Estonian Data Protection Association (EDPA)

II conference

Future of privacy, data protection and cybersecurity

Tallinn, November 14, 2024

Future threats to privacy, data protection and cybersecurity

Elisabetta Zuanelli

Coordinator of the National Partnership for education & training in Cybersecurity, Cyberthreat,Privacy (www.cybersecurityprivacy.it)

UN and NATO expert in Artificial intelligence

Future threats in digital technology

- The governance of technological government by high tech giants
- Data protection security as disrupted by quantum and AI
- The increasing mandate of human activities to digital technologies
- The cloud vulnerabilities
- Internet and data vulnerabilities: post Quantum AI
- The satellite vulnerabilities and the space competition
- Cyber competition and Cyberwarfare

The context: questions about norms

1.What is data protection in GDPR: Articles 1 and 3 of the GDPR. The question implies typology of data, personal data and systems data: **data modeling in workflows**

2. Customisation of answers depends on users: military, financial, health, mobility, utilities, nuclear, etc.

3. Critical infrastructures and essential services: responsibility of vendors and consultants as related to compliance

No security standards for data management. **Web security standards in encrytption will be disrupted by quantum technologies**: quantum communication, quantum computing and storage.

A specific question is: **the relation between western and eastern communication security standards and authorities**

They are different and security is generally guaranteed by high tech vendors.

GDPR, NIS 2, AI Act

Vagueness-indeterminacy of language drafting: adequate? and proportionate? (GDPR/NIS)

Redefinition of workflows (GDPR): very expensive (SCADA)

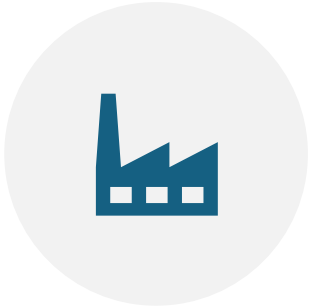
Personal data vs personal data: the ambiguity of protection (Articles 1 and 3 GDPR)

Definition and compliances of essential services: diversity in the different states (NIS, NIS 2, AI)

Responsibilities and notifications: cybersecurity vendors ? (coreferents and DPO)

The AI ACT

POOR DEFINITION OF AI



RISKS AND TYPOLOGY OF COMPANIES

RESPONSIBILITIES: VENDORS AND INTERMEDIARIES

IMPACTS ACCORDING TO DOMAINS

The UN concern the Common Regulation Agreement (CRA)

WP.6 for the November 2023 Annual Session,
"The regulatory compliance of products with **embedded artificial intelligence or other digital technologies**"
(ECE/CTCS/WP.6/2023/9)

Compliances (for instance the ISO 42001)

The typology of risks and the classification of companies

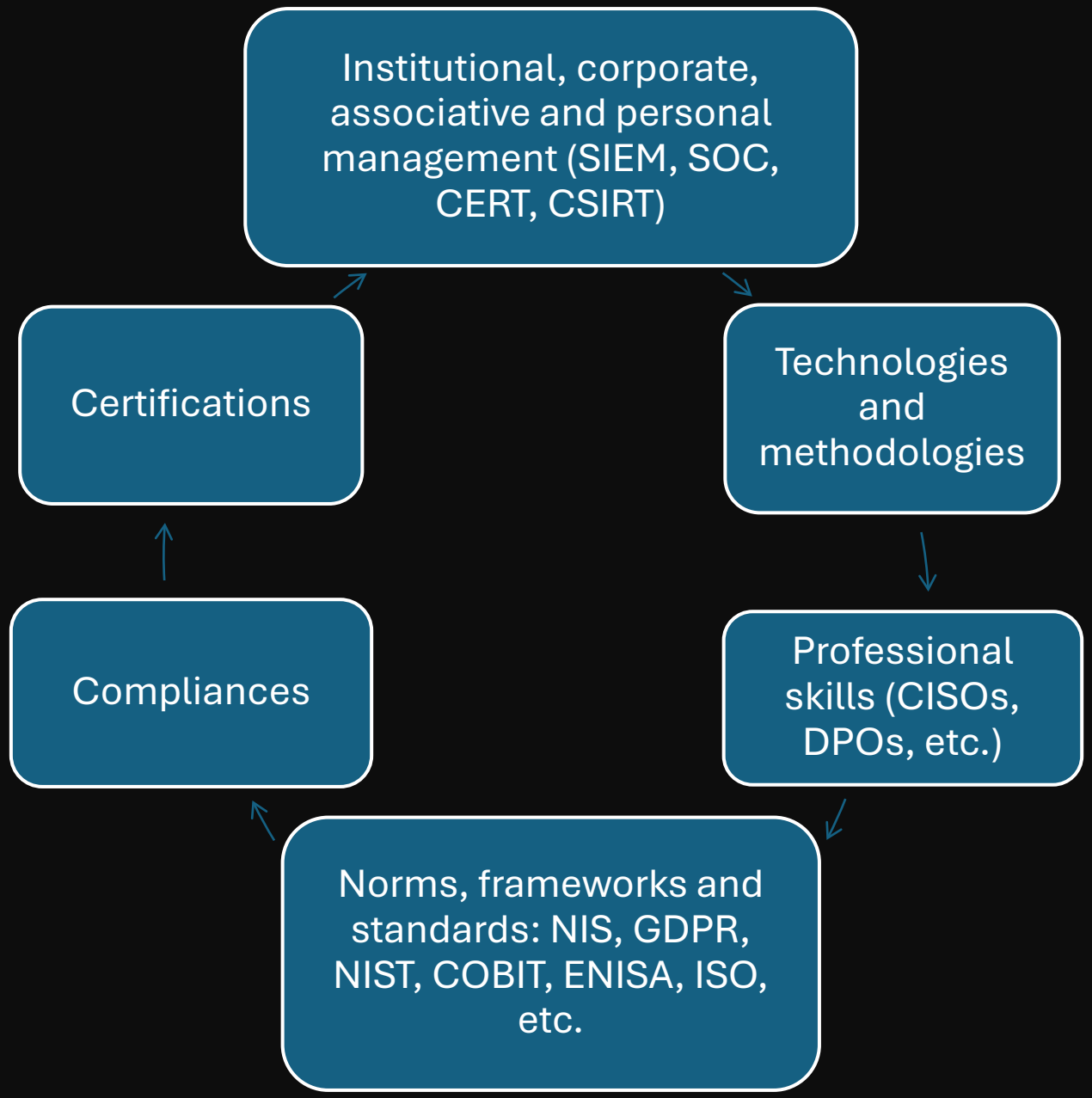
Questions? Evaluators???

Who checks

What do you check

How do you check

Data and the protection defense system



Lights

GLOBALIZATION OF THE PROBLEM

COORDINATED APPROACHES

LAUNCH OF COMMUNICATION AND AWARENESS ACTIVITIES

EMPLOYEES TRAINING

DETERRENCE OF REGULATIONS

Shadows

Difficult operational coordination of CERTs, CSIRTs and national and international agencies, public and private

Modest investment by Institutions and Companies in security

Unprecedented professional skills in a disciplinary and interdisciplinary key

Chaotic data sharing languages and solutions

Certification difficulties

Poor integration and comparison of system operators

Cyber defense of data technology solutions: detection and prevention

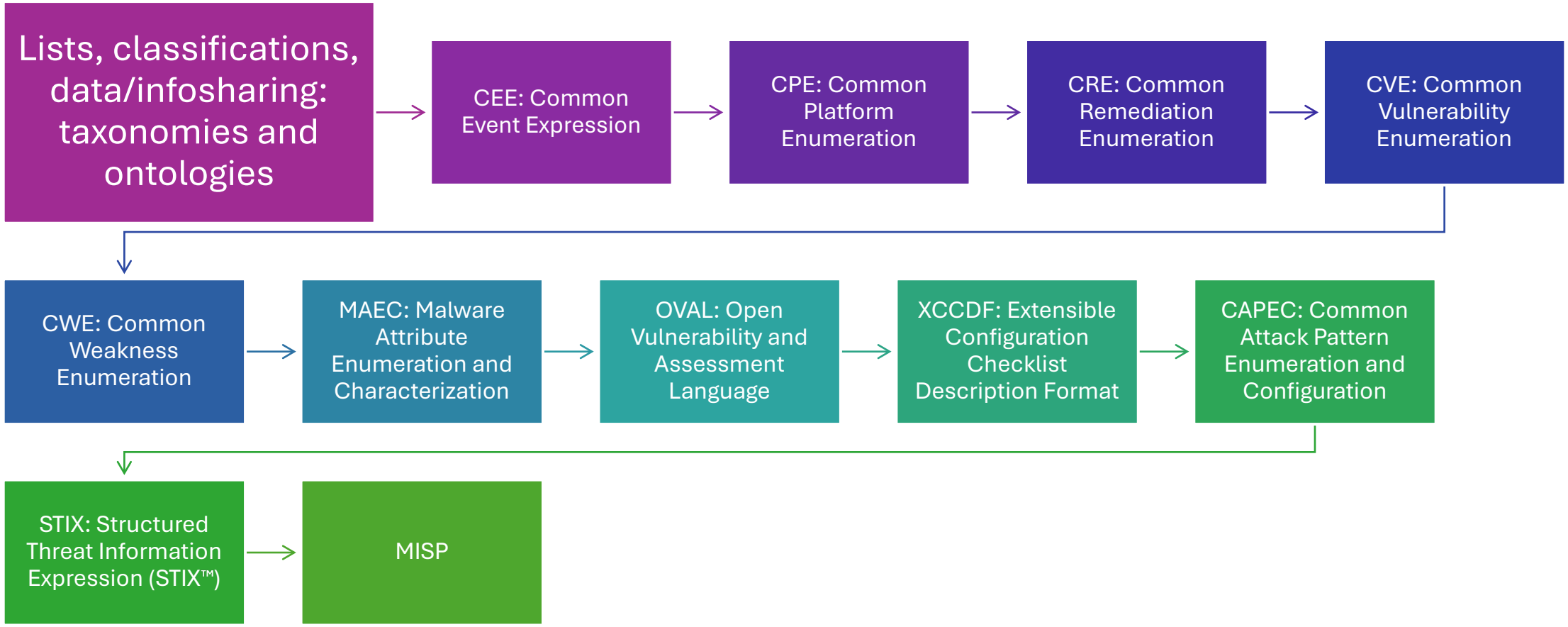
Typologies of defenses

network, OS, apps, behavioral governance

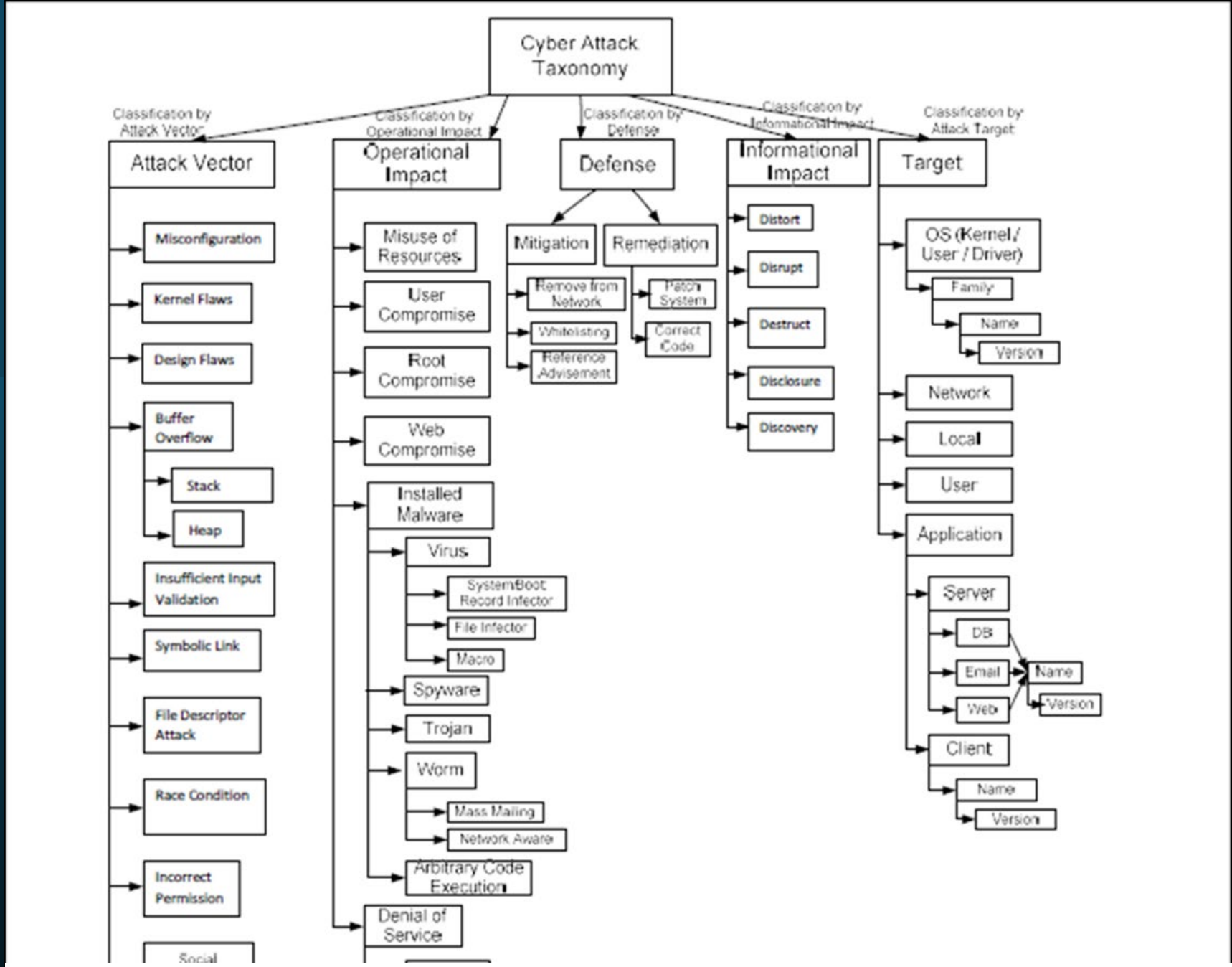
Typology of devices

- asset monitoring
- IDS
- IPS
- firewall
- antimalware
- antivirus
- antispam
- honeypot
- pen testing

Threat intelligence and infosharing platforms



AVOIDIT: an attack taxonomy



ENISA
A sample: the resilience ontology

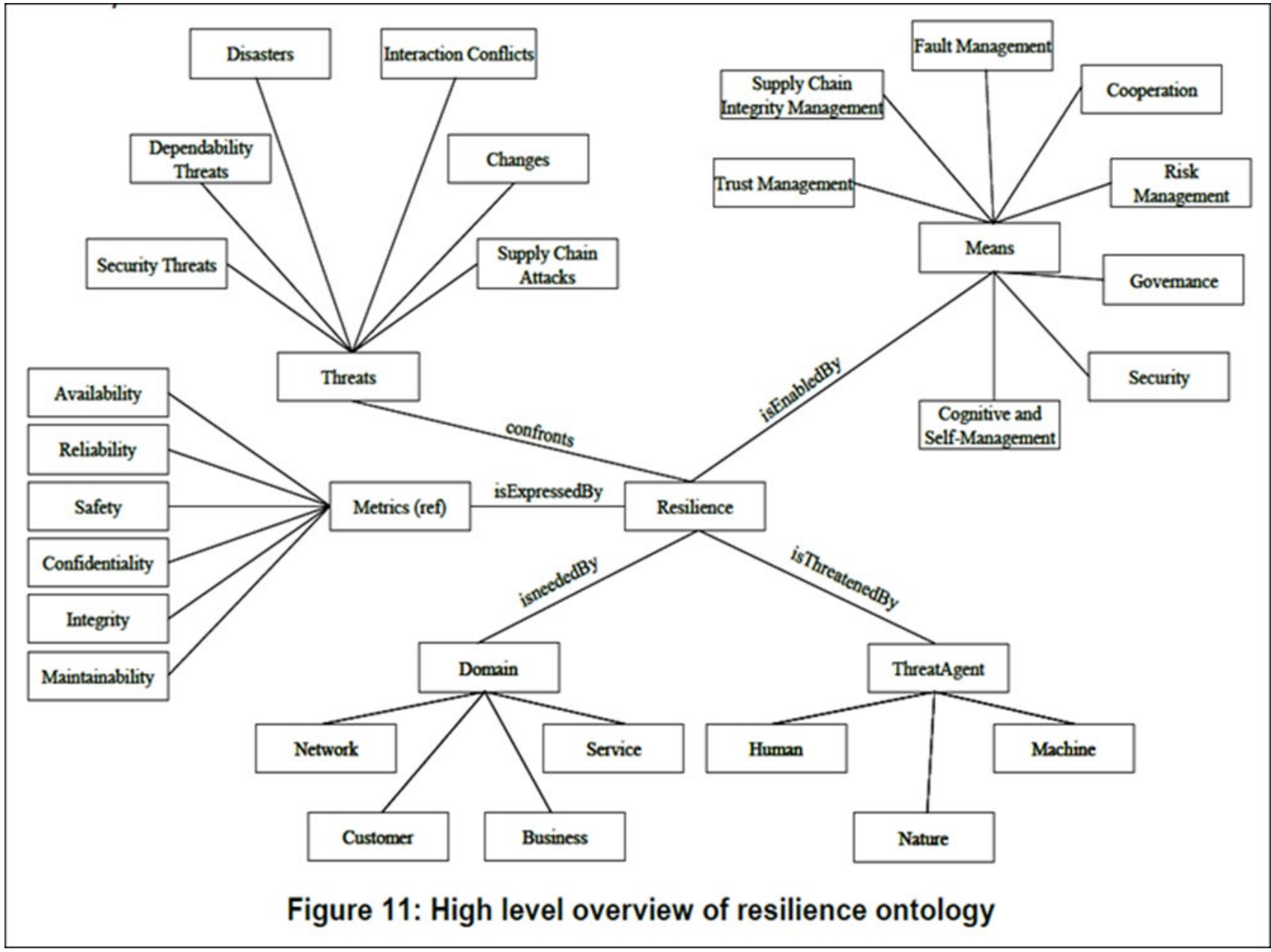


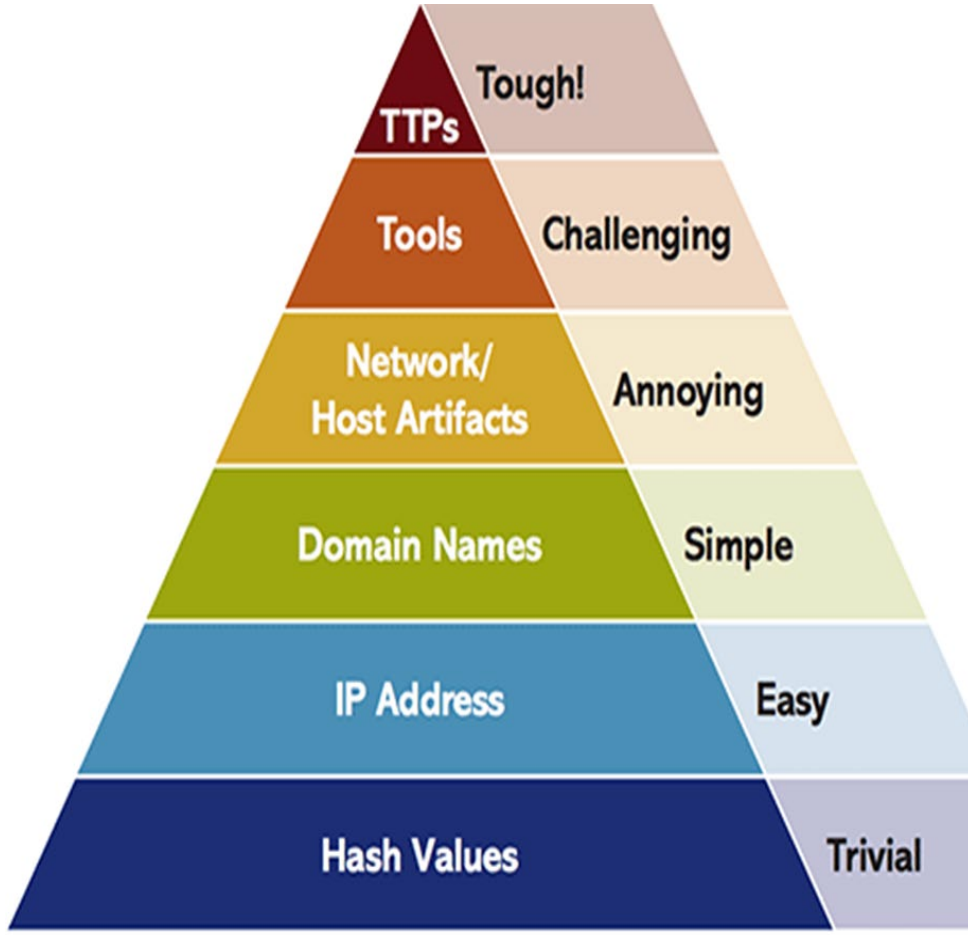
Figure 11: High level overview of resilience ontology

IoCs IoAs: data analytics, integration, representation

DATA and IoCs: the Pyramid of Pain

David Bianco

http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html



State of the art of cyber defense: problems

- overlapping of technologies and unrelated data
- necessity and limits of manual interventions
- contradictory and arbitrary detections of indicators and attacks
- lack of contextualization of generalizable data/IoCs
- lack of AI analytics and classifications: ontologies and taxonomies
- absence of logical-semantic relationships in classifiers
- arbitrary conceptualization and naming of taxonomic and ontological entities
- precariousness of algorithms due to theoretical insufficiency of data sets modelling
- undue trust in the ability of the machine to learn data on incorrect logical-semantic relationships
- need for specific R&D on AI modeling and data correlation: neural networks and models
- preventive and predictive helplessness

Quantum/AI attacks

Quantum /AI defense

the double bind

encryption algorithms disruption

vs

advanced encryption algorithms for communication and storage

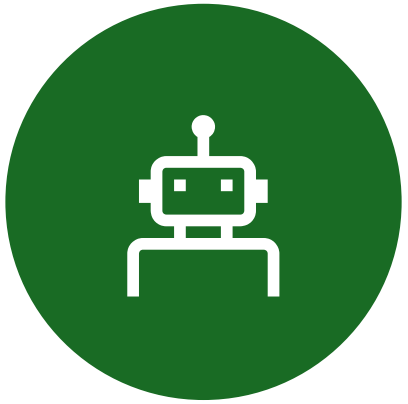
AI adversarial attacks

vs

preventive and predictive AI platforms

AI, cybersecurity, data protection: the triple perspective

KNOWLEDGE ARCHITECTURES KNOWLEDGE BASES FOR DEFENSE SYSTEMS



THE AI KNOWLEDGE BASES INSECURITY

AI ADVERSARIAL ATTACKS

AI development activities, approaches, modeling

- Neural, cognitive and linguistic approaches

CHAT GPT 4: (transformer attentive models) NLP, data base/ knowledge base, linguistic processing and services: extraction, composition, information queries, multimodal production (generative), etc.

- Deep neural network machine learning: Gitta Kutyniok on mathematical foundational support and criticism for data architectures
- Ontologies and taxonomies: def and methods

  Guarino, MITRE, Protégés/Stanford University
- POC Cybersecurity defense systems
- Mixed/blended languages

LLM/image recognition: labelled images e polisemy of images (Google image analytics)

Large multimodal systems (LMM)

- Quality and typology of images
- Images and texts:

the logical semantc correlation: the vectorial representation (embedding) of images as compatible with the vectorial phrase representation

- Machine learning, data sets

The AI concepts methodology

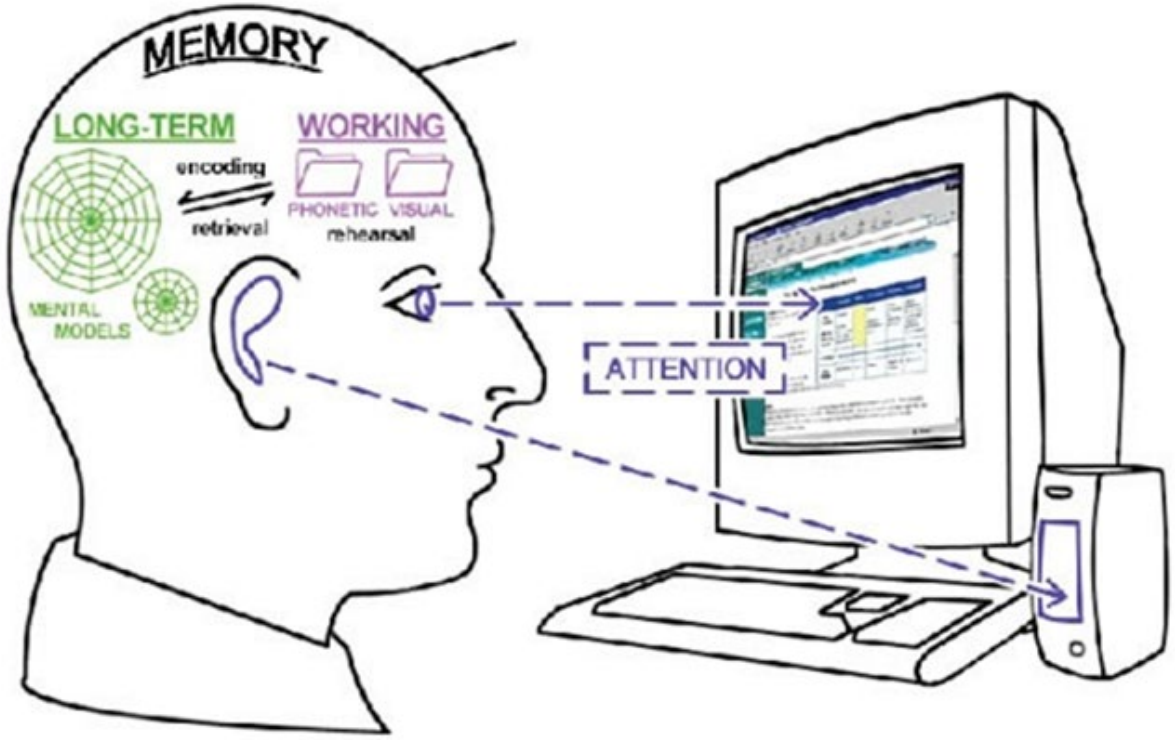
The architectural profile

- Domains, classes, entities, logical-semantic relations, controlled semantic vocabularies, metadata languages
- Advanced machine learning

Gitta Kutyniok “a comprehensive theoretical mathematical foundation in AI is completely lacking at present”

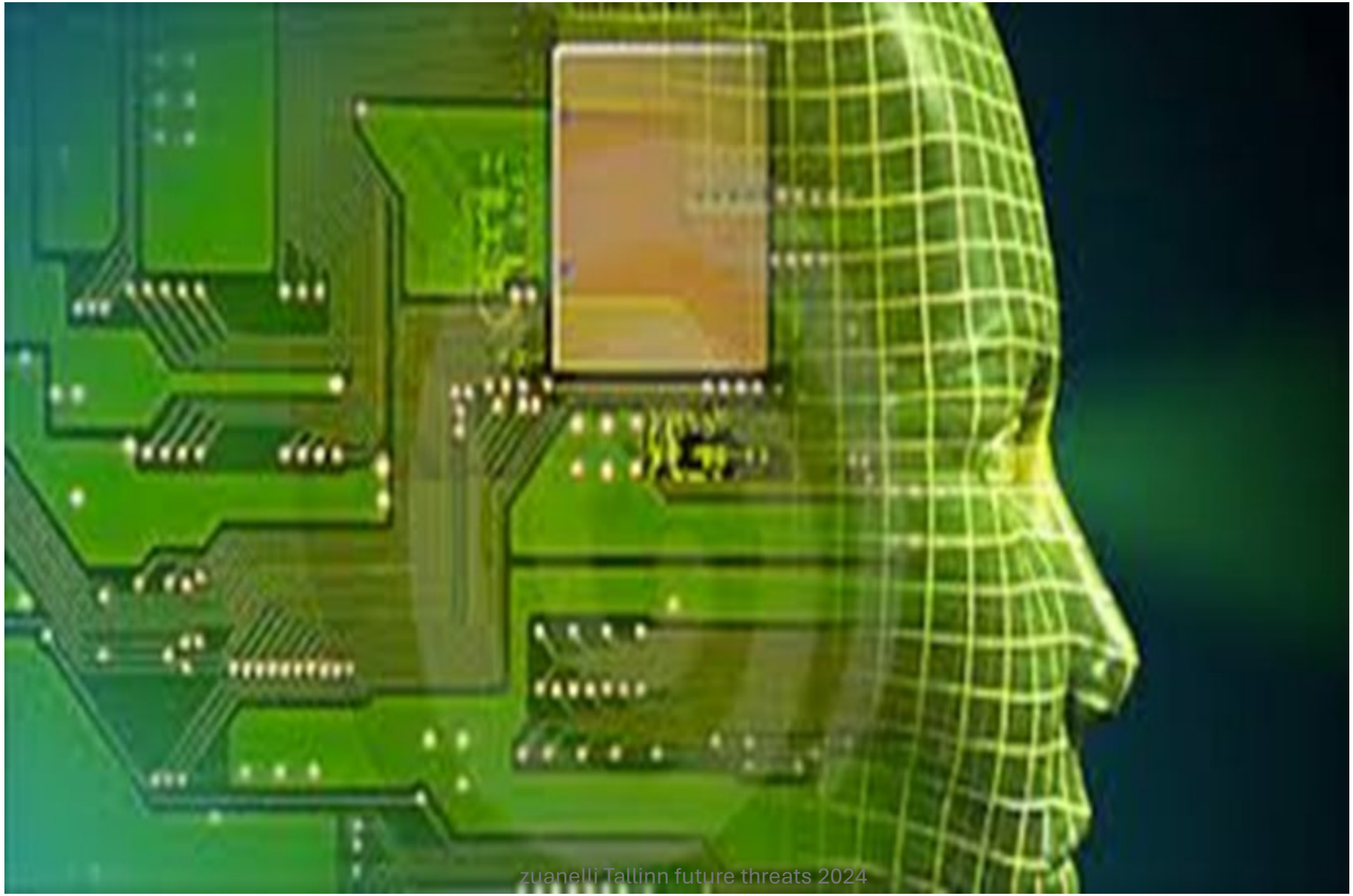
- In AI, …, in the case of deep neural networks, “the search results is a timeconsuming work for a suitable network architecture,
- a highly delicate trial-and-error-based (training) process,
- and missing error bounds for the performance of the trained neural networks”.
- Layers, data sets (numerical, bivariate, multivariate, categorical, correlational, etc.), architectures: criteria for typological coherence of collected data and knowledge base architectures

Cognitive functions and mind: the great engine of human activities



- perception
- analysis
- transduction
- integration/memorization
- elaboration
- retrieval
- applications

Cognitive architecture: from mind to machine

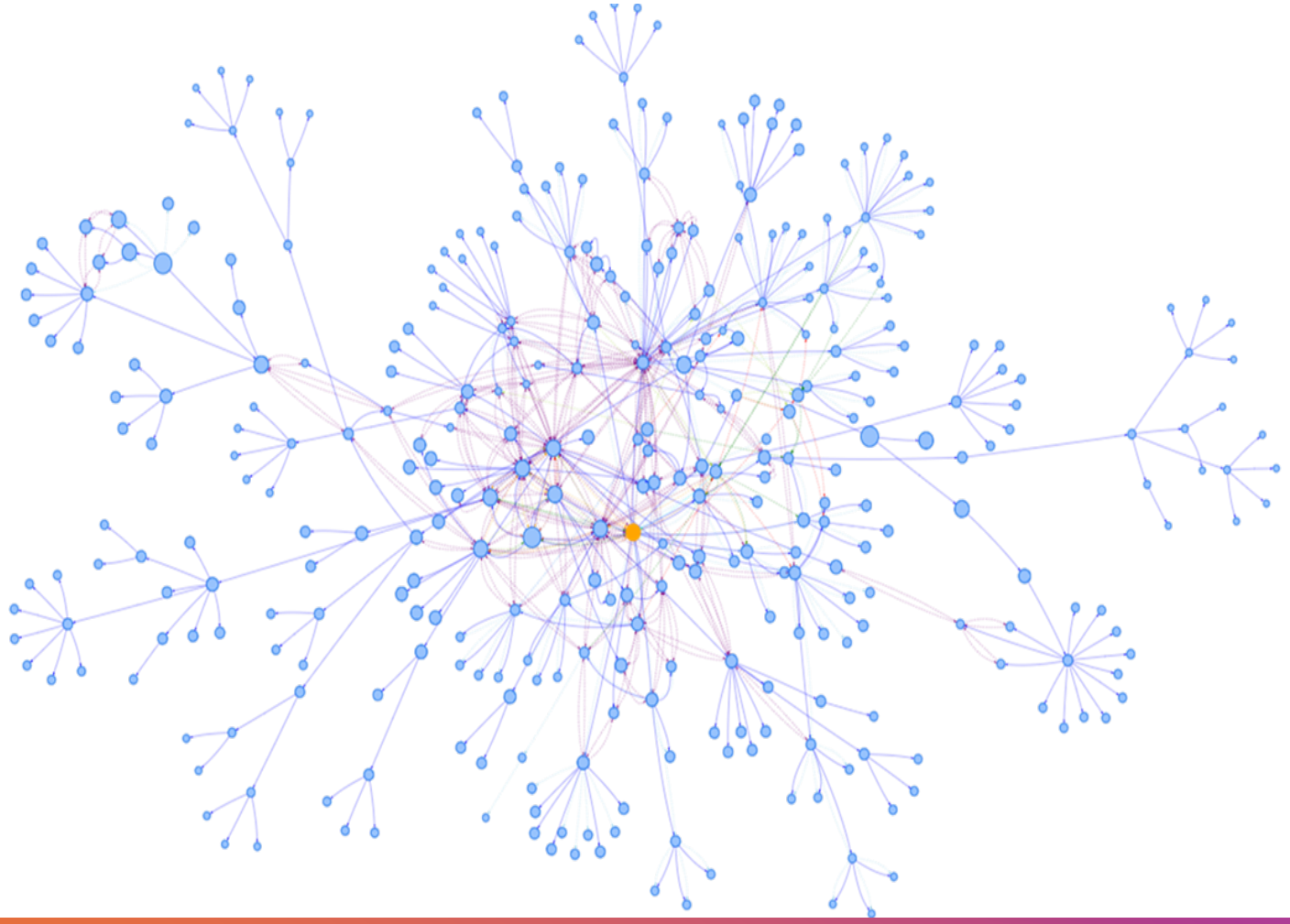


The POC ontology defense solution: threat intelligence, information sharing, incident reporting (2024) Pragmema

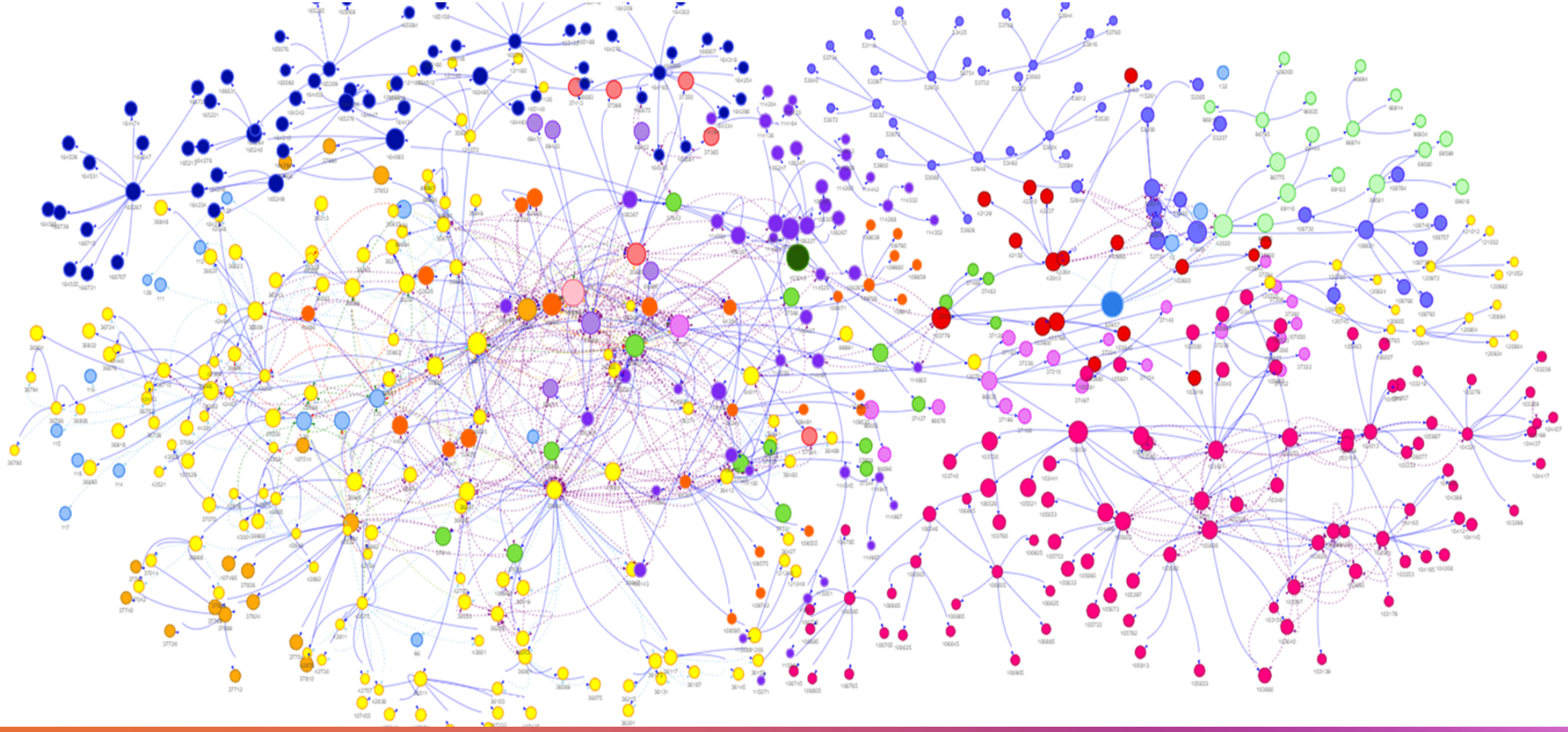
POC knowledge ontology

POC cybersecurity domain ontology: prevention and prediction

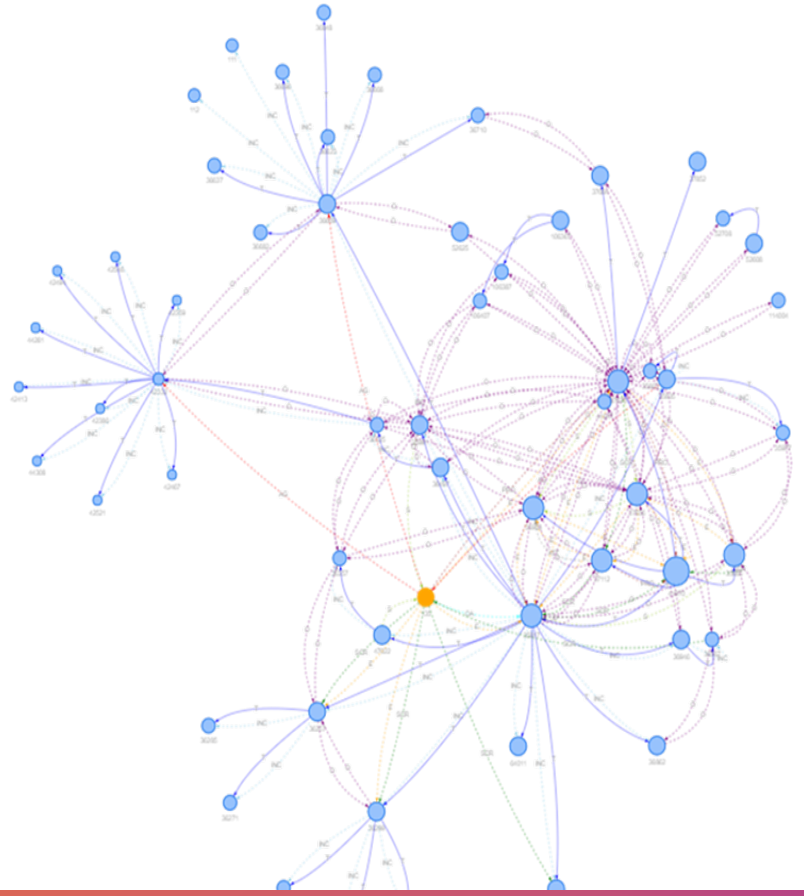
POC cybersecurity pragmatic ontology: services



POC knowledge ontology



POC Cybersecurity domain ontology

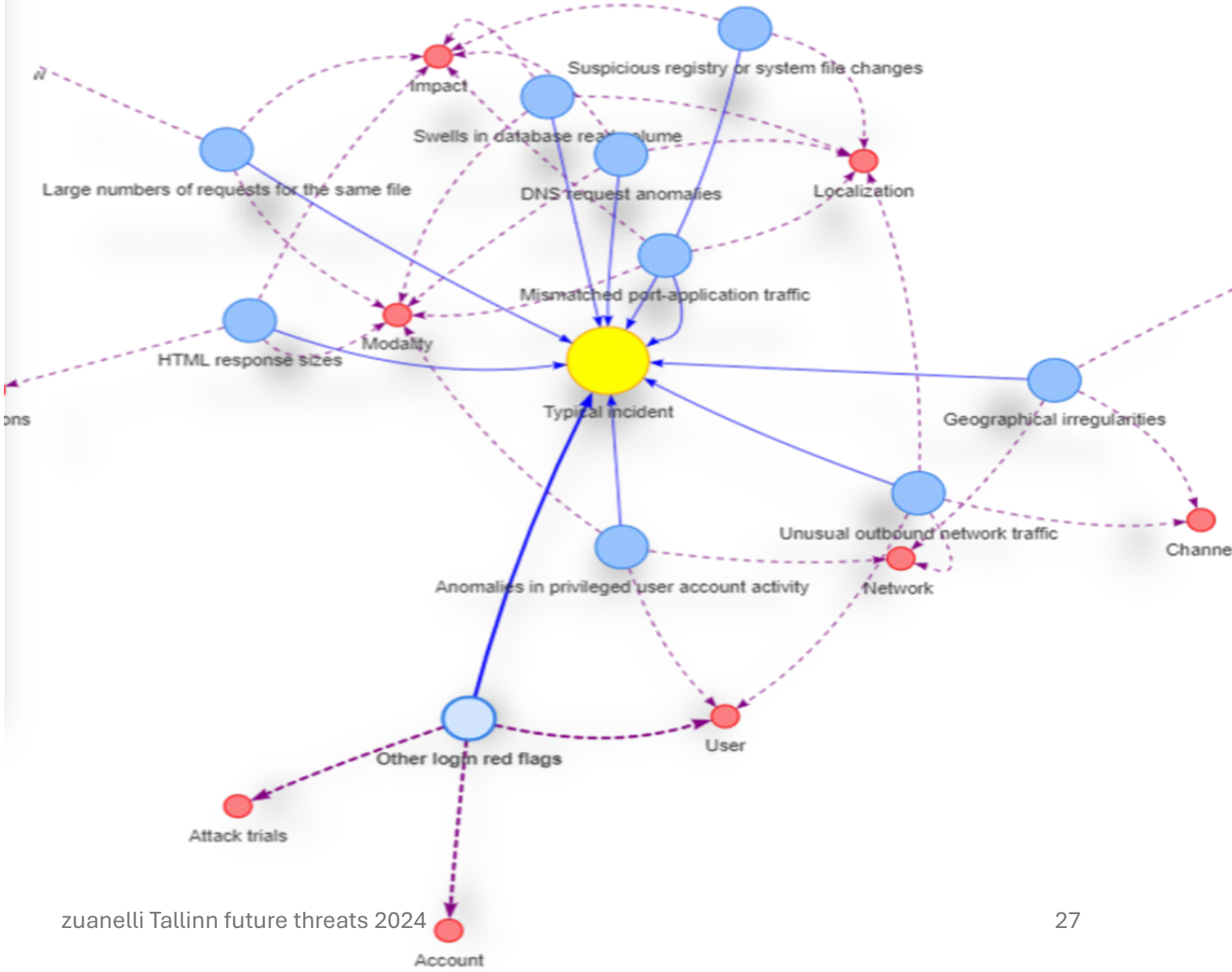


POC typical incident

POC: typical incident

IoC Integration and filter

Parameters clustering



Normative extraction and summarization KBs

- usefulness
- feasability
- productive/ applicative functions
- the ontology of digital norms: extraction, summarization, comparison

Knowledge bases for detection and prevention of data breaches

- typology of data
- customised analyses of domains (finance, healt utilities, nuclear, etc.) users and workflows
- normative domains ontology: entities, classes, logical semantic relations
- technological adequacy of data protection syste
- users training
- R&D

The knowledge workers

THE UNLIMITED POWER OF AI: COLLABORATION WITH HUMAN ACTIVITIES

THANKS!