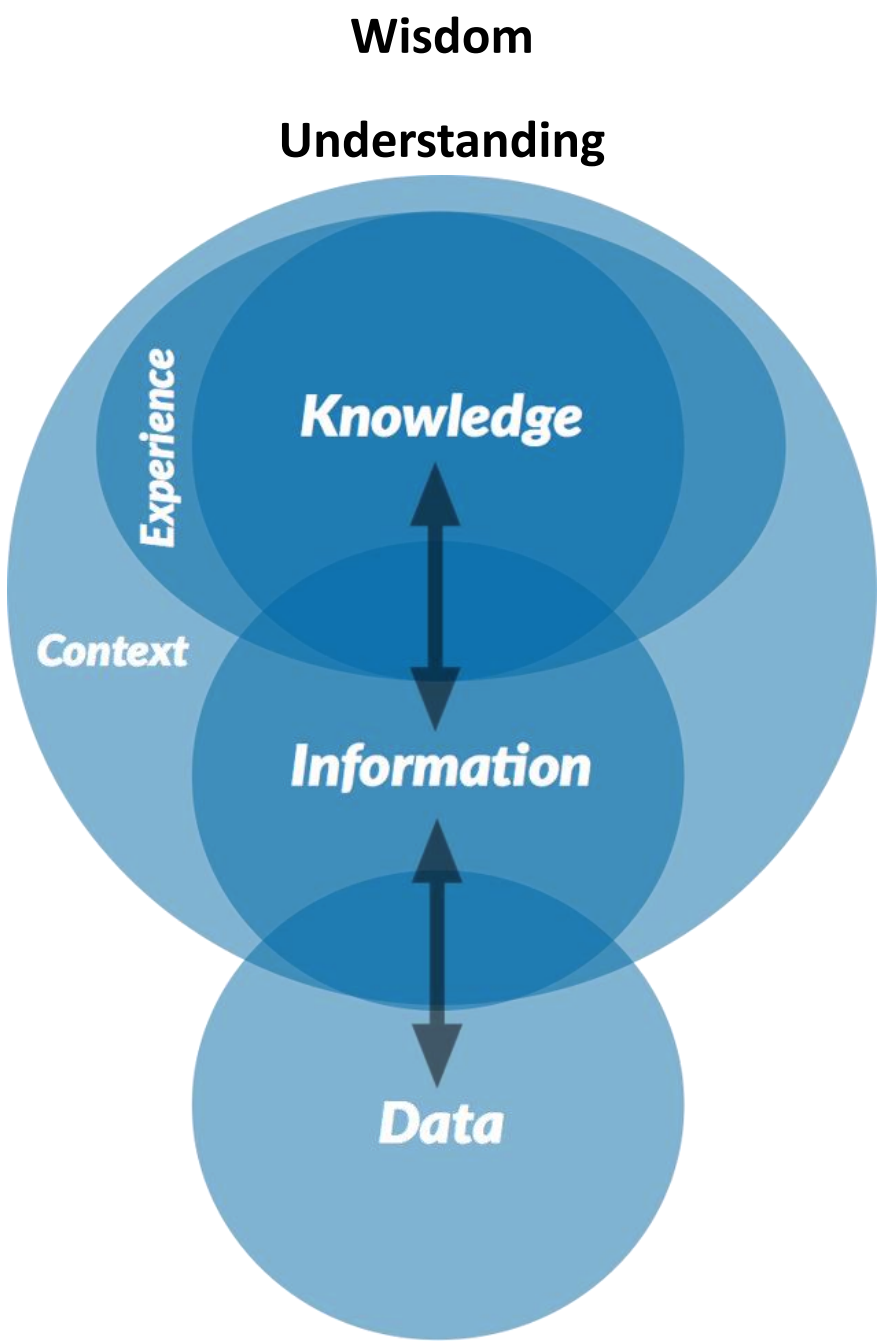
# Cybersecurity Science

Knowledge Representation and Reasoning (KR&R) is closely related to the Cybersecurity Science core theme of Common Language. In cybersecurity science, Common Language refers to establishing a standardized and shared understanding of concepts, terms, and representations within the field.

KR&R plays a vital role in achieving a Common Language in cybersecurity by providing a formal framework for representing and organizing knowledge related to cybersecurity concepts, threats, vulnerabilities, attacks, and defense mechanisms. It allows cybersecurity professionals to capture and structure domain-specific knowledge in a consistent and machine-readable manner.

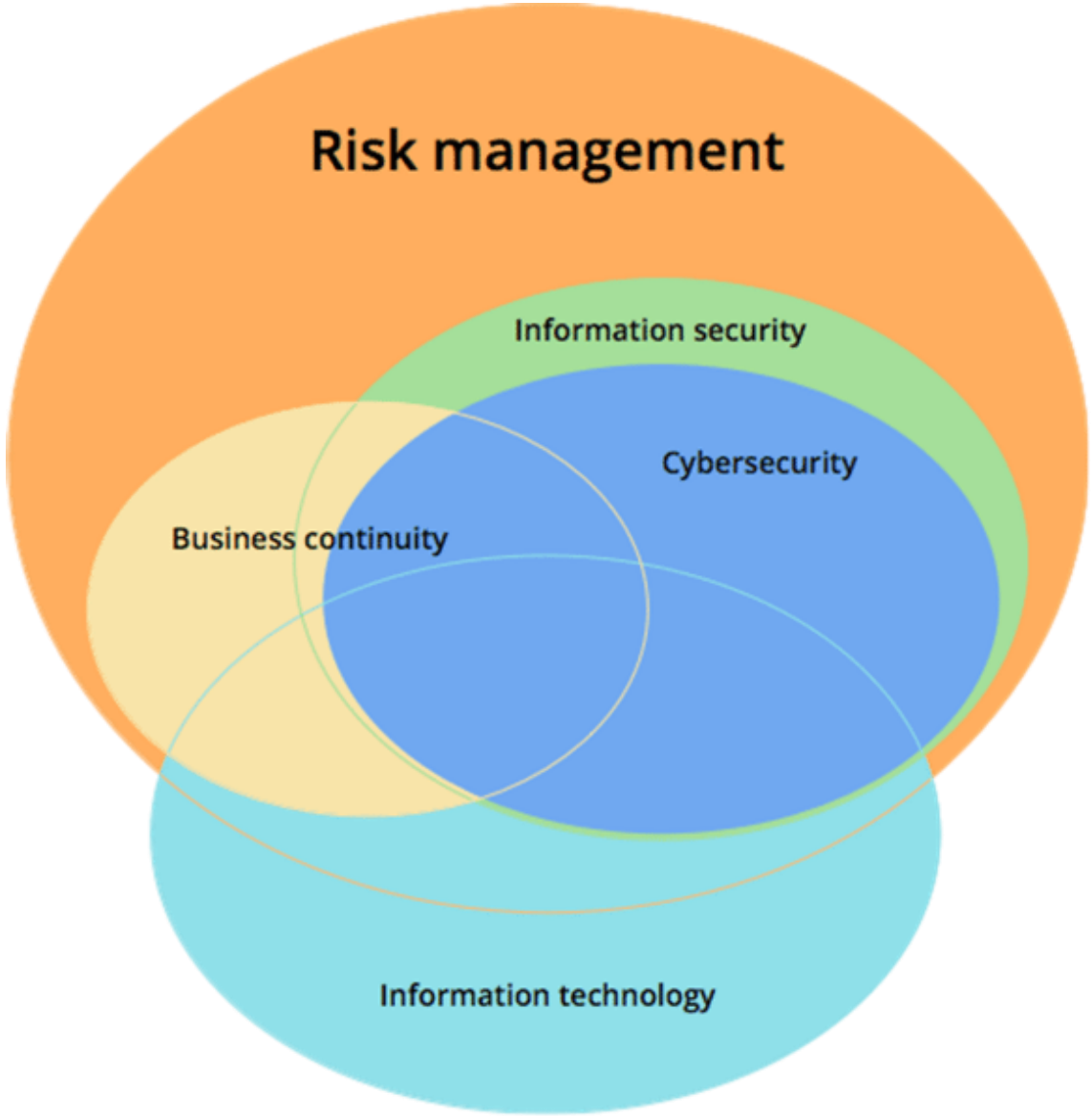
By employing KR&R techniques, cybersecurity experts can create ontologies, taxonomies, and knowledge graphs that facilitate the sharing, integrating, and analyzing of cybersecurity information. These formal representations enable the development of intelligent systems and decision-support tools to reason about cybersecurity knowledge, detect anomalies, identify patterns, and propose effective countermeasures.

# From Data to Wisdom

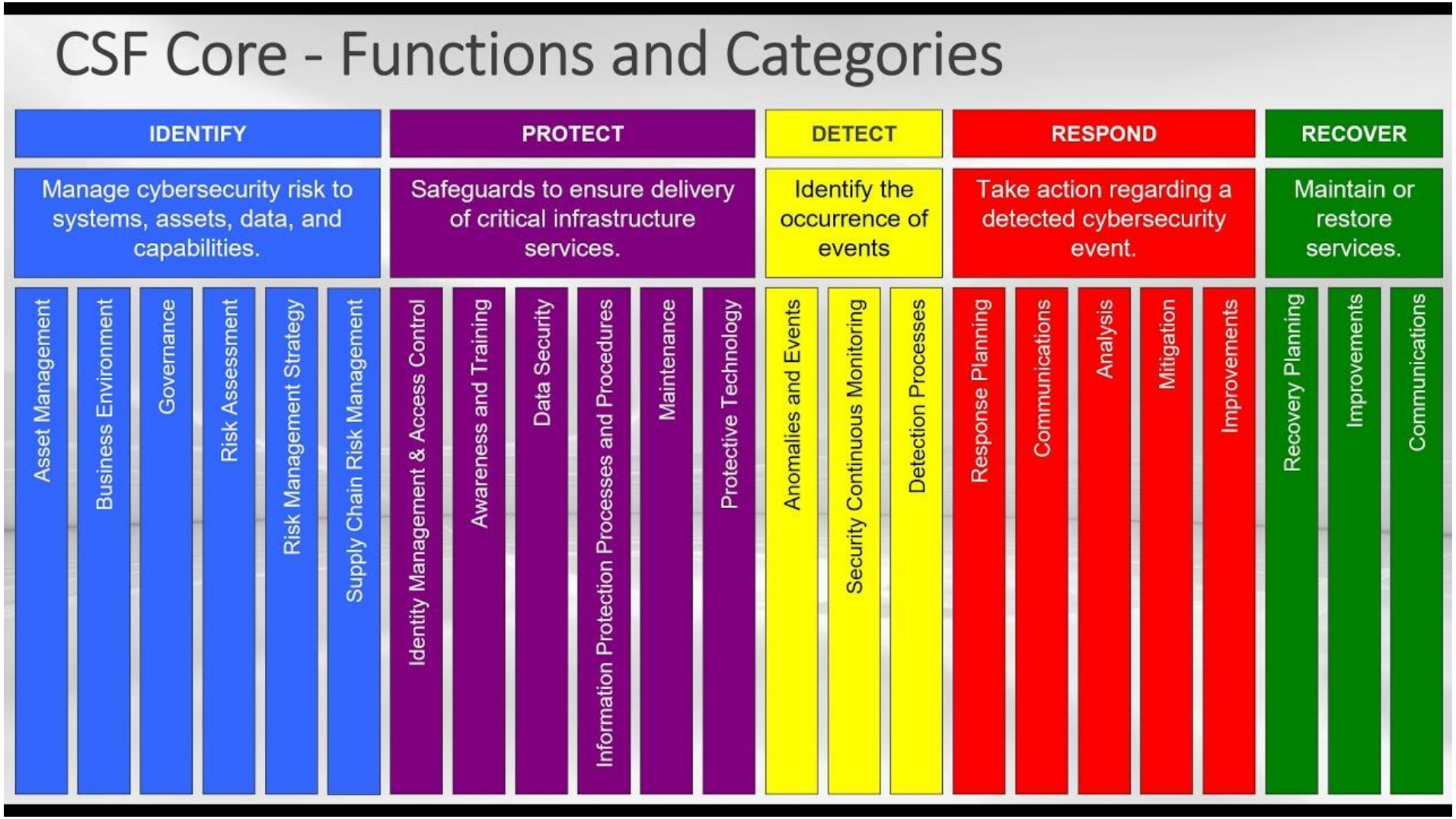



https://www.linkedin.com/pulse/from-data-wisdom-integrated-adaptive-cyber-defense-importance-riley/

# What is Cybersecurity

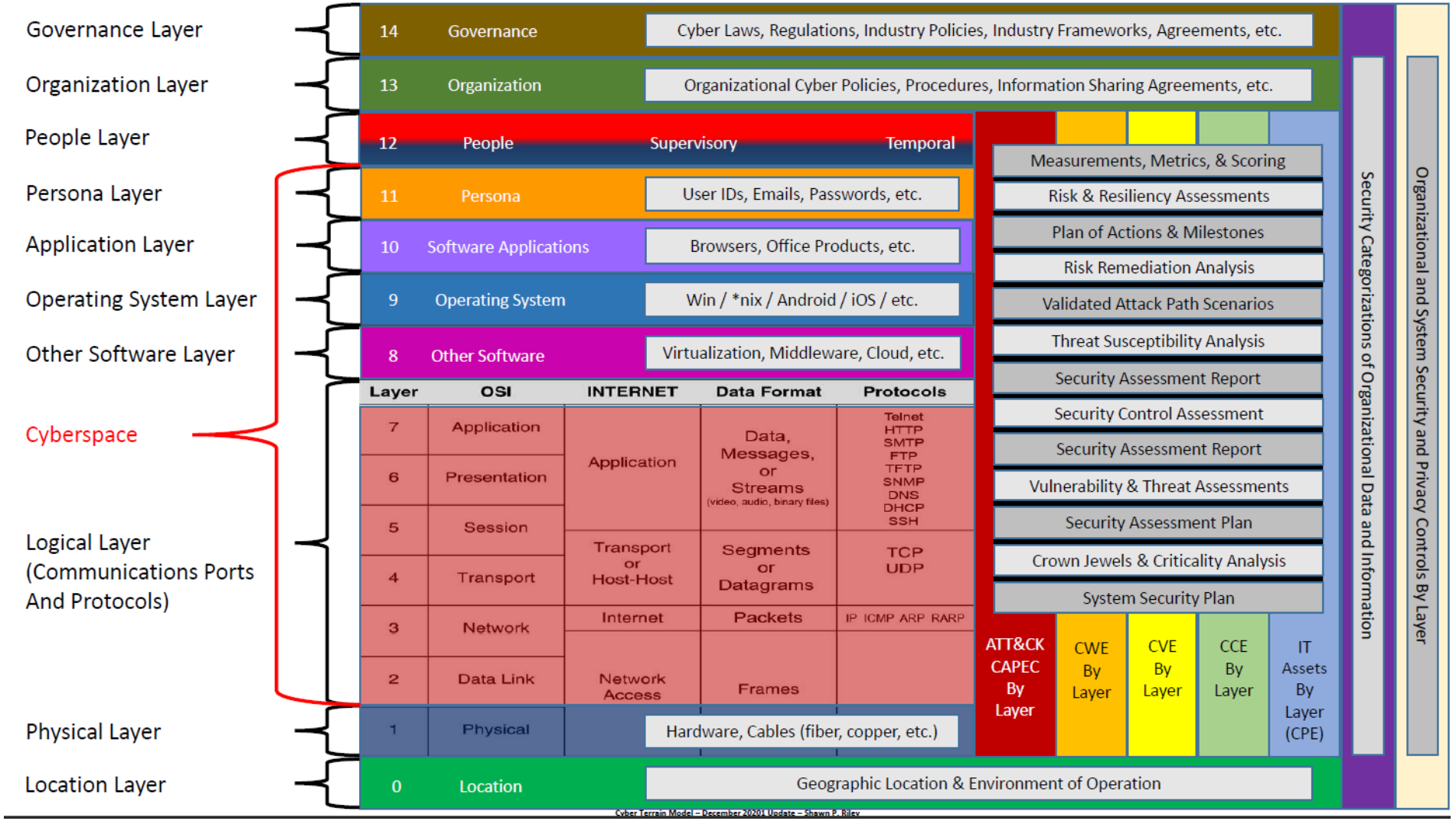


# Cybersecurity Core Functions & Categories



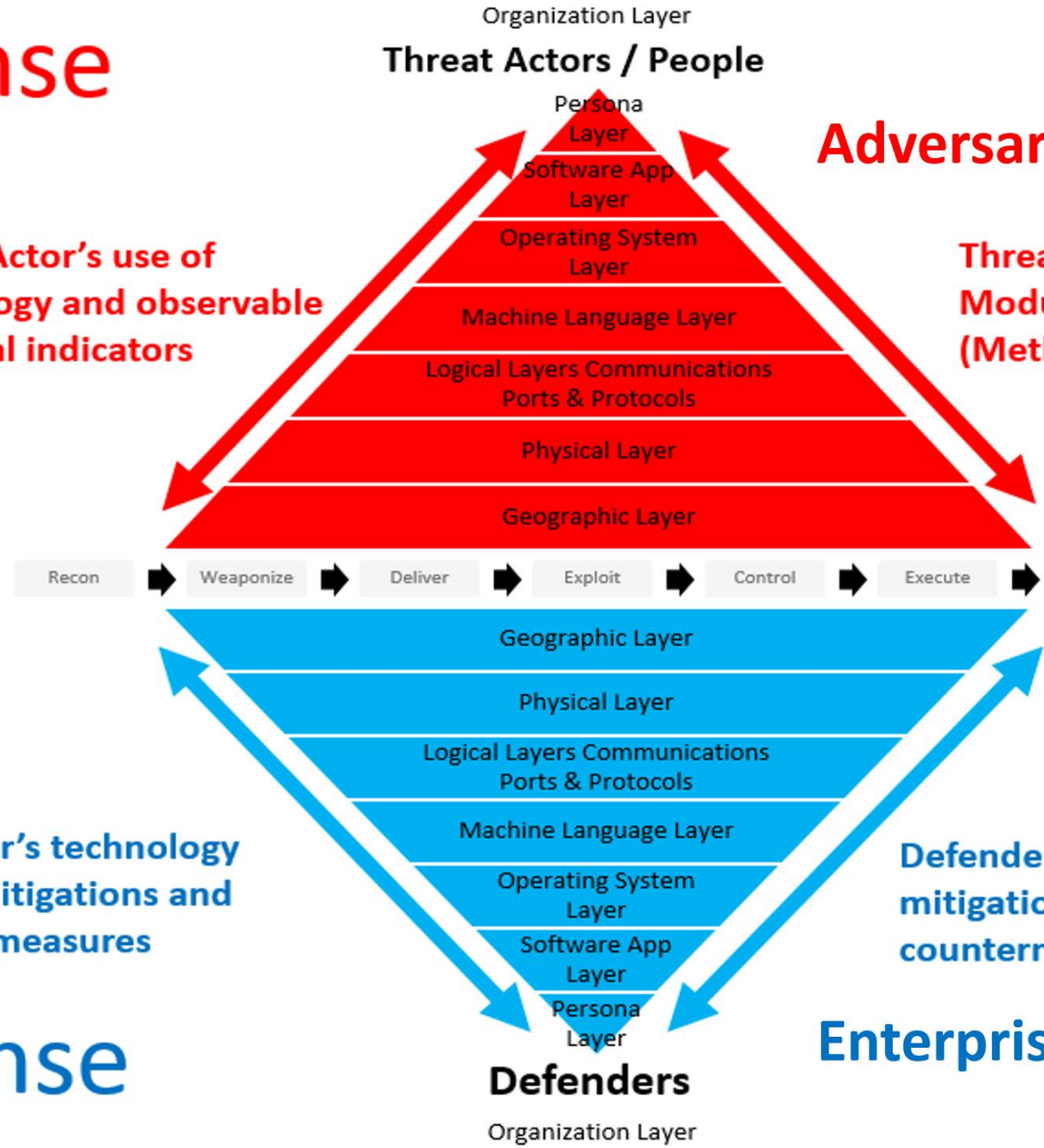

https://www.nist.gov/cyberframework

# The complexity of Information in the Cyber Environment




https://www.linkedin.com/pulse/asking-chatgpt4-what-thought-my-cyber-terrain-model-shawn-riley/

# Offense




**Adversarial Contextual Knowledge**

**Threat Actor's use of technology and observable technical indicators**

**Threat Actor's Modus Operandi (Methods of Operation)**

**Technology / Cyber Terrain**

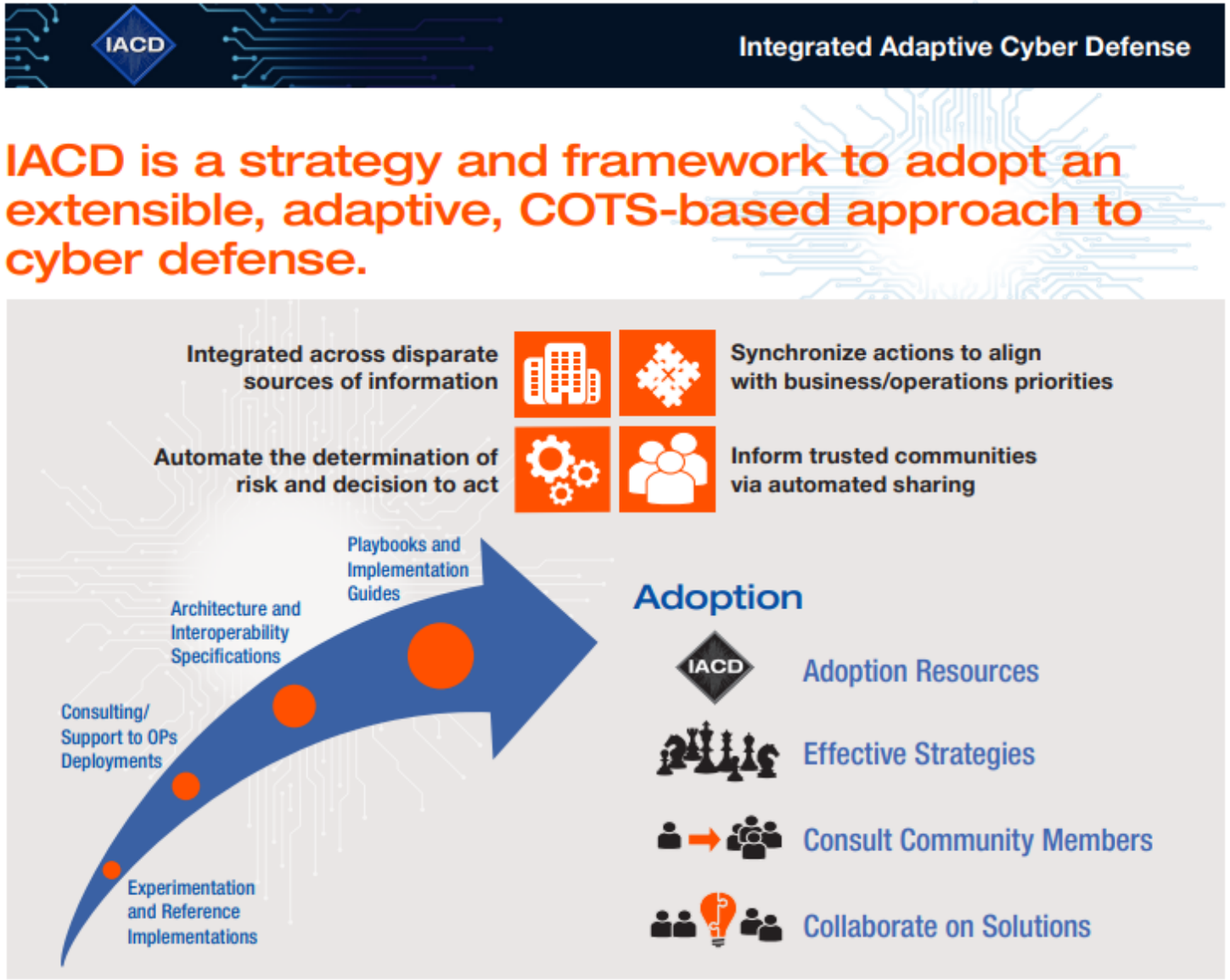
**Processes TTPs**

**Defender's technology based mitigations and countermeasures**

**Defender's process based mitigations and countermeasures**

# Defense

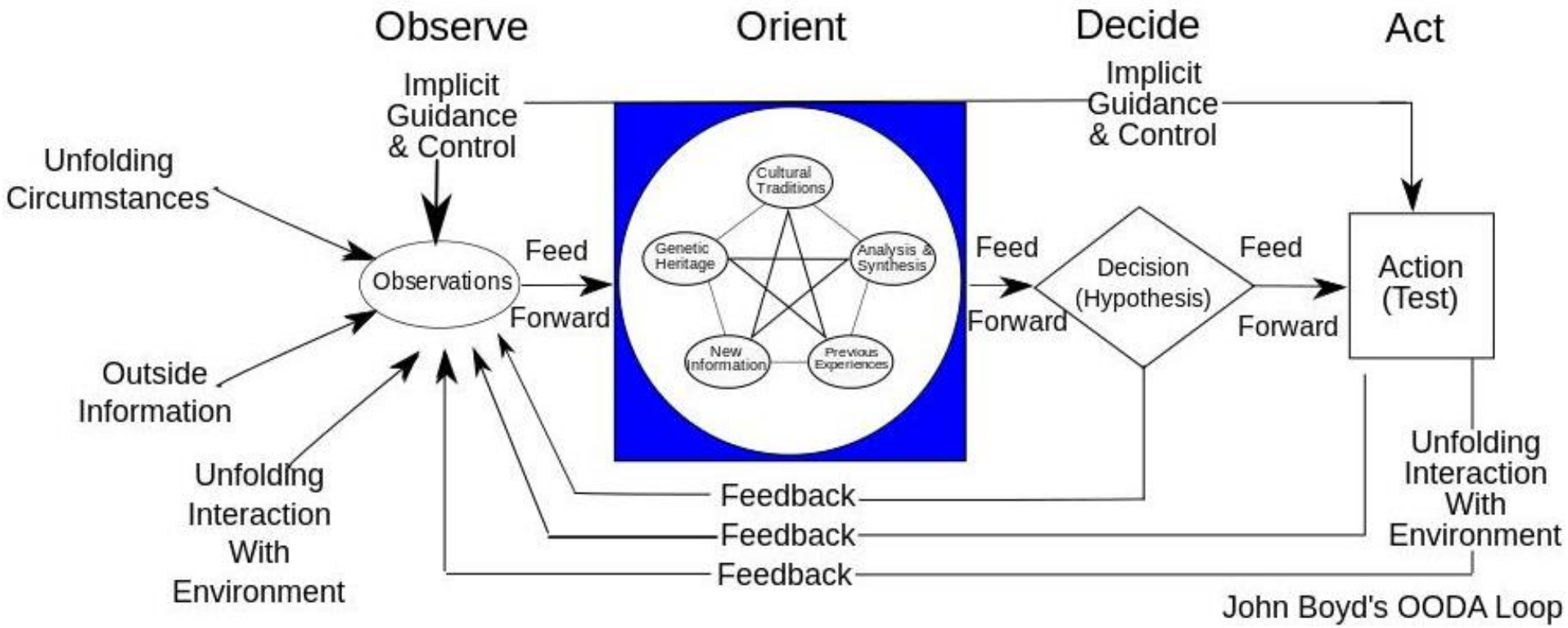
**Enterprise Contextual Knowledge**



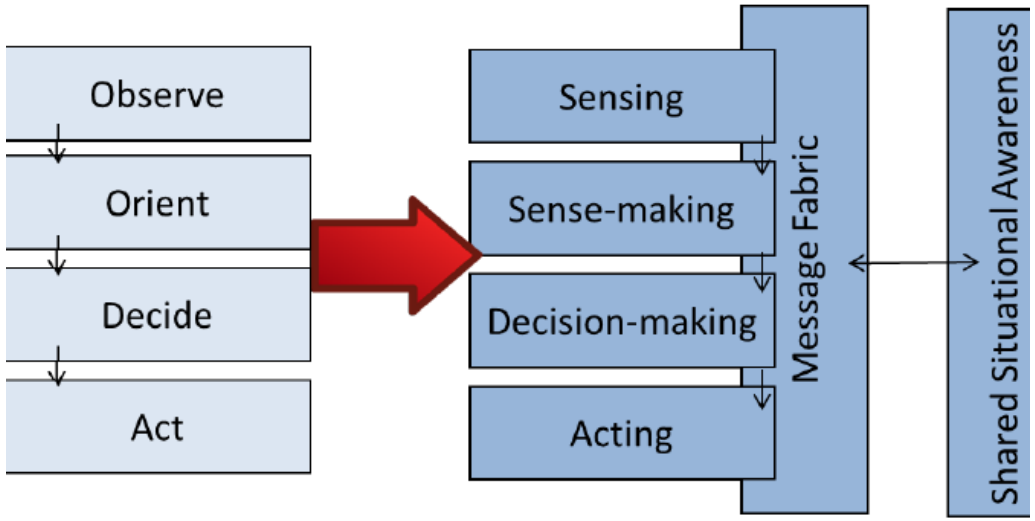

# Integrated Adaptive Cyber Defense (IACD)

Our goal is to dramatically change the timeline and effectiveness of cyber defense via integration, automation, orchestration, and sharing of machine-readable cyber threat information.

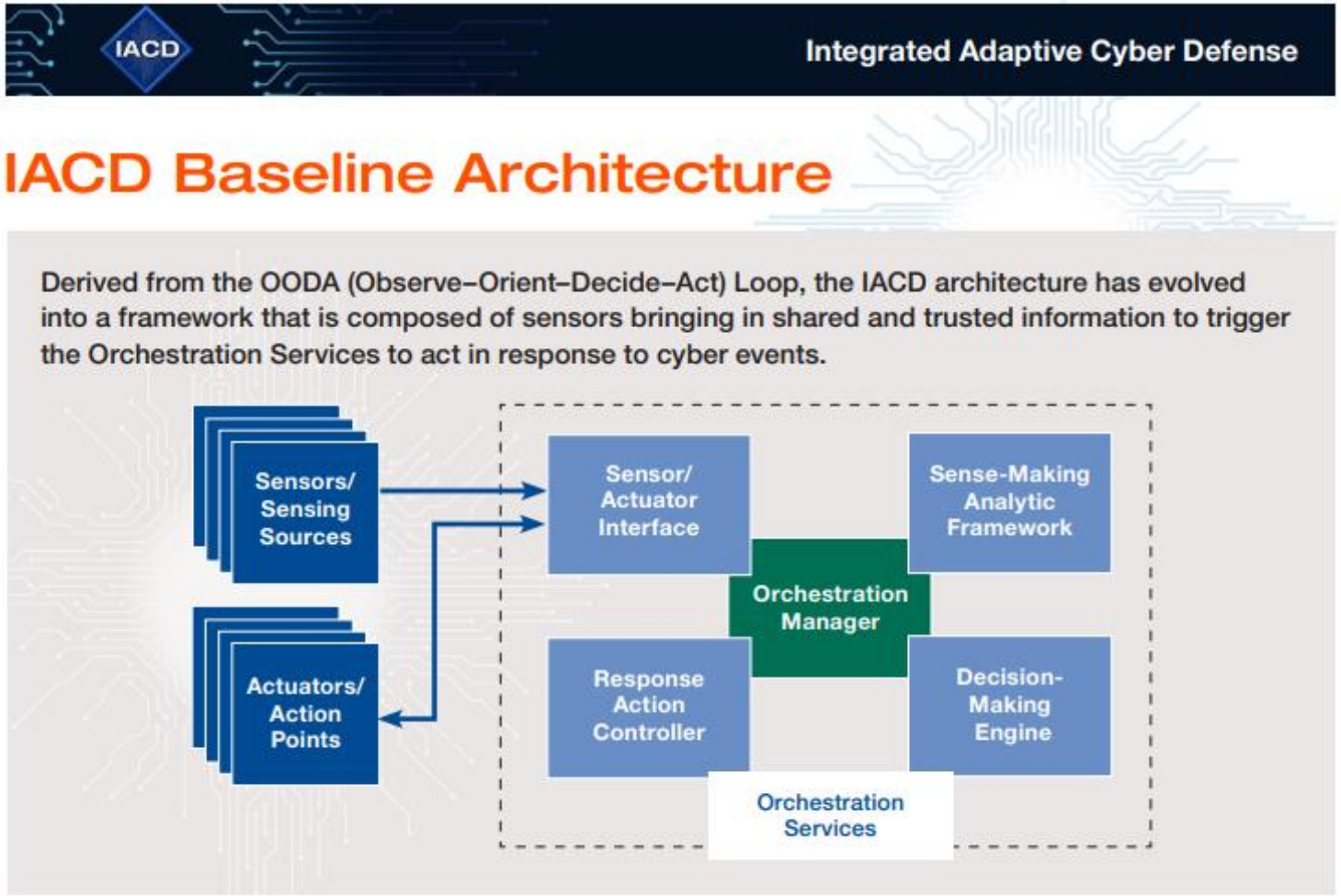
https://www.iacdautomate.org/




John Boyd's OODA Loop



# The Cyber OODA loop in IACD



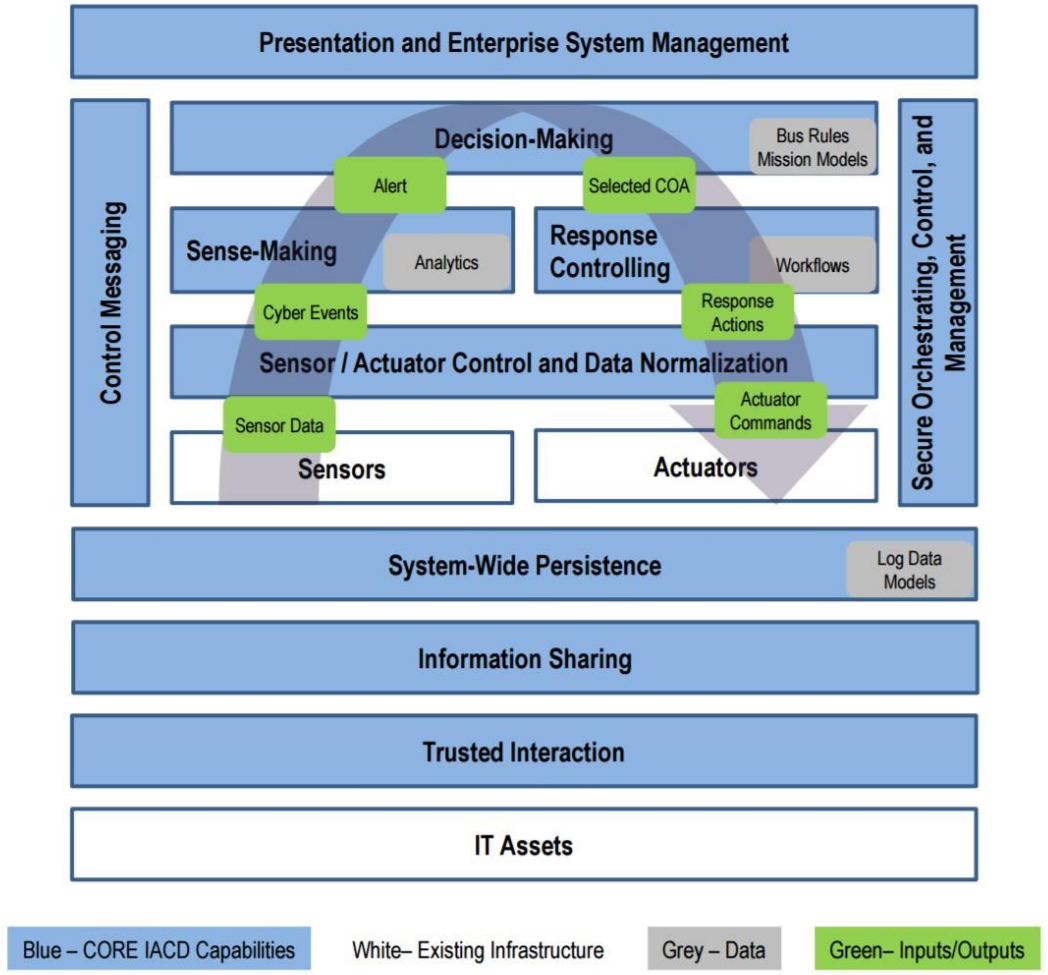
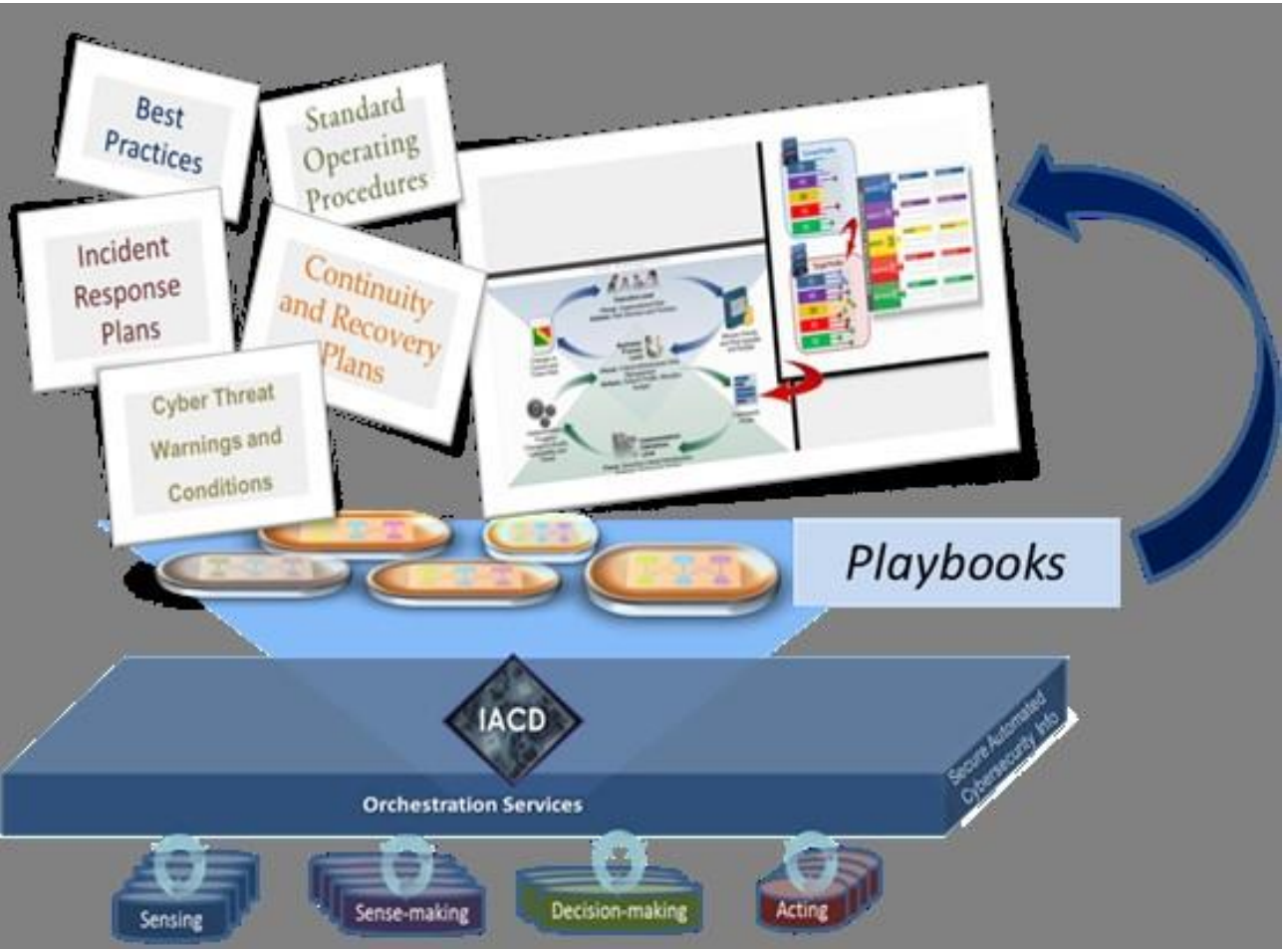
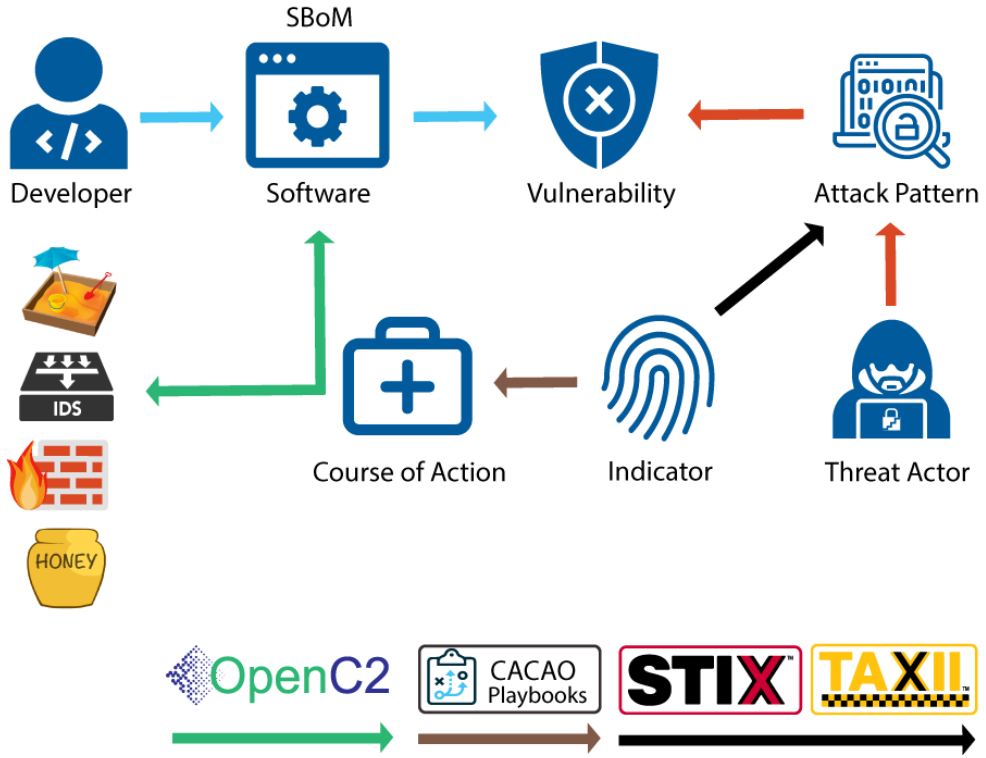




**Figure 1 Integration of IACD Capabilities through the OODA Loop**

https://www.iacdautomate.org/

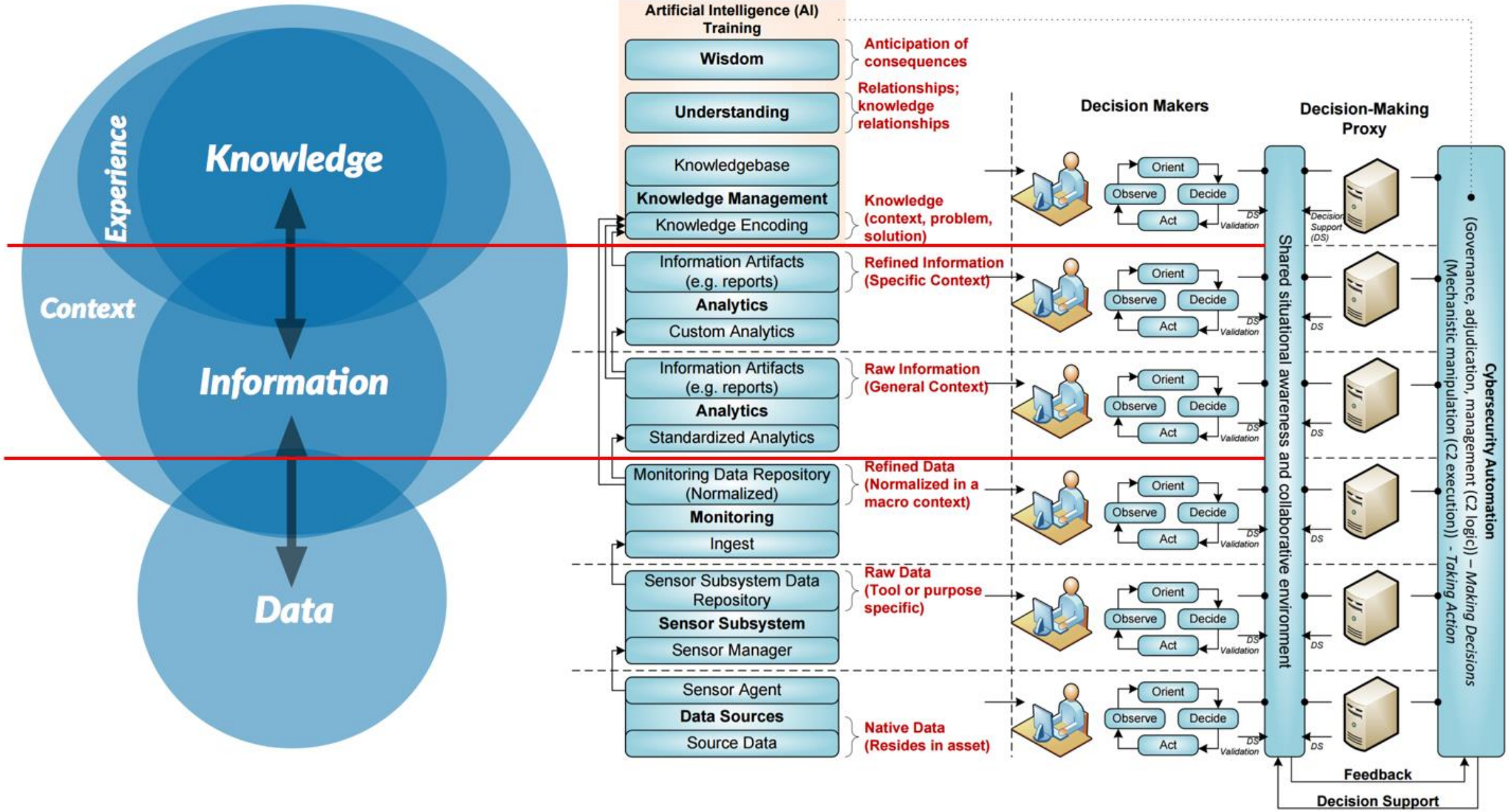
# IACD Playbooks → OASIS Open Standards

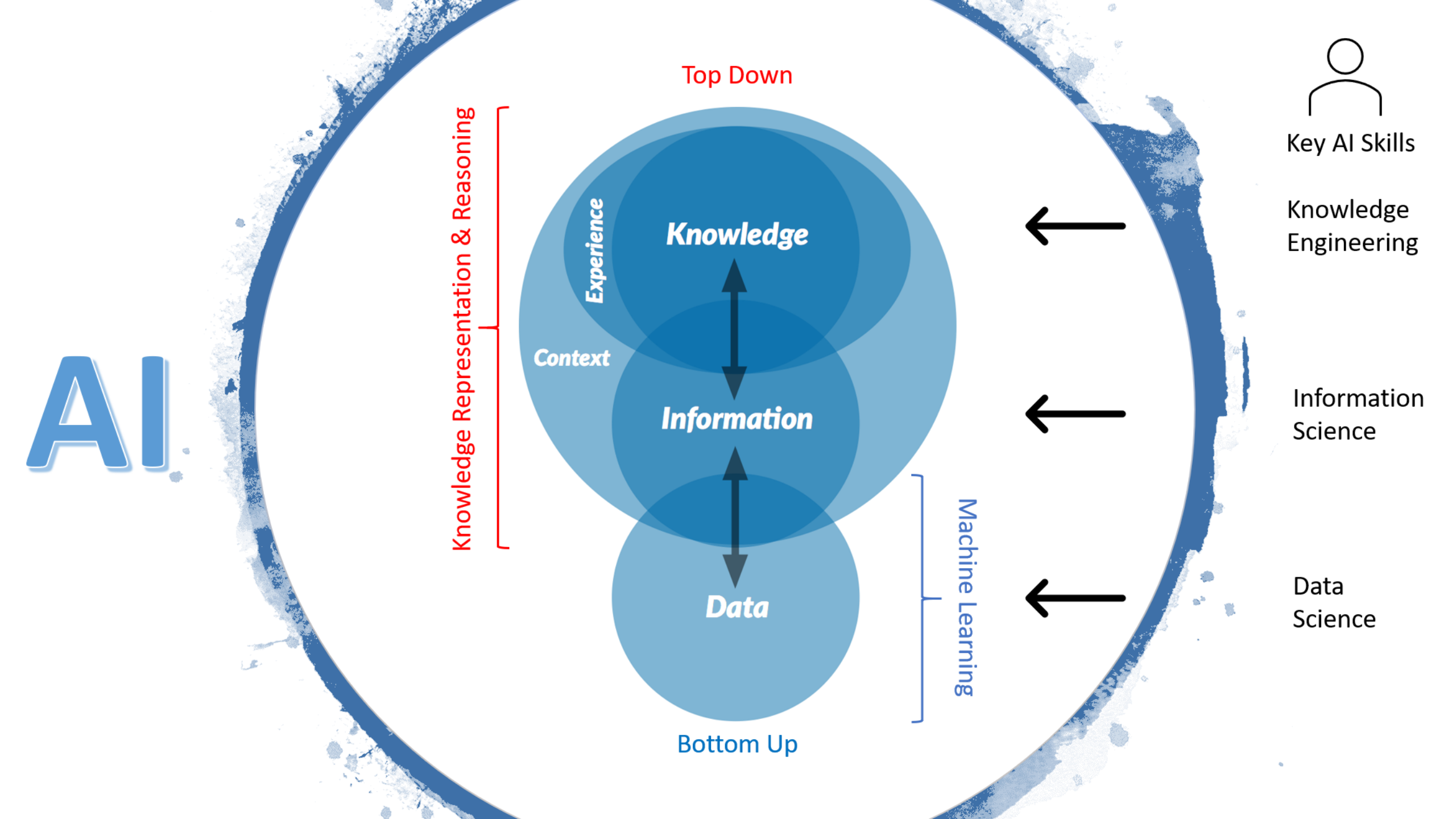



**OpenC2 – Open Command & Control Language**
**CACAO - Collaborative Automated Course of Action Operations**
**STIX – Structured Threat Information eXpression**
**TAXII – Trusted Automated eXchange of Indicator Information**

# Integrated Cybersecurity Decision Pattern Knowledge = Context, Problem, Solution

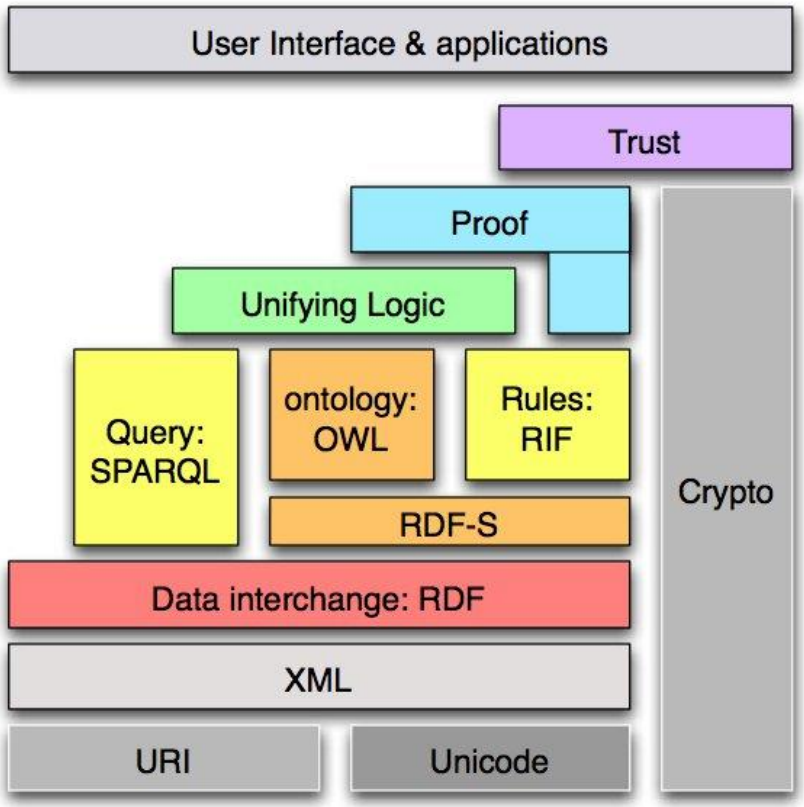



AI
Top Down
Knowledge Representation & Reasoning
Experience
Knowledge
Context
Information
Data
Machine Learning
Bottom Up
Key AI Skills
Knowledge Engineering
Information Science
Data Science

# Knowledge Representation & Reasoning

- Knowledge Representation and Reasoning (KR&R) is a field of artificial intelligence that deals with the representation of knowledge, allowing computational systems to reason, make inferences, and solve problems. It involves the development of formal languages, frameworks, and techniques to capture and organize knowledge in a structured and computationally tractable form.
- Knowledge representation refers to capturing and encoding knowledge from a specific domain into a formal representation that a computer can understand and process. This representation typically uses symbols, concepts, relationships, rules, and constraints to model real-world knowledge.
- Reasoning refers to drawing logical deductions, making inferences, and answering questions based on the knowledge representation. It involves applying rules, algorithms, and inference mechanisms to manipulate and derive new knowledge from existing knowledge.
- A.K.A. Machine Reasoning, Machine Understanding, Expert Systems, Knowledge-Driven AI, Knowledge Graph AI, etc.

# Most Used for KR&R – W3C OWL/RDF (Not Prolog)




**SHACL – Constraints**

**RML – RDF Mapping**
**(Not W3C but popular)**

**OWL (Web Ontology Language) and RDF (Resource Description Framework) are considered leading knowledge representation languages for several reasons:**

1.Expressive Power: OWL and RDF provide a rich set of constructs for representing knowledge, including classes, properties, individuals, relationships, and axioms.

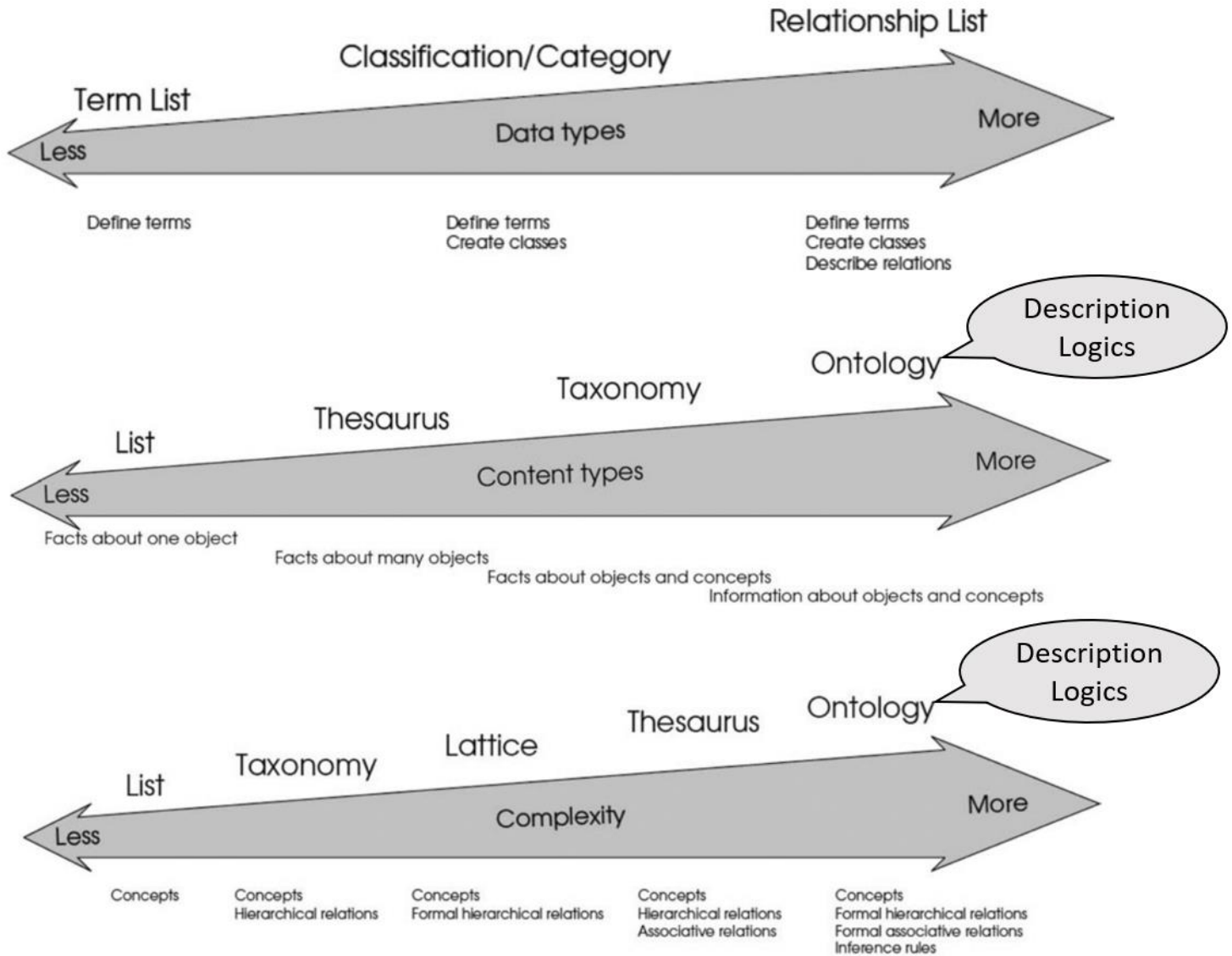
2. Semantic Interoperability: OWL and RDF promote interoperability by providing a standardized and flexible framework for representing and linking data across different domains and sources. They enable the integration of diverse information and facilitate data sharing and exchange.

3.Reasoning Capabilities: OWL, specifically, is designed to support automated reasoning. It provides a set of logical constructs and reasoning mechanisms that allow for inferencing and deduction.

4.Semantic Web Compatibility: OWL and RDF are designed to capture and convey semantic information, enabling machines to understand and process the meaning of data.

# Data Information Knowledge

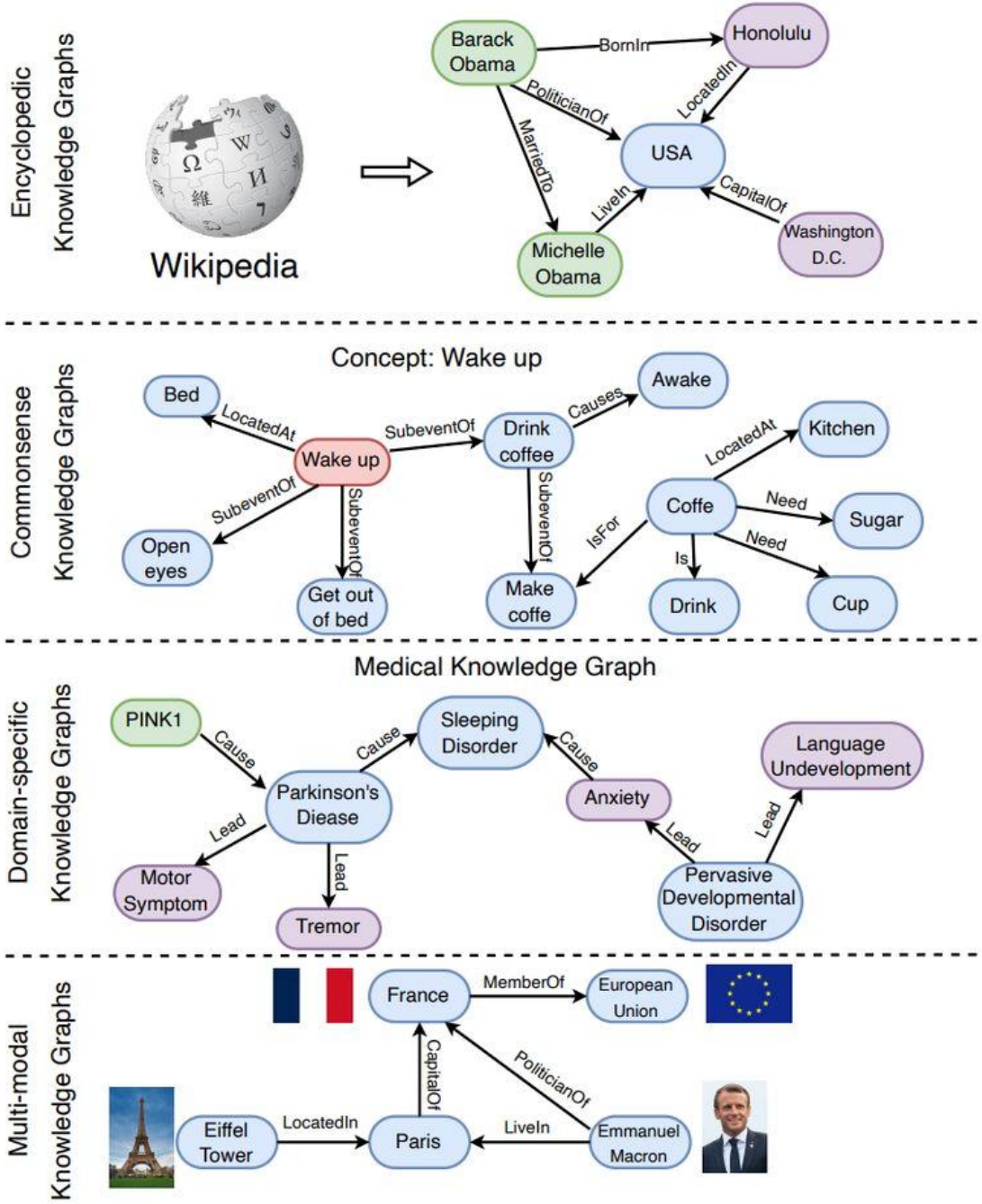
Data Science
Machine Learning
Inductive Statistical Inference




Deductive Logical Inference
Machine Understanding
Knowledge Engineering

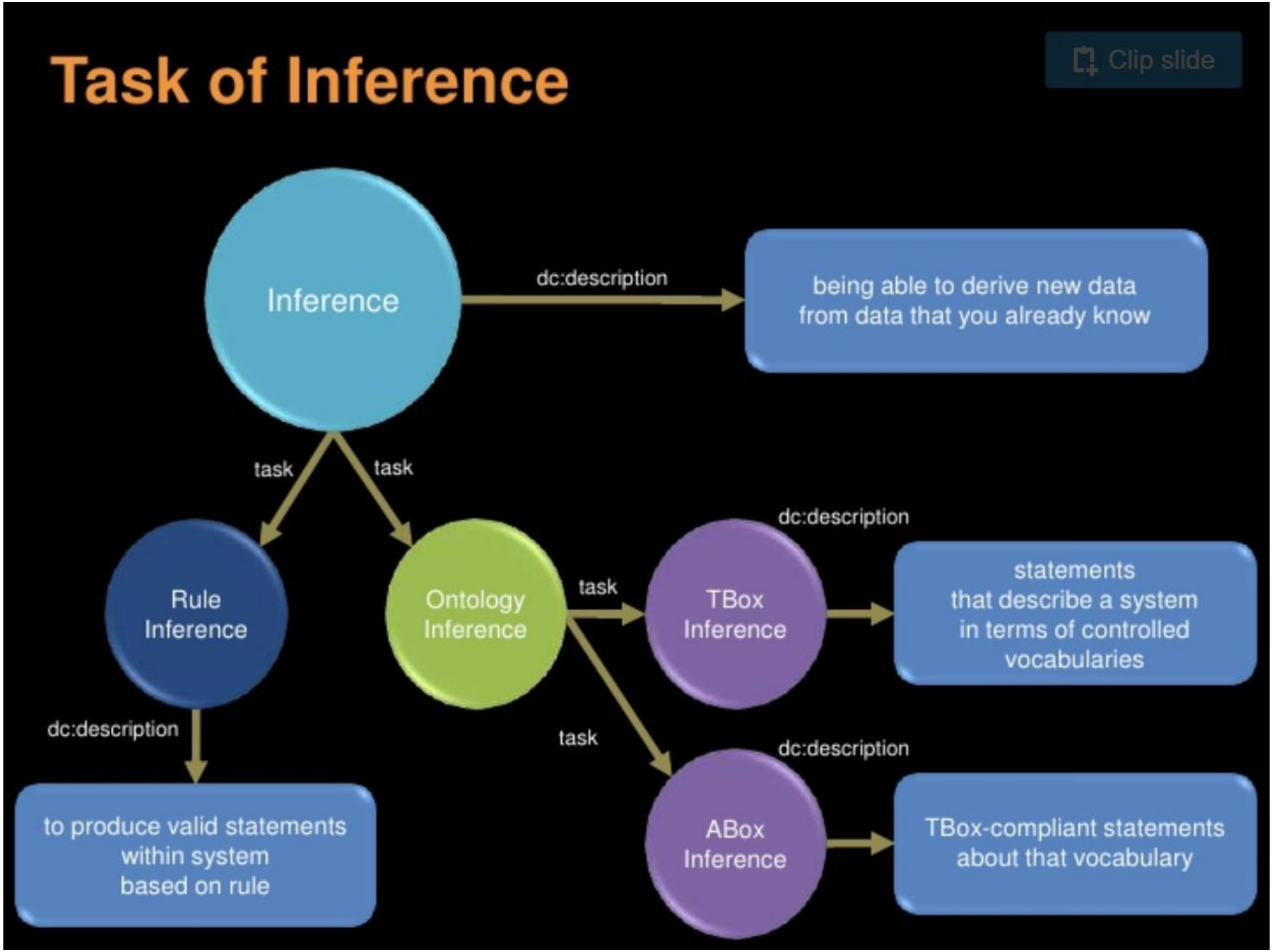
https://cybersecurityscience.blogspot.com/2023/03/understanding-data-models-from-lists-to.html

# Knowledge Graphs




https://arxiv.org/pdf/2306.08302.pdf

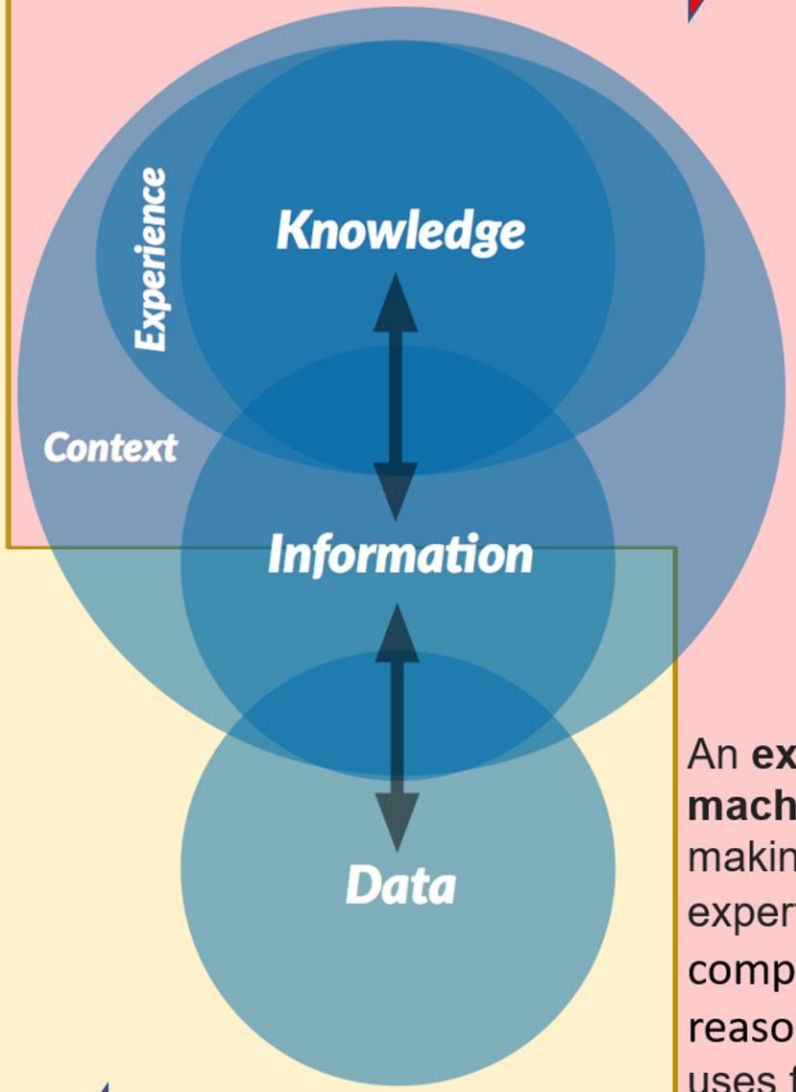
# Task of Inference

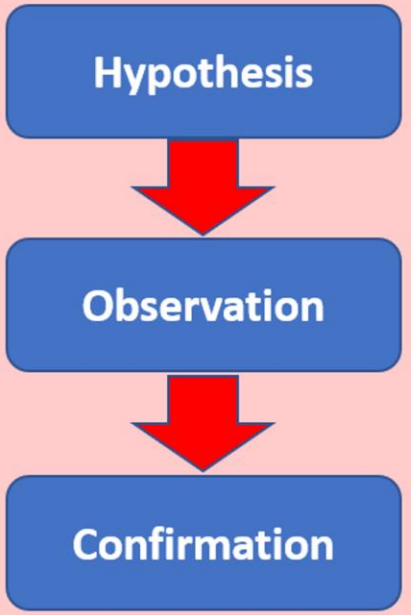


**Machine Learning** focuses on prediction, based on *known* properties learned from the training data. **Inductive Reasoning** uses patterns to arrive at a conclusion (conjecture). **Note:** A conclusion derived through inductive reasoning is called a hypothesis and is always less certain than the evidence itself. In other words, the conclusion is ***probable***.

**Knowledge Representation And Reasoning Expert System**

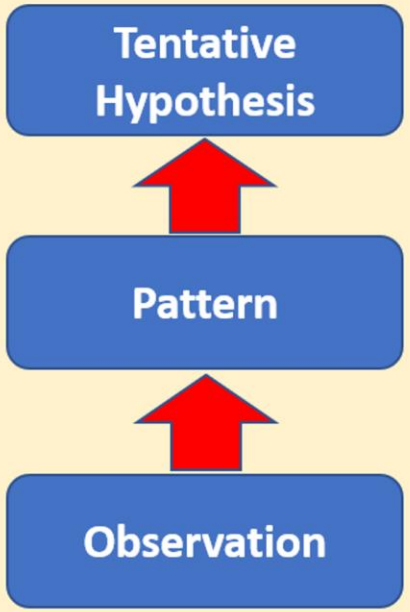
**Deductive Reasoning Top-Down Approach General to Specific**




**Knowledge Graphs**

**Property Graphs**




An **expert system** is an A.I. system focuses on **machine understanding** that emulates the sense-making and decision-making ability of a human expert. Expert systems are designed to solve complex problems by understanding and reasoning about knowledge. **Deductive Reasoning** uses facts, rules, definitions or properties to arrive at a conclusion.

**Inductive Reasoning Bottom-Up Approach Specific to Generalization**

**Machine Learning Predictive Analytics Scoring Engines**

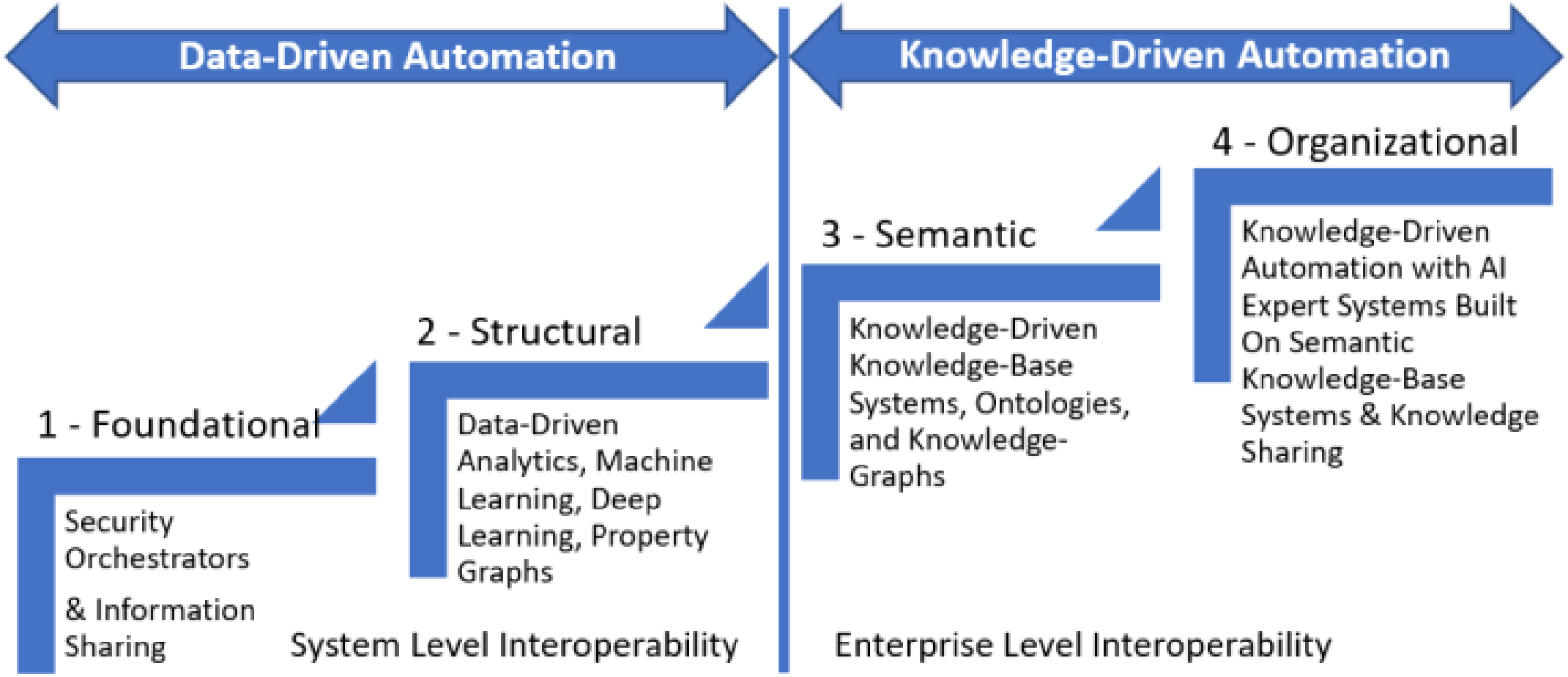
# KR&R Supports FAIR Data Principles


≠

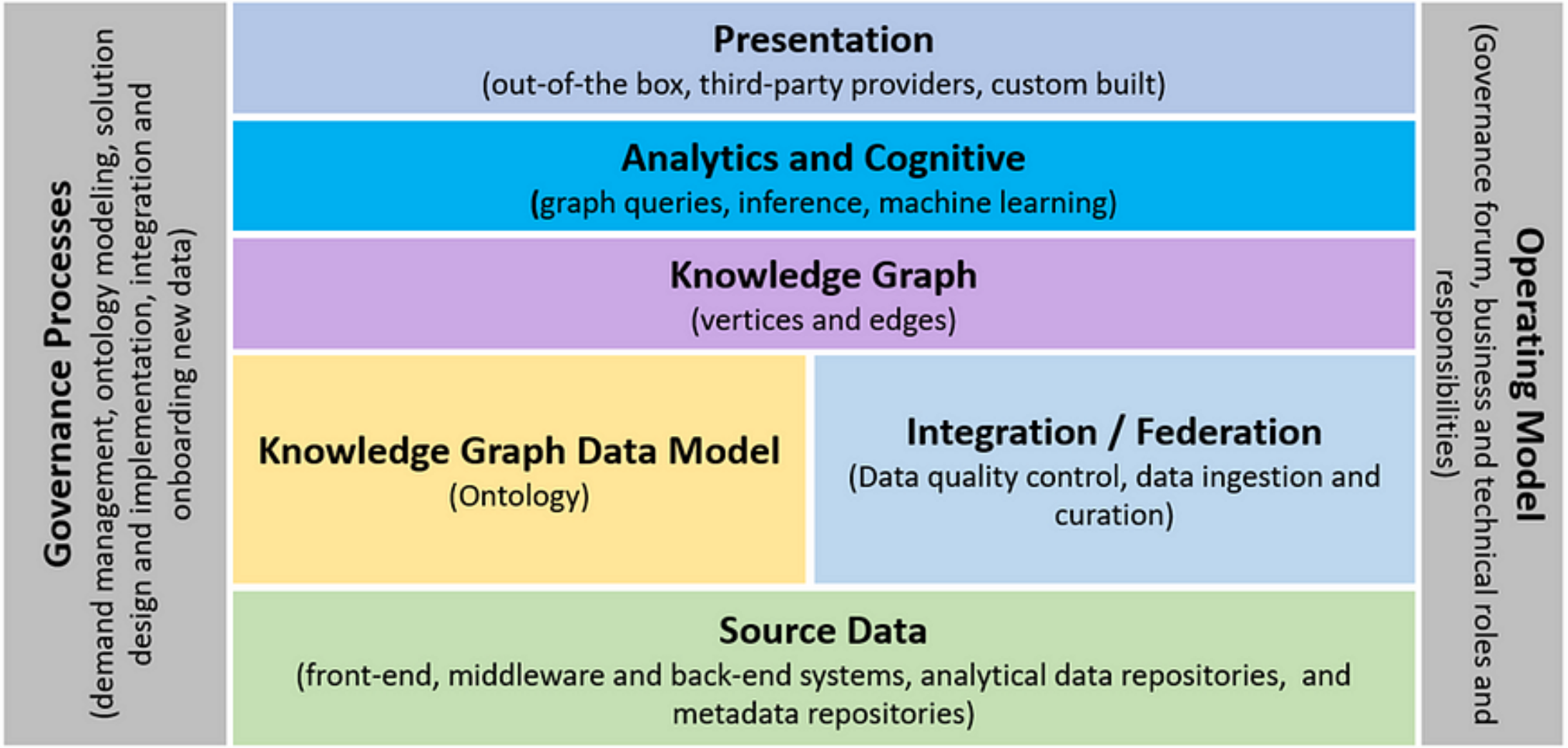
Open

https://www.go-fair.org/fair-principles/

# 4 Levels of Interoperability

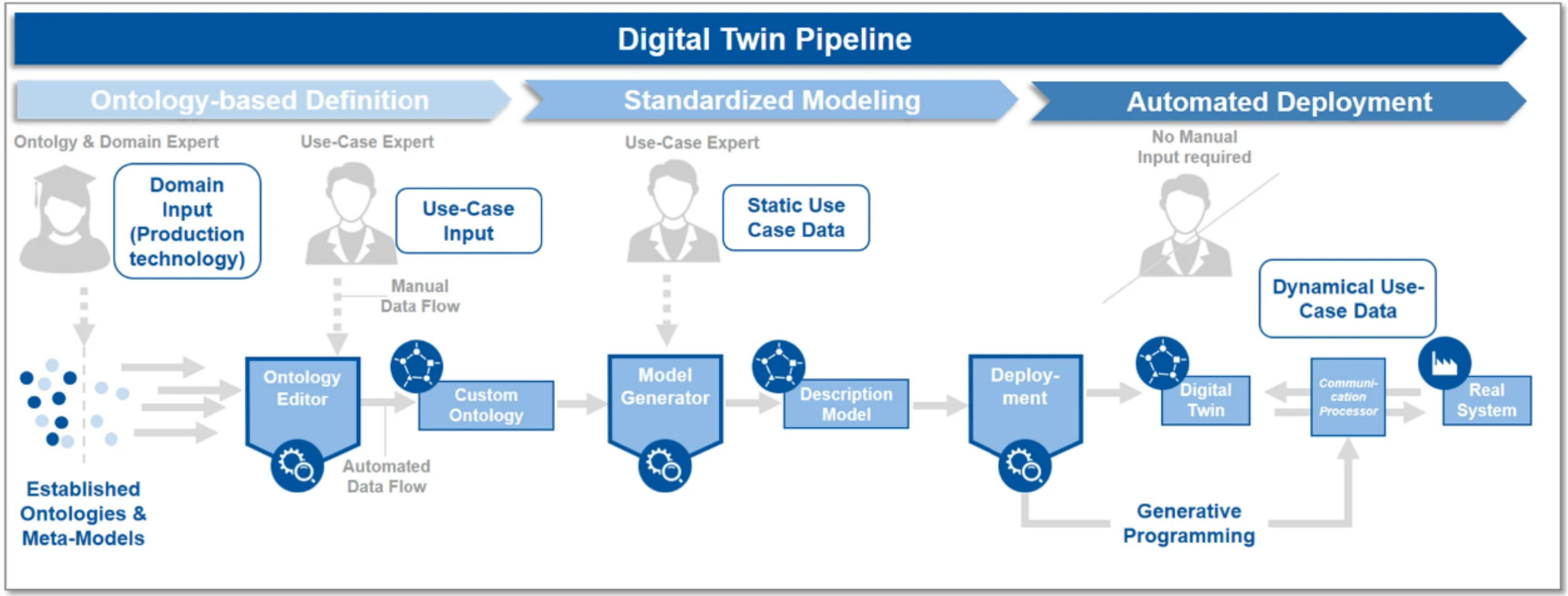


# We Need Cybersecurity Data Fabrics w/KR&R



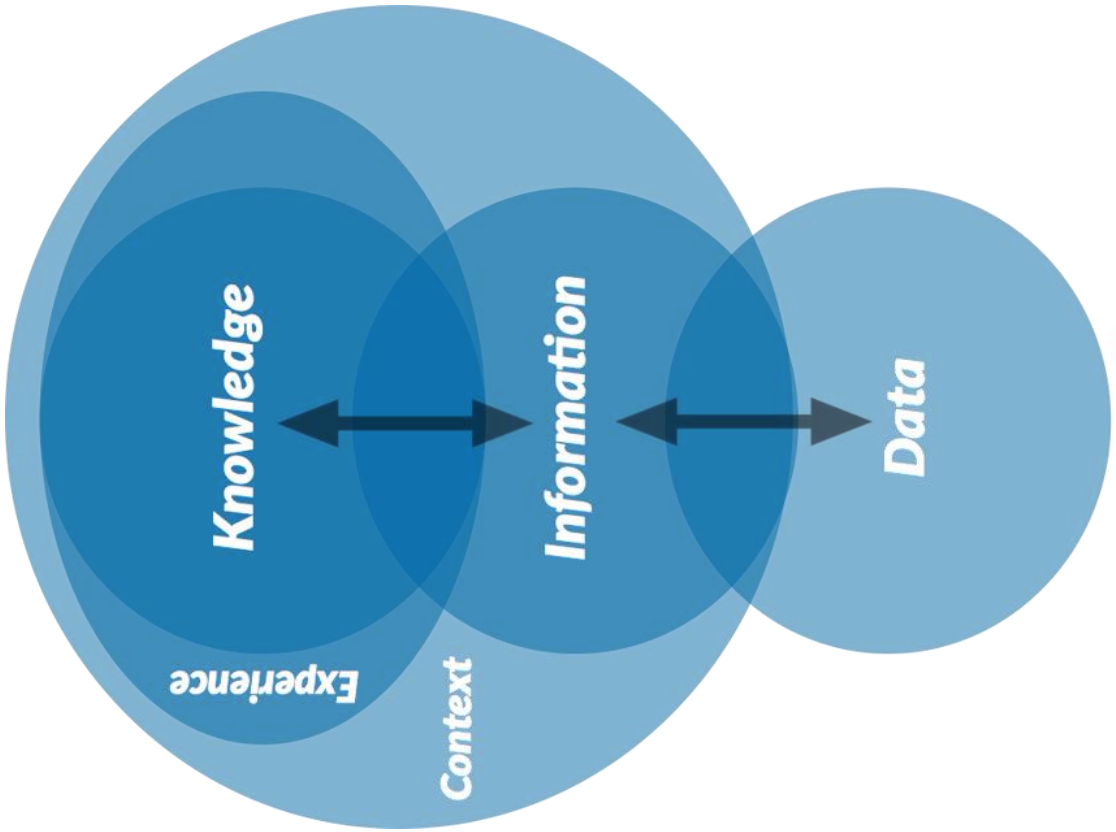

https://medium.com/the-future-of-data/the-perfect-data-architecture-data-mesh-data-fabric-or-something-in-between-15df778048c3

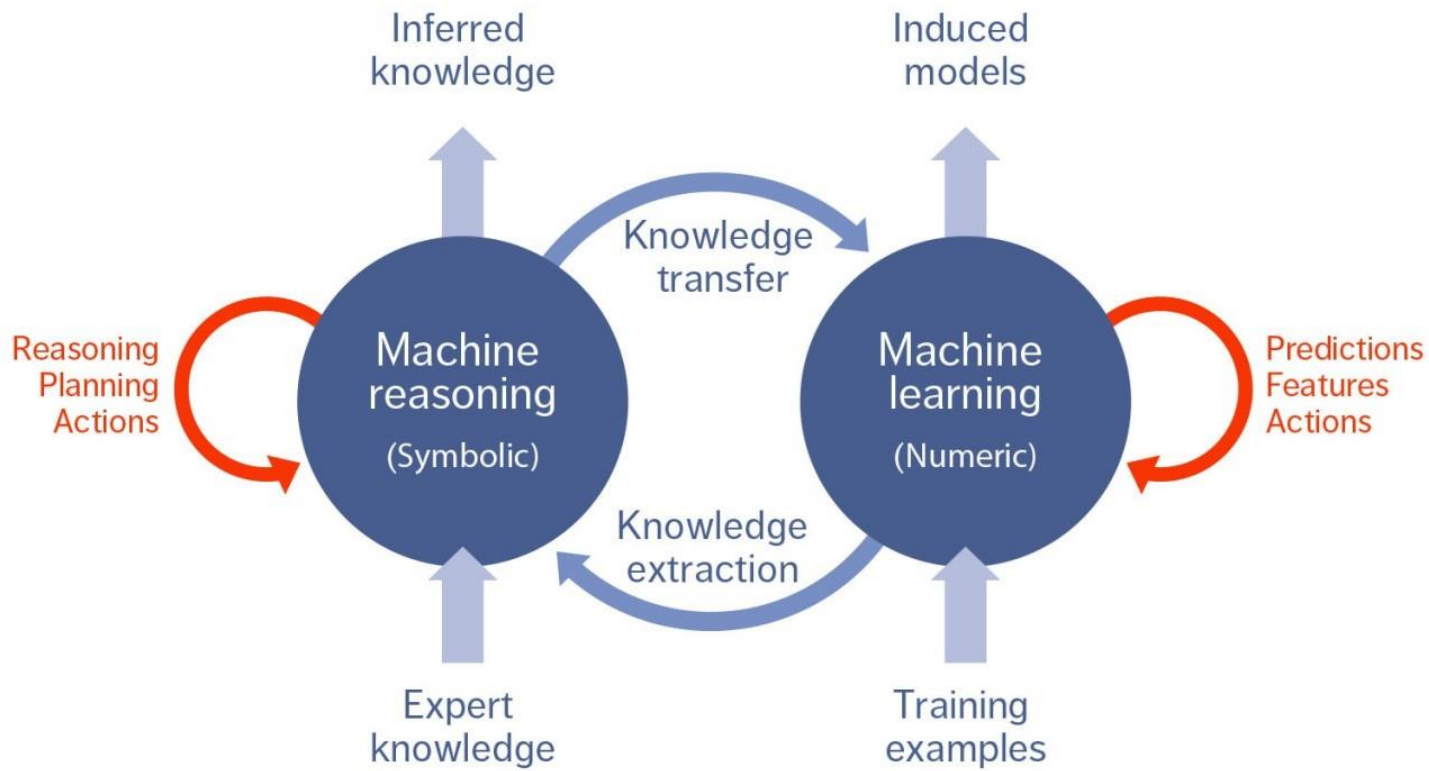
# We Need Cybersecurity Digital Twins w/KR&R



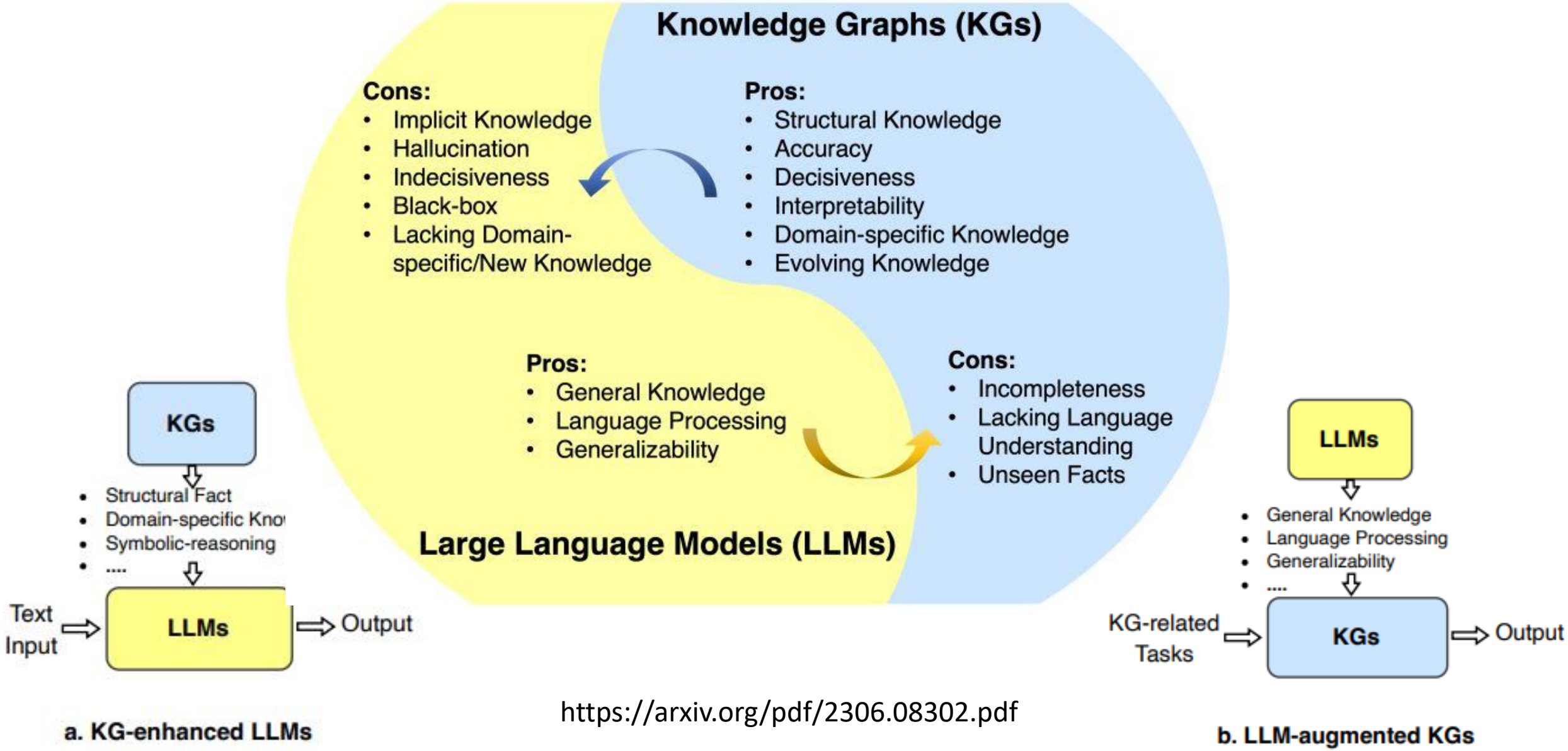

Three phases of the end-to-end digital twin pipeline for the application in cyber-physical systems

https://www.researchgate.net/publication/356291687_Pipeline_for_ontology-based_modeling_and_automated_deployment_of_digital_twins_for_planning_and_control_of_manufacturing_systems


Knowledge
Information
Data
Experience
Context

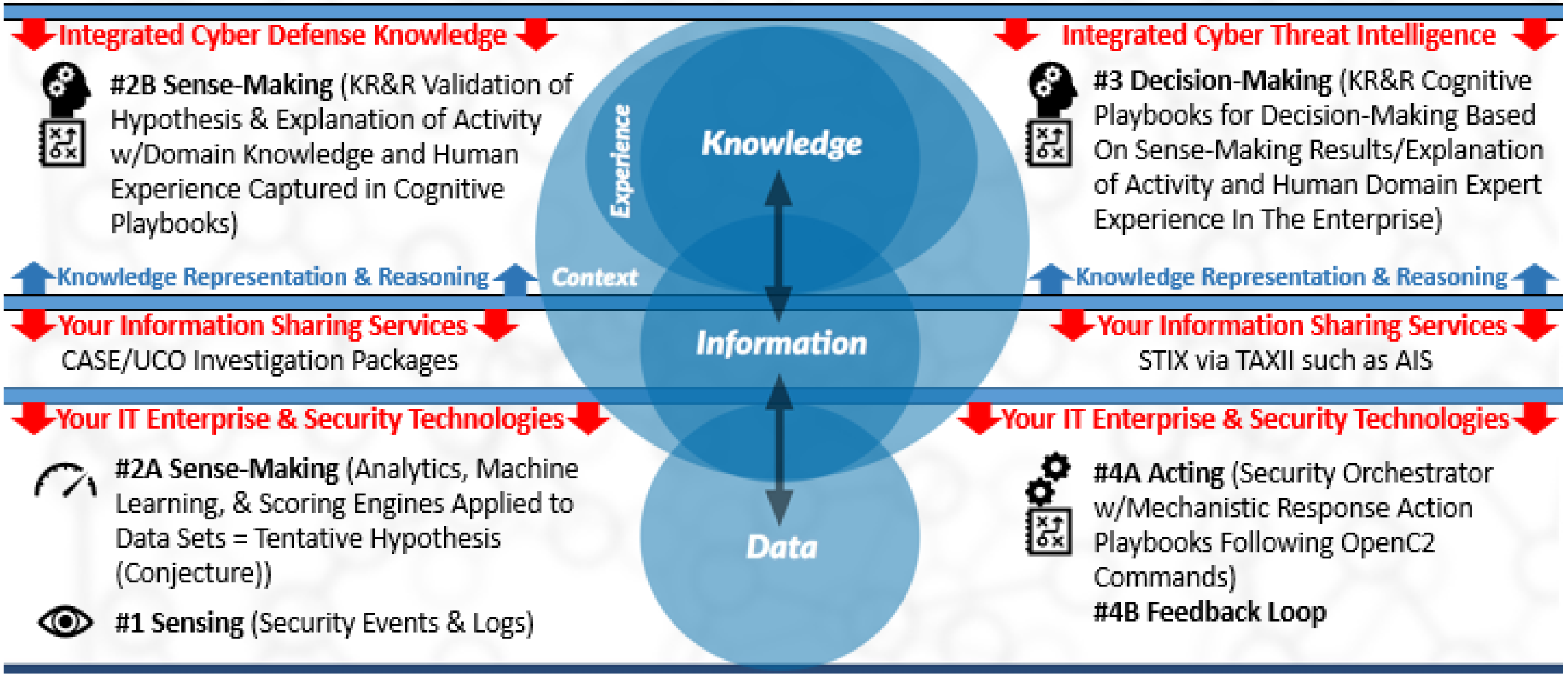

Inferred knowledge
Induced models
Knowledge transfer
Reasoning
Planning
Actions
Machine reasoning
(Symbolic)
Machine learning
(Numeric)
Predictions
Features
Actions
Knowledge extraction
Expert knowledge
Training examples

# We Need Cybersecurity Hybrid LLMs w/KR&R




https://arxiv.org/pdf/2306.08302.pdf

# AI-Driven Integrated Adaptive Cyber Defense Overview



# W3C Working on Updates to RDF & SPARQL

The W3C published the first (mostly skeletal) documents for the RDF 1.2 and SPARQL 1.2 Working groups. Little new has been added yet and a quick survey indicates that much of what does exist has primarily been imported from 1.1, but the very fact that this working group has been established is important in that it indicates that the W3C is actively working on an upgrade, not just tinkering around the edges.

# Questions