ASREN
e-Age 18
Amman, Jordan
2-3 December 2018

"Cybersecurity as a service: standards and tools for risk assessment and evaluation"

Elisabetta Zuanelli

University of Rome "Tor Vergata"

President of CreSEC (www.cresec.com)

National Coordinator of the " Education and Training Plan for Cybersecurity, Cyberthreat, Privacy"(www.cybersecurityprivacy.it)

Pragmema srl (www.pragmema.it)

The state of the art

- The overwhelming **increase of cyberattacks** in all fields of Internet interactions: cloud, ecommerce, IoT, search engines, apps for mobile,etc.
- Among other domains, a growth of 138% in the domain of online research and education in the first semester 2017.

Cybersecurity as a service: a framework

- A **framework** for the interpretation of the **global cybersecurity challenges** dealing with vulnerabilities and threats, on one side.
- On the other, **the definition of proper standards and tools for prevention, detection and resiliation** of cyberattacks by defining a new approach to cybersecurity.
- **Cybersecurity as a service** is here meant as a **multifaceted protection design** in the technological approach and development of online services in the cyberspace context.

The approach

- Cybersecurity as a service asks for a **brand new design and implementation of Internet infrastructures and services** to be required of vendors on one side for asset technologies supplied to clients.
- On the other, cybersecurity as a service implies **the capability of companies and institutions to manage cyber risks and perform assessment and evaluation according to structured analytics parameters that can manage conspicuous amounts of data**.

Stakeholders and cyber security market size

The global Cyber Security market size was estimated to grow from $106.32 Billion in 2015 to $170.21 Billion by 2020, at a Compound Annual Growth Rate (CAGR) of 9.8%

- **Stakeholders:**
- Cyber security vendors
- Networking solution providers
- Independent Software Vendors (ISVs)
- Software vendors
- System integrators
- Value-added resellers
- Service providers and distributors
- Research organizations
- IT security agencies
- Suppliers, distributors, and contractors
- Consulting companies
- Cloud Business Intelligence (BI) platform vendors/cloud infrastructure providers

- Investors and venture capitalists

The submarkets

Security Types:

- Network security
- Endpoint security
- Application security
- Content security
- Wireless security
- Cloud security

By Service:

- Consulting
- Design and integration
- Risk and threat assessment
- Managed security services
- Training and education

By Vertical:

- Aerospace, defenseand intelligence
- Government (excluding defense) and public utilities
- Banking, Financial Services, and Insurance (BFSI)
- Telecommunication
- Healthcare
- Retail
- Manufacturing

ENISA NIS 2017: the modus operandi

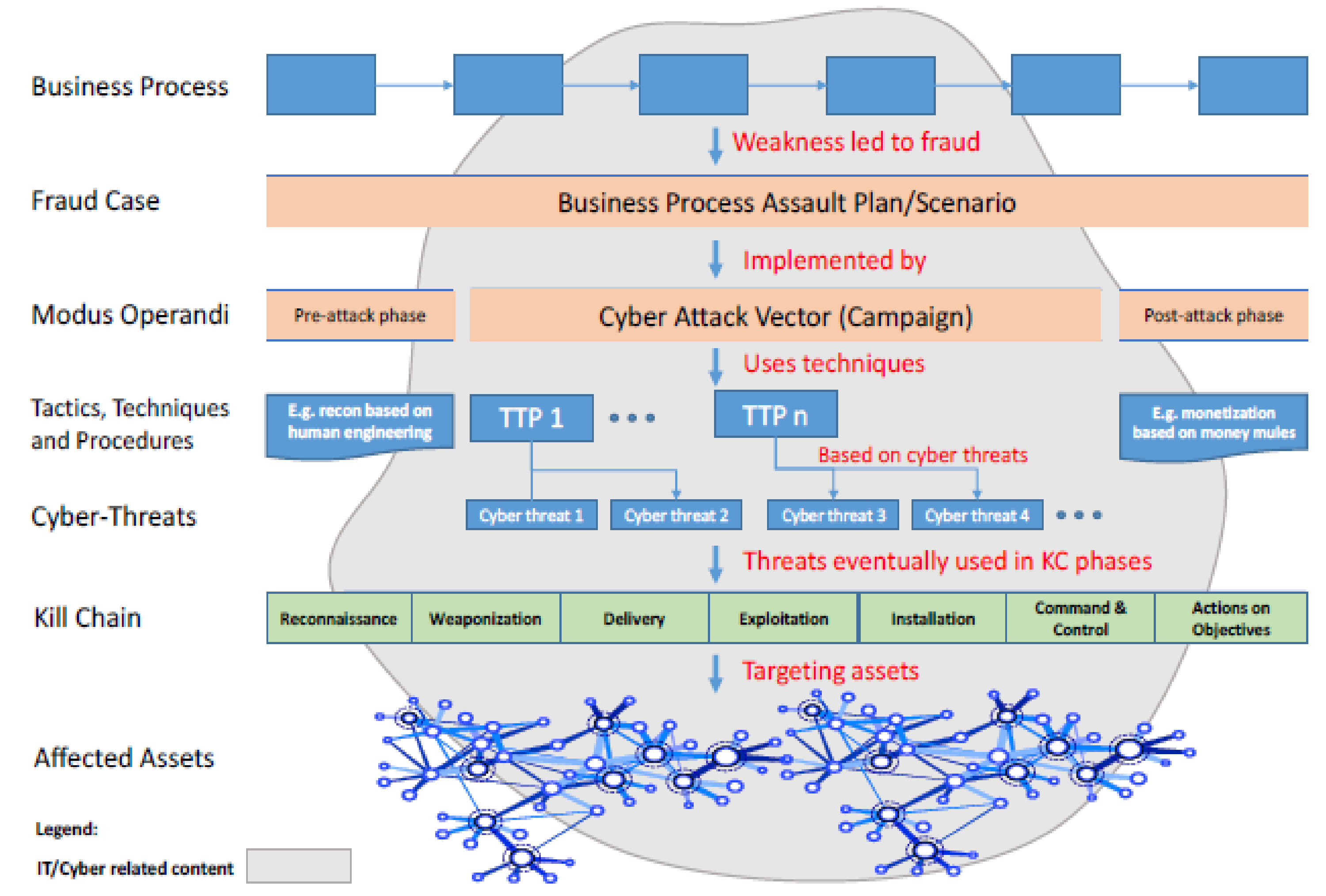


Figure 2: Big picture CTI elements from Modus Operandi to affected assets

Typology of logical impact

- Espionage (political, institutional, industrial, commercial, etc.)
- Data exfiltration
- Data destruction
- Data manipulation
- Denial of service
- Data encryption

Cybersecurity by defense

- Knowledge representation and info-sharing
- Resilience
- Technological solutions (detection, removal, alarm, etc.): prevention and prediction

- Human interventions (CERTs, CSIRTs, CIRTs, SIEM, SOC)
- Legislation
- Education and training: awareness
- R&D
- Public private partnerships

- Cybersecurity diplomacy
- Cybersecurity by design
- **Cybersecurity as a service**

- **Big data analytics**
- **AI applications: ontologies, taxonomies, data architectures**

The cybersecurity ecosystem and knowledge representation

- conceptual definitions and analyses of the cybersecurity domain and sub-domains: **prospective standards for cybersecurity digital knowledge representation** and **related tools**
- applications needed in **risk assessment** and **evaluation**: ISO, COBIT, NIST framework, etc.
- **quality/quantity metrics** for risk evaluation
- **standards and tools for cyber security analytics** and applications in defense and resilience:
  - taxonomies /ontologies
  - vulnerabilities/threats
  - semantic web metalanguages/logical semantic modeling

Ontologies and taxonomies: tools and standards

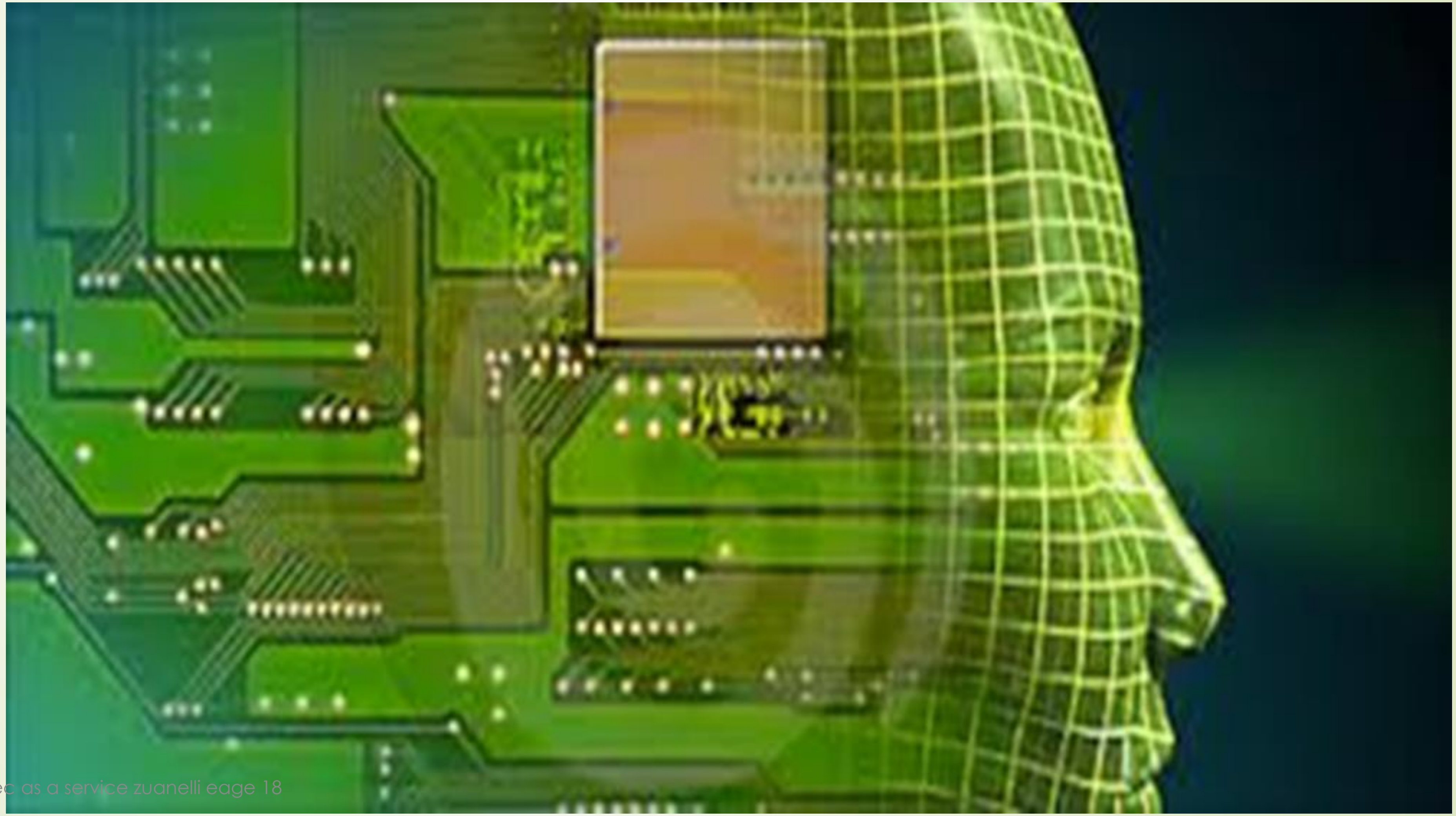
- Definition and approaches
- Top level, middle level, domain ontology, pragmatic ontology
- Conceptual specifications: metalanguages for technological interoperability and logical semantic relationships
- Domains and subdomains

N. Guarino (ed.), *Formal Ontology in Information Systems*, IOS Press, Amsterdam, 1998

- Some twenty years ago Guarino postulated the increasing relevance of ontology in the fields of **Artificial Intelligence, Computational Linguistics and Database Theory** and mentioned specific research fields such as **knowledge engineering**, **knowledge representation**, **qualitative modelling**, **language engineering**, **database design**, **information modelling and integration**, **object oriented analysis**, **information retrieval and extraction**, **knowledge management and organization**, **agent-based systems design**.

- At the methodological level he stressed the main peculiarity of an **ontology as its being a highly interdisciplinary approach where philosophy and linguistics play a fundamental role.**

The digital mind, artificial intelligence and big data architecture



Artificial intelligence and data

- Modeling of data and of logical semantic relationships
- Design and development of the model: data cluster, univocal definition of terminology, search functions
- Technological translation into the platform and data implementation
- Metadata languages
- Metadata applications
- Data representation formats

Cybersecurity ontology methodology: big data and AI technologies

- "Middle-out" approach: bottom-up and top-down sources, partially used and functionally redefined by the model and the technological development
- Upper ontology and mid-level ontology underlying the cybersecurity ontology as domain ontology
- Functional/pragmatic ontology as related development of the cybersecurity domain

Ontologies and taxonomies: conceptual and operative functions

- Ontologies: logical semantic systems of entities and relationships based on a high level definition as applied to the cybersecurity domain

  Best definitions are contextualized entities and relations

- Taxonomies: mainly hierarchical classes with single decontextualized entities

The Babel conceptualization: critical issues

- General vs domain and subdomain ontologies
- Ontologies and taxonomies relations
- Vocabulary standards
- Goals of description

General and domain sub-domain ontologies

Oltramari et alii 2014: **ontology of cybersecurity**/Dolce/Secco/Osco

Syed et alii 2016: UCO **a unified cybersecurity ontology** (semantic web languages and UCO)

Pragmema/Zuanelli 2017: the Poc **ontology platform** / 3level and pragmatic domain ontology)

Mavroeidis and Bromander 2017 : **cyber threat intelligence** comparison and model

Domain/sub-domain ontologies

Enisa 2011: Ontology and taxonomy of **resilience**

Bromander et alii 2017: **Semantic threat modeling** (threat agent/threat scenario)

Mavroeidis and Bromander 2017: **Cyber threat intelligence** model/Taxonomies, ontologies in cyberthreat intelligence

Nistir 2016: **Vulnerability ontology**

Silva and Rodriguez 2017: **Network ontology/Cyber threat intelligence** comparison and model

Taxonomies

- **Attack taxonomies**

Van Heeerden et alii 2015: attack taxonomy

- **Taxonomies in incident prevention and detection**

Enisa 2016

Enisa 2016: taxonomy/data classification

CERT.PT	CERT.BE	CESNET CERT	ECSIRT.NET MKII
Malware	Spam	Spam	Spam
Botnet Drone	Abusive Content	Bounce	Harassment
Ransomware	Malware	Virus	Child/Sexual/Violence/...
Malware Configuration	Scan	Malware	Virus
C&C	System/Account Compromised	Trojan	Trojan
DDoS	(D)DoS	Malware	Spyware
Scanner	Phishing	Probe	Dialler
Exploit	Vulnerability Report	Crack	Rootkit
Brute-force	Other	Botnet	Scanning
IDS alert		Dos	Sniffing
Defacement		Copyright	Social Engineering
Compromised		Scam	Exploiting of known Vulnerabilities
Backdoor		Phishing	Login attempts
Drop zone		Pharming	New attack signature
Phishing		Other	Privileged Account Compromise
SPAM		Unknown	Unprivileged Account Compromise
Vulnerability			Application Compromise
Service			Bot
Other			DoS

cybsec as a service zuanelli eage 18

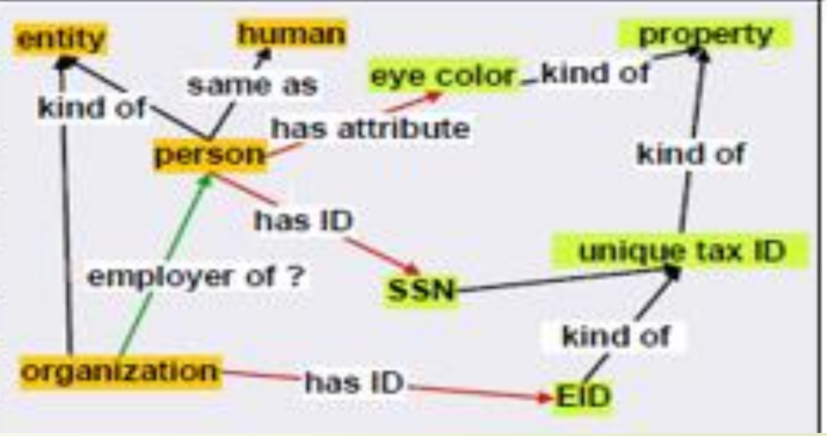
The NIST/Mitre corporaton Machine processable data

Ontologies, Controlled Vocabularies and Semantic Interoperability

	Controlled Vocabulary	Ontology
Definition	A controlled vocabulary (CV) is a set of lexical expressions that are vetted according to some criteria, such as their accepted usage in a community. • CVs are structured by one or more ordering relations, such as "narrower-than," "broader-than," or "related-to." • Structure is machine processable and semantics are human interpretable.	An ontology specifies the meaning of a controlled vocabulary in the form of a conceptual model. • Ontologies can be independent of any given controlled vocabulary. • Structure is machine processable and semantics are machine interpretable.

Example

Terms	Relation
entity	broader-than person broader-than organiz.
> person	narrower-than entity
>> eye color	related-to person
>> SSN	related-to person
>> employer	related-to person
> organization	narrower-than entity
>> EID	related-to organization



Controlled Vocabularies for Standards: contents and representation NIST/MITRE

- – CEE: Common Event Expression
- – CPE: Common Platform Enumeration
- – CRE: Common Remediation Enumeration
- – CVE: Common Vulnerability Enumeration
- – CWE: Common Weakness Enumeration
- – MAEC: Malware Attribute Enumeration and Characterization
- – OVAL: Open Vulnerability and Assessment Language
- – XCCDF: Extensible Configuration Checklist Description Format

■ Both MITRE and NIST maintain public repositories and Web sites for the various standards: http://nvd.nist.gov/ http://oval.mitre.org/repository/ http://measurablesecurity.mitre.org/

CVE (SR-13/03/2018)/MITRE

Incident	TXT	HTML	XML
CVE-2018-7580	Name: CVE-2018-7580 Status: Candidate URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7580 Phase: Assigned (20180301) Category: ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided. Current Votes: None (candidate not yet proposed)	Name: CVE-2018-7580<p> <p>Description: ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided. <p>Status: Candidate Phase: Assigned (20180301) <p>Votes: <pre></pre>	<item seq="2018-7580" name="CVE-2018-7580" type="CAN"><status>Candidate</status><phase date="20180301">Assigned</phase><desc>** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.</desc><refs></refs><votes> </votes><comments> </comments></item>
CVE-2018-7581	Name: CVE-2018-7581 Status: Candidate URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7581 Phase: Assigned (20180301) Category: ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided. Current Votes: None (candidate not yet proposed)	Name: CVE-2018-7581<p> <p>Description: ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided. <p>Status: Candidate Phase: Assigned (20180301) <p> Votes: <pre></pre>	<item seq="2018-7581" name="CVE-2018-7581" type="CAN"><status>Candidate</status><phase date="20180301">Assigned</phase><desc>\ProgramData\WebLog Expert\WebServer\WebServer.cfg in WebLog Expert Web Server Enterprise 9.4 has weak permissions (BUILTIN\Users:(ID)C), which allows local users to set a cleartext password and login as admin.</desc><refs><ref url="https://www.exploit-db.com/exploits/44270/" source="EXPLOIT-DB">44270</ref><ref url="http://hyp3rlinx.altervista.org/advisories/WEBLOG-EXPERT-WEB-SERVER-ENTERPRISE-v9.4-AUTHENTICATION-BYPASS.txt" source="MISC">http://hyp3rlinx.altervista.org/advisories/WEBLOG-EXPERT-WEB-SERVER-ENTERPRISE-v9.4-AUTHENTICATION-BYPASS.txt</ref><ref url="http://packetstormsecurity.com/files/146697/WebLog-Expert-Web-Server-Enterprise-9.4-Weak-Permissions.html" source="MISC">http://packetstormsecurity.com/files/146697/WebLog-Expert-Web-Server-Enterprise-9.4-Weak-Permissions.html</ref></refs><votes> </votes><comments> </comments></item>

Network resilience ontology Enisa 2011

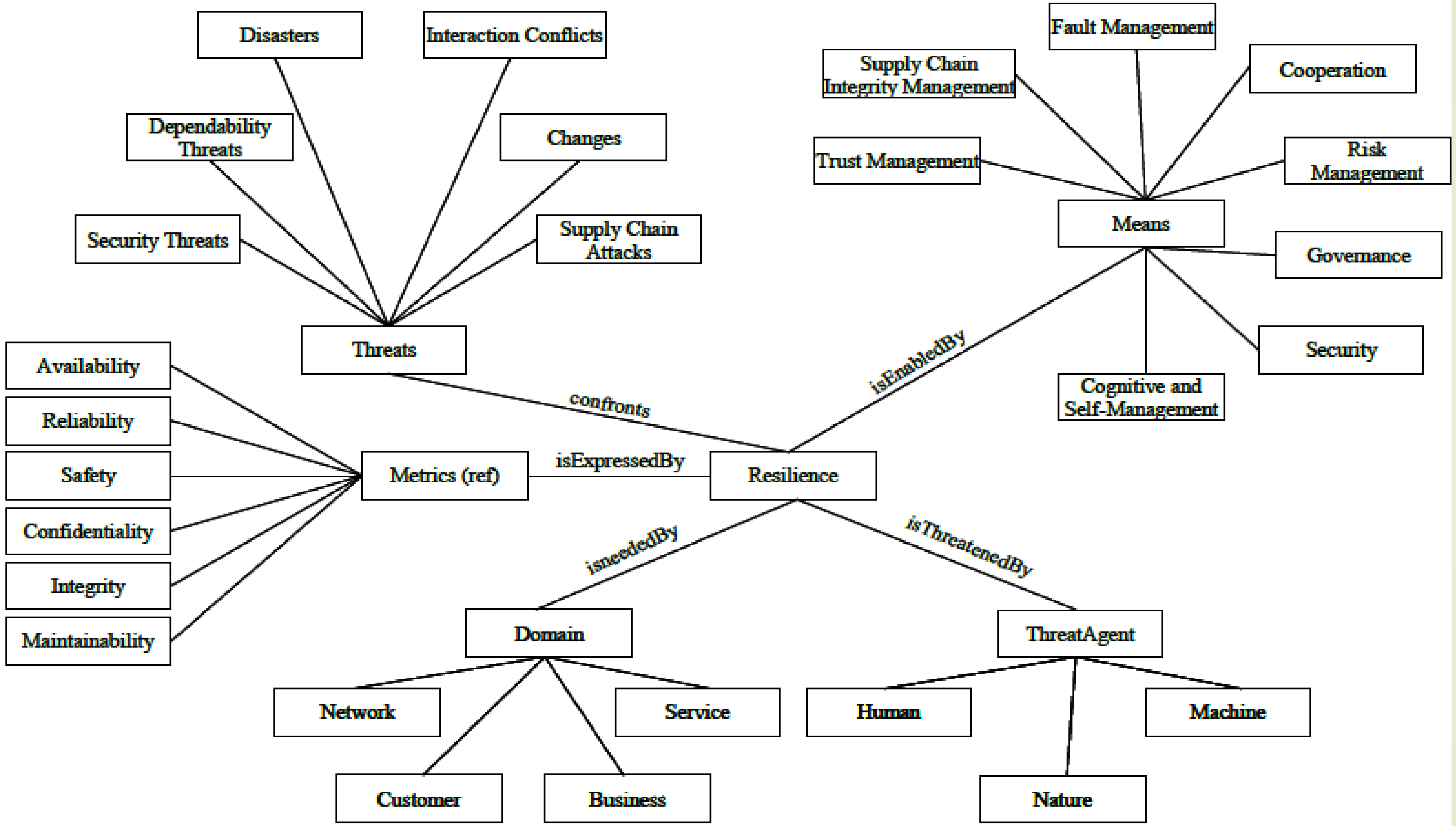


Figure 11: High level overview of resilience ontology

Business ontology (sub-domain)

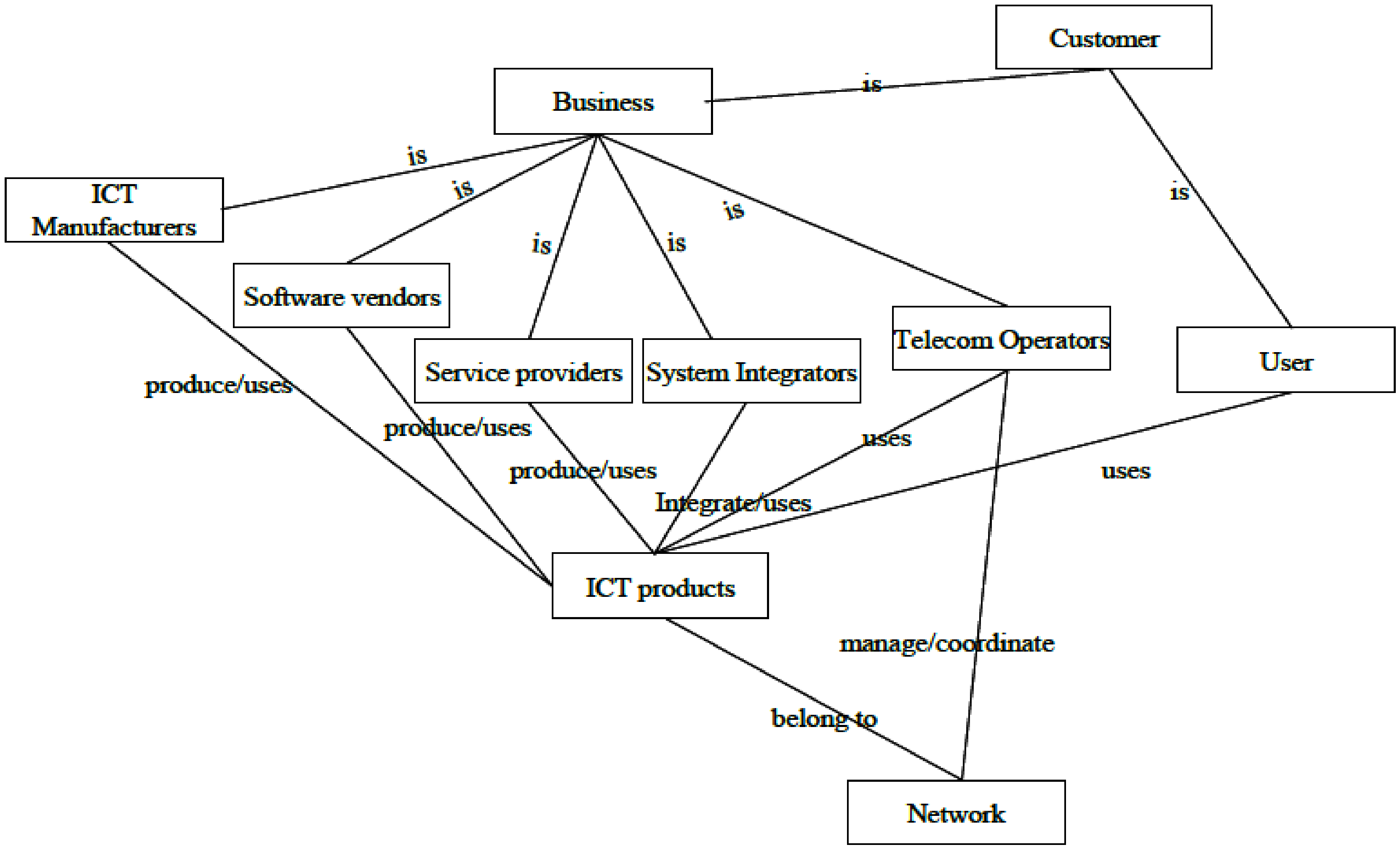


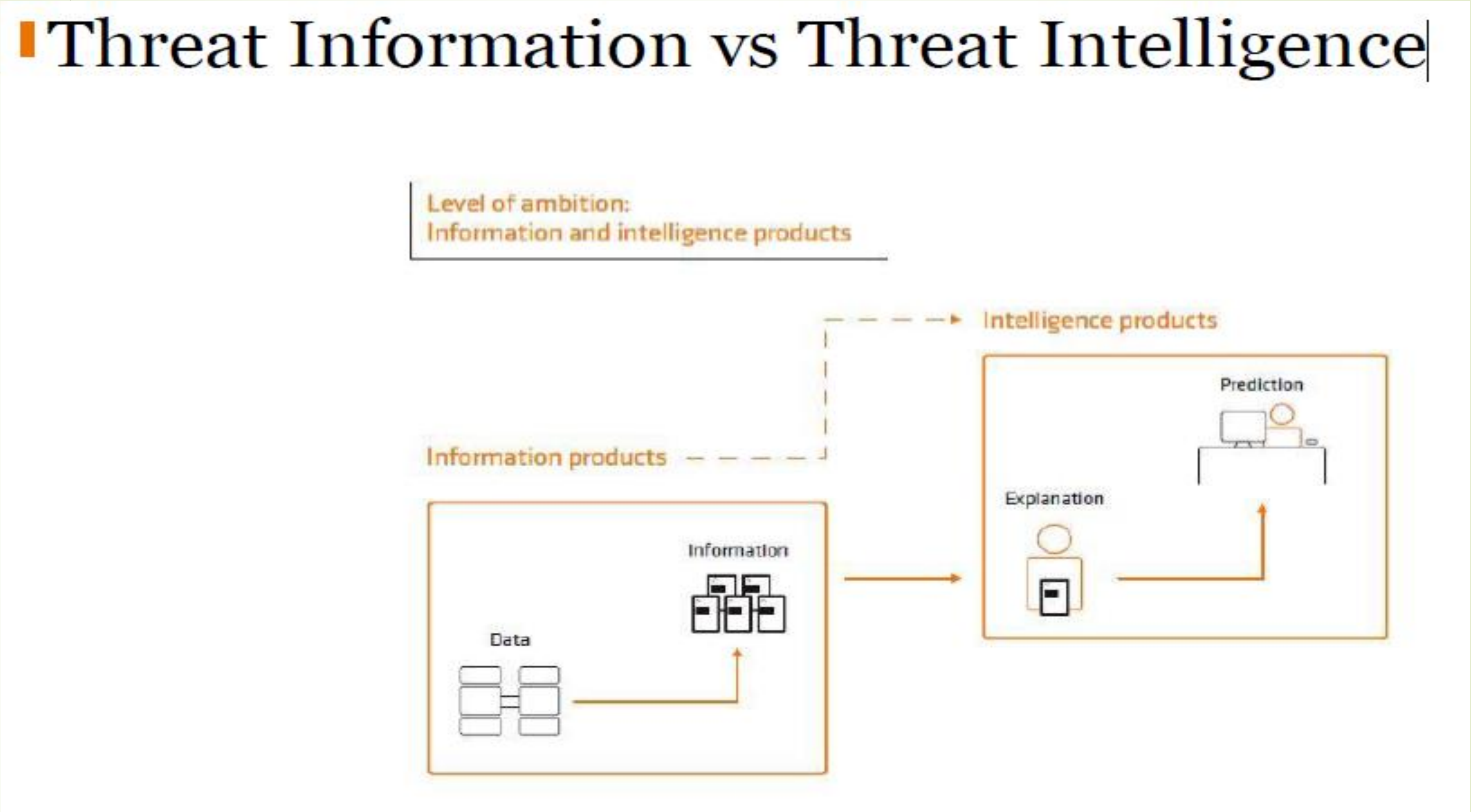
Figure 19: Business domain

cybsec as a service zuanelli eage 18

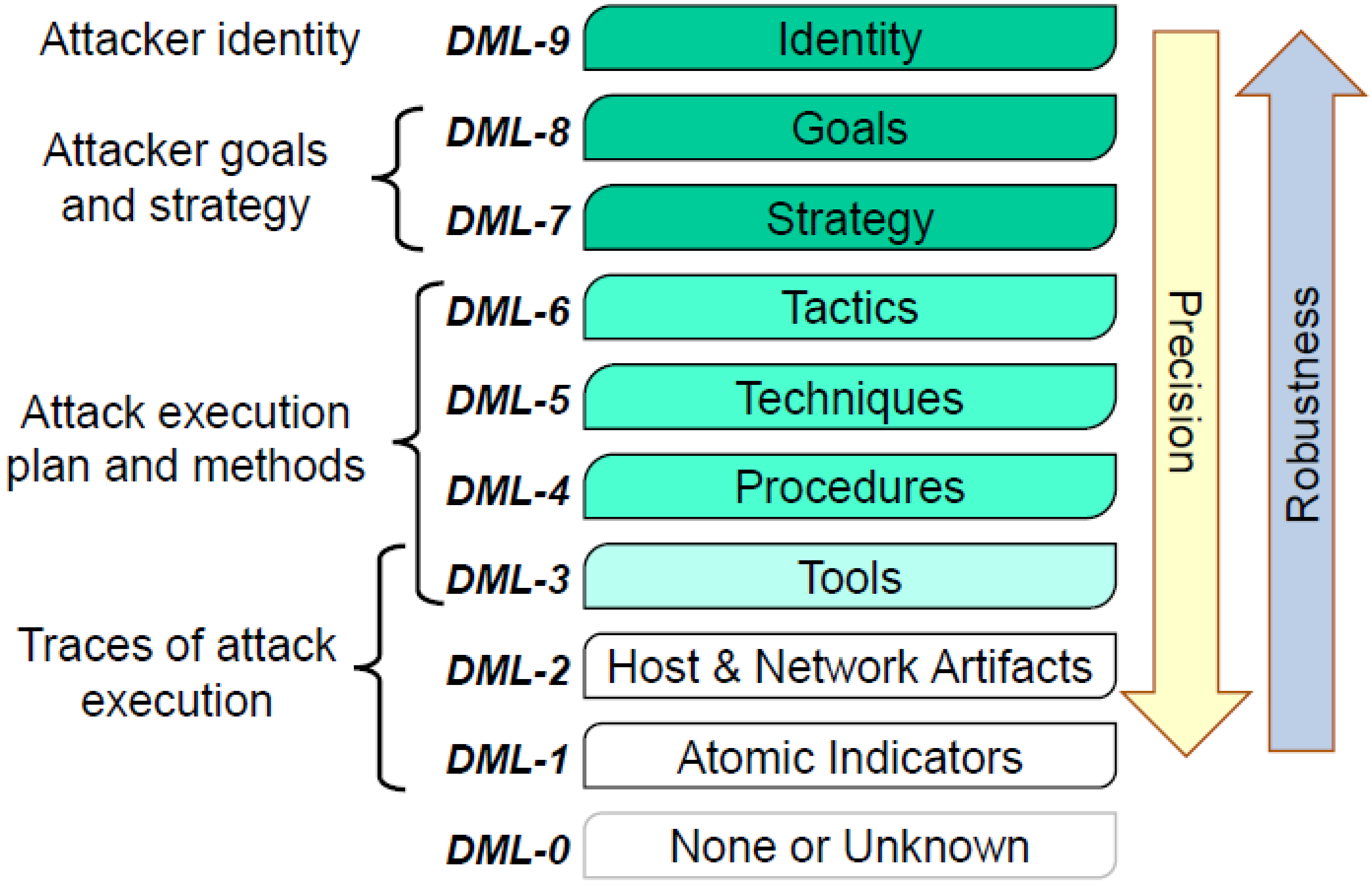
ACT, TOCSA and Oslo Analytics (2017)

•Semi-Automated Cyber Threat Intelligence (ACT)
-Open Source Threat Intelligence Platform
-https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/
•Threat Ontologies for Cyber Security Analytics (TOCSA)
-Ontologies
-PhD Project
-https://www.mnemonic.no/no/research-and-development/threat-ontologies-for-cybersecurity-analytics/
-http://www.mn.uio.no/ifi/english/research/projects/tocsa/
•Operable Subjective Logic Analysis Technology for Intelligence in Cybersecurity (Oslo Analytics)
-Analytics
-Subjective Logic (quantifying uncertainty)
-Trust Networks
-Academic
-http://www.mn.uio.no/ifi/english/research/projects/oslo-analytics/

The approach

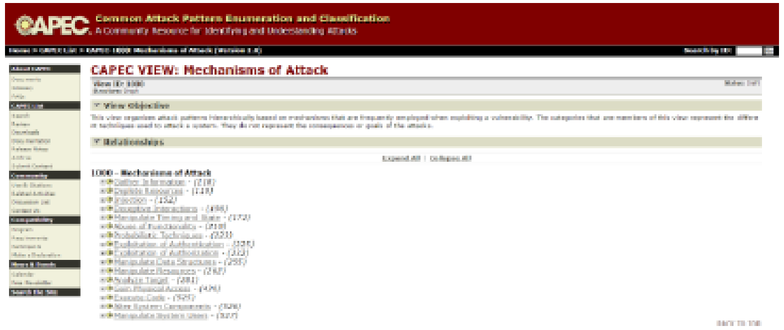


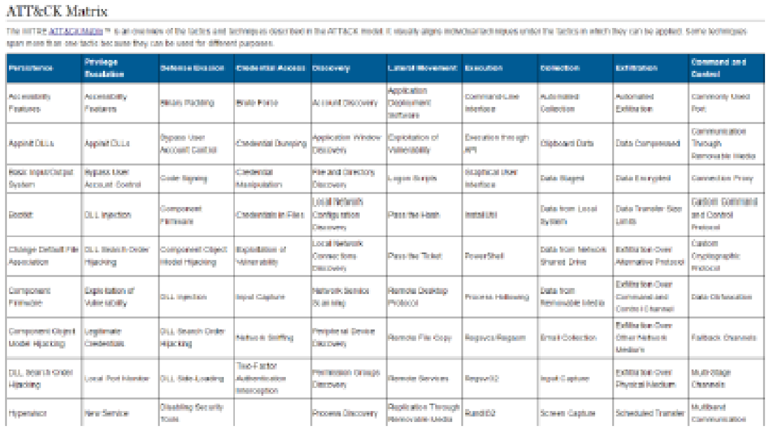
The Detection Maturity Level (DML) Model



Semantic Feature Extraction

- Formal definitions of
  - -Goals
  - -Strategy
  - -Tactics
  - -Techniques
  - -Procedures
- Relevant initiatives
  - -MITRE CAPEC
    - https://capec.mitre.org
  - -MITRE ATT&CK
    - https://attack.mitre.org
  - -MITRE CAR
    - https://car.mitre.org





Network security ontologies

- Network security ontologies: aspects/ compaison (V. Silva and G. Rodriguez 2017 in https://arxiv.org/pdf/1704.02441)

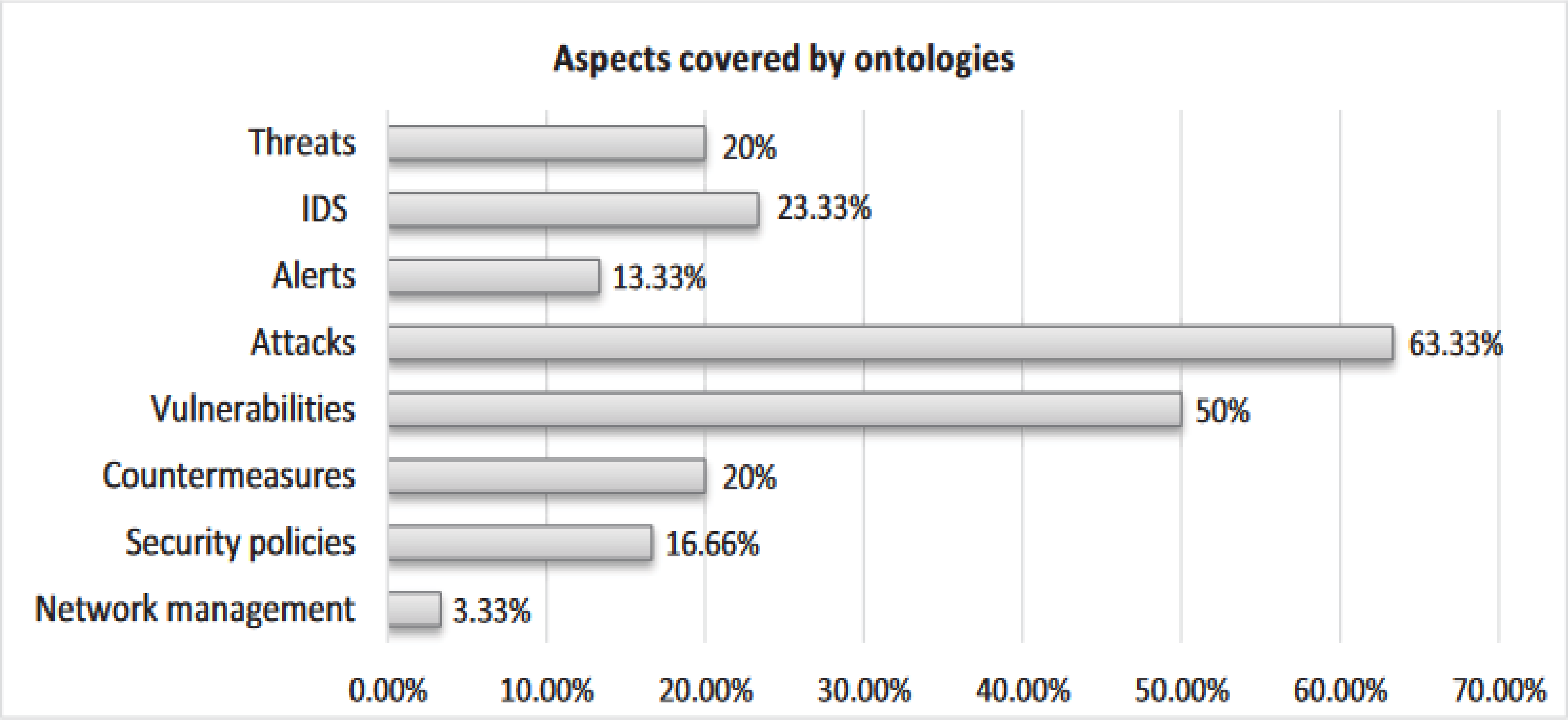


Figure 1: Aspects covered by ontologies

Comparison features (Silva & Rodriguez 2017)

- 63.33% of the ontologies make reference to attacks and their taxonomical structure. Their focus is mainly on the network layer **missing attacks at the application layer**.

- 80% of the papers reviewed **do not present the results obtained from test scenarios**, and therefore it is unachievable to evaluate the ontology and determin if it adapts to the requirements or to measure its effectiveness.

- Only 13.33% of the papers validate their proposals, trying to identify the **correct use of the language, the accuracy of the taxonomic structure, the validity of the vocabulary, and the adequacy of the requirements** for the purpose of documenting the process of development to verify if the proposal complies with the terms specified …

.

…Comparison features

- One of the challenges that constitutes a potentially interesting area arises when data is collected from **different safety equipment** (IDS, Intrusion prevention system, firewall, antivirus system, system security audit, honeynet,etc.).
- The **safety equipment is distributed in different domains in the network**, which is required to develop an ontology that can integrate real-time data from this safety equipment and allows the captured data to be properly administered

The proposal: neither ontology nor taxonomy (Silva and Rodriguez)

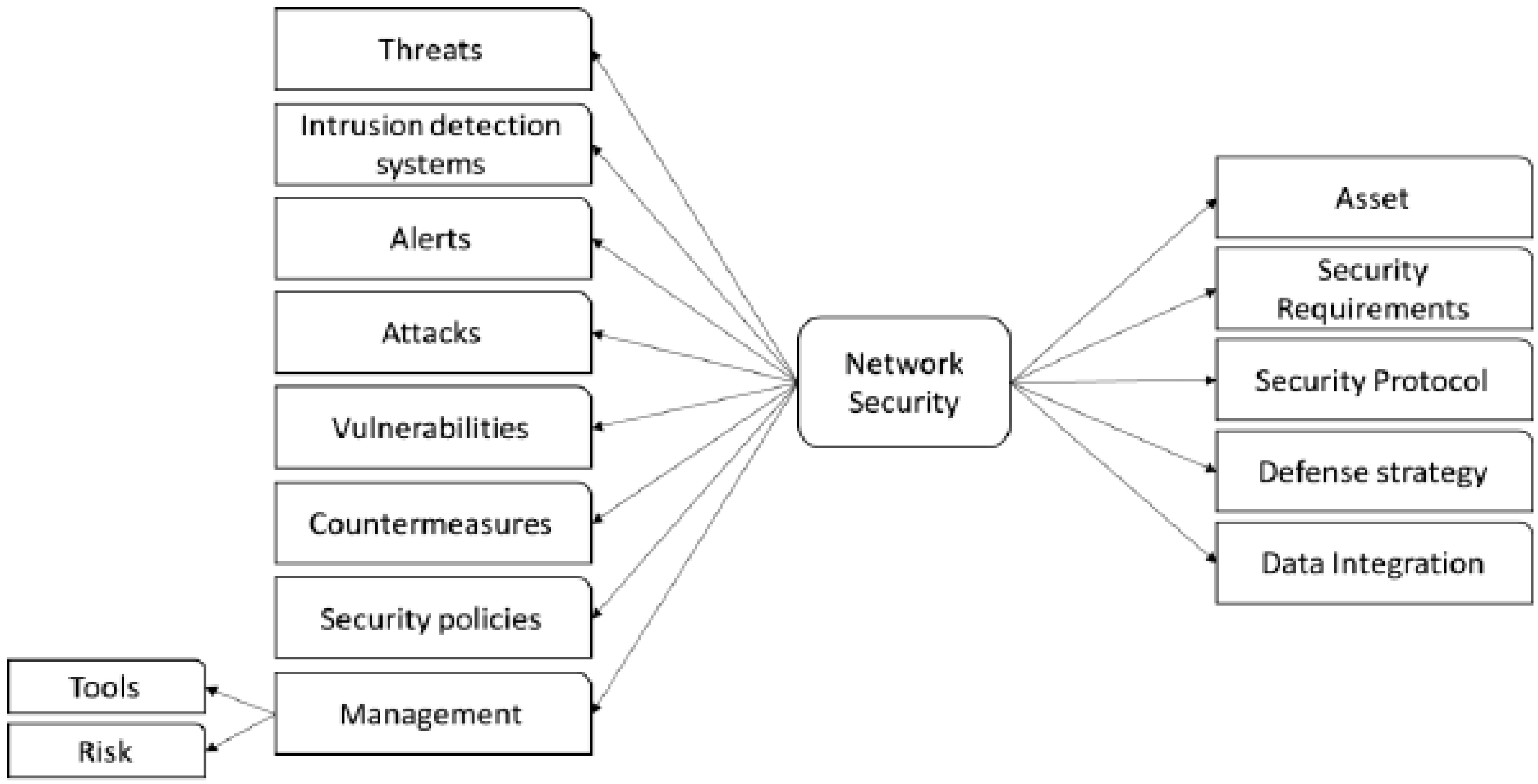


Figure 2: Comprehensive ontology in network security

cybsec as a service zuanelli eage 18

General ontologies frameworks

UCO: A Unified Cybersecurity Ontology: Zareen Syed, Ankur Padia, Tim Finin, Lisa Mathews and Anupam Joshi, 2016)

Table 1: Syntax and Semantics of Description Logic constructors

Name	Syntax	Semantics	Symbol
Top	$\top$	$\Delta^{\mathcal{I}}$	$\mathcal{AL}$
Bottom	$\perp$	ϕ	$\mathcal{AL}$
Intersection	$C \sqcap D$	$C^{\mathcal{I}} \cap D^{\mathcal{I}}$	$\mathcal{AL}$
Union	$C \sqcup D$	$C^{\mathcal{I}} \cup D^{\mathcal{I}}$	$\mathcal{U}$
Negation	$\neg C$	$\Delta^{\mathcal{I}} \setminus D^{\mathcal{I}}$	$\mathcal{C}$
Value restriction	$\forall R.C$	$\{a \in \Delta^{\mathcal{I}} \mid \forall b. (a,b) \in R^{\mathcal{I}} \rightarrow b \in C^{\mathcal{I}} \}$	$\mathcal{AL}$
Existential quant.	$\exists R.C$	$\{a \in \Delta^{\mathcal{I}} \mid \forall b. (a,b) \in R^{\mathcal{I}} \wedge b \in C^{\mathcal{I}}\}$	$\mathcal{E}$
Nominal	I	$I^{\mathcal{I}} \subseteq \Delta^{\mathcal{I}}$ with $\lvert I^{\mathcal{I}} \rvert = 1$	$\mathcal{O}$
Qualified Number restriction (less than)	$\leq nR.C$	$\{a \in \Delta^{\mathcal{I}} \mid \lvert \{ \forall b \in \Delta^{\mathcal{I}} \mid (a,b) \in \mathcal{R}^{\mathcal{I}} \wedge b \in C^{\mathcal{I}} \} \rvert \leq n \}$	$\mathcal{Q}$
Qualified Number restriction (equal than)	$= nR.C$	$\{a \in \Delta^{\mathcal{I}} \mid \lvert \{ \forall b \in \Delta^{\mathcal{I}} \mid (a,b) \in \mathcal{R}^{\mathcal{I}} \wedge b \in C^{\mathcal{I}} \} \rvert = n \}$	$\mathcal{Q}$
Qualified Number restriction (greater than)	$\geq nR.C$	$\{a \in \Delta^{\mathcal{I}} \mid \lvert \{ \forall b \in \Delta^{\mathcal{I}} \mid (a,b) \in \mathcal{R}^{\mathcal{I}} \wedge b \in C^{\mathcal{I}} \} \rvert \geq n \}$	$\mathcal{Q}$
Role Hierarchy	$R_1 \sqsubseteq R_2$	$\{ (a, b) \in \Delta^{\mathcal{I}} \times \Delta^{\mathcal{I}} \mid (a, b) \in R_1^{\mathcal{I}} \rightarrow (a, b) \in R_2^{\mathcal{I}} \}$	$\mathcal{H}$
Role Inverse	R^{-}	$\{ (b, a) \in \Delta^{\mathcal{I}} \times \Delta^{\mathcal{I}} \mid (a, b) \in R^{\mathcal{I}} \}$	$\mathcal{I}$
Role Composition	$R_1 \circ R_2$	$\{ (a, c) \mid \exists b. (a, b) \in R_1^{\mathcal{I}} \wedge (b, c) \in R_2^{\mathcal{I}} \}$	$\mathcal{R}$

cybsec as a service zuanelli eage 18

UCO conceptual relationships

In addition to mapping to STIX, UCO has also been extended with a number of **relevant cybersecurity standards, vocabularies and ontologies** such as CVE4, CCE5, CVSS6, CAPEC7, CYBOX8, KillChain9 and STUCCO10

To support diverse use cases,UCO ontology has been mapped to general **world knowledge** available through Google's knowledge graph, Dbpedia knowledge base (Auer et al. 2007), Yago knowledge base (Suchanek, Kasneci, and Weikum 2008) etc.

Linking to these knowledge sources provides **access to large number of datasets for different domains** (e.g. geonames) as well as terms in different languages (e.g. Russian

UCO's 'important' classes present in UCO ontology

1. **Means**: This class describes various **methods of executing an attack** and consists of sub-classes like BufferOver-Flow, SynFlood, LogicExploit, TcpPortScan etc., which can further consist of their own sub-classes. The Means class maps to TTP field in STIX which characterizes specific details of observed or potential attacker Tactics, Techniques and Procedures.

2. **Consequences:** This class describes the **possible outcomes of an attack**. It consists of sub-classes like DenialOfService, LossOfConfiguration, PrivilegeEscalation,UnauthUser, etc. It maps to Observables in STIX.

3. **Attack**: This class characterizes a **cyber threat attack** and is mapped to Incident in STIX.

4. **Attacker**: This class represents **identification or characterization of the adversary** and is mapped to ThreatActor in STIX.

UCO classes

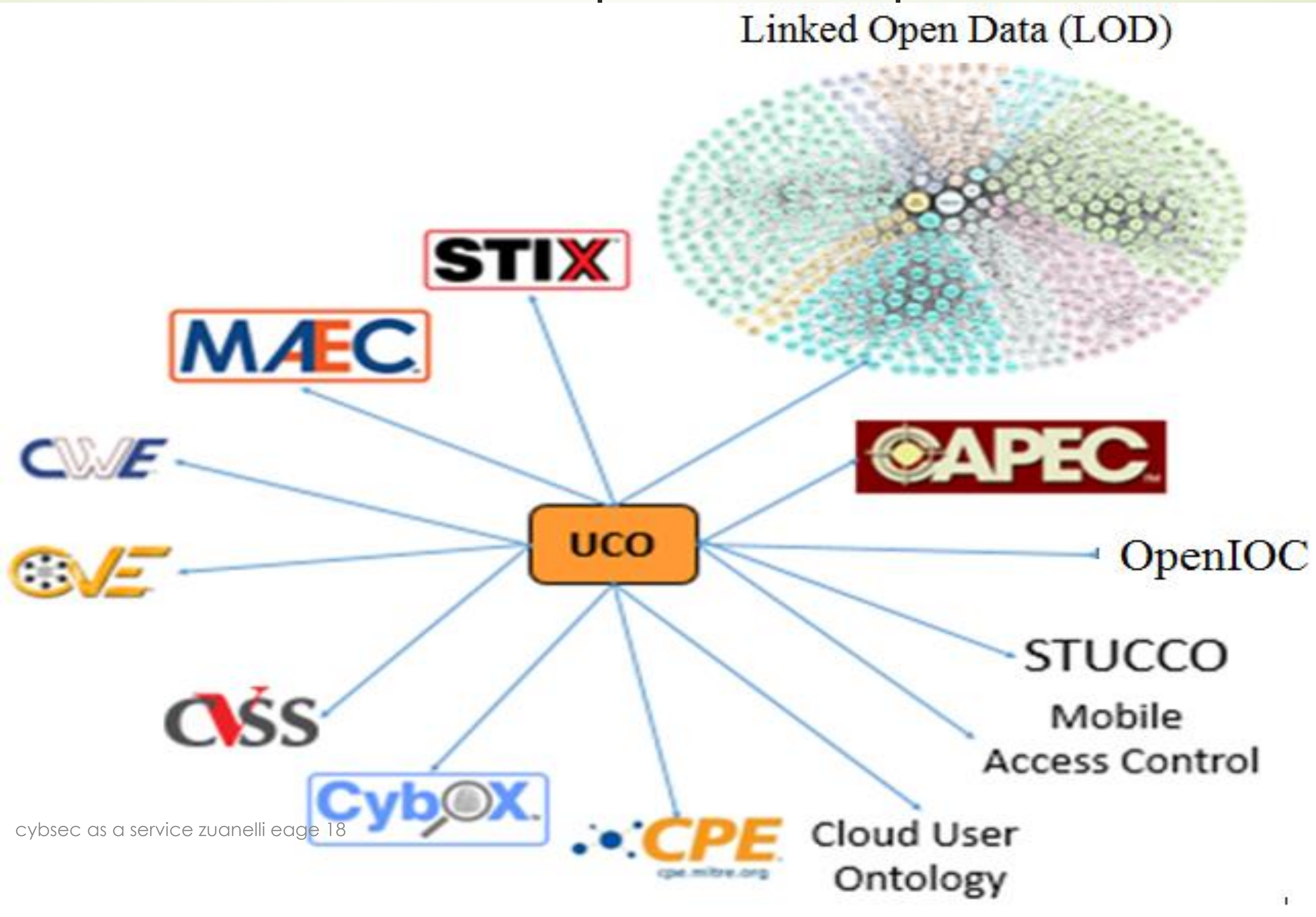
5. **Attack Pattern**: Attack Patterns are **descriptions of common methods for exploiting software** providing the attackers perspective and guidance on ways to mitigate their effect. An example of attack pattern is Phishing.

6. **Exploit:** This class characterizes **description of an individual exploit and maps** to ExploitType in STIX schema.

7. **Exploit Target**: **Exploit Targets are vulnerabilities or weaknesses** in software, systems, networks or configurations that are targeted for exploitation by the TTP (cyber threat adversary Tactic, Technique or Procedure).

8. **Indicator**: A cyber threat indicator is made up of **a pattern identifying certain observable conditions as well as contextual information** about the patterns meaning, how and when it should be acted on, etc. This class is mapped to IndicatorType in STIX schema and Indicator class in CAPEC ontology.

UCO ontology serves as the core for



Limitations of approach

- **Difference of conceptual relational descriptors** in a metadata language such as OWL as opposed to logical semantic entities as defined by (fuzzy) logic criteria in terminology
- UCO classes lack **entities definition**: no logical semantic definition
- **Useful linked open data**

Cyber threat intelligence model: **taxonomies, sharing standards and ontologies**

Cyber threat intelligence comparison and model (V. Mavroeidis and S. Bromander 2017 in

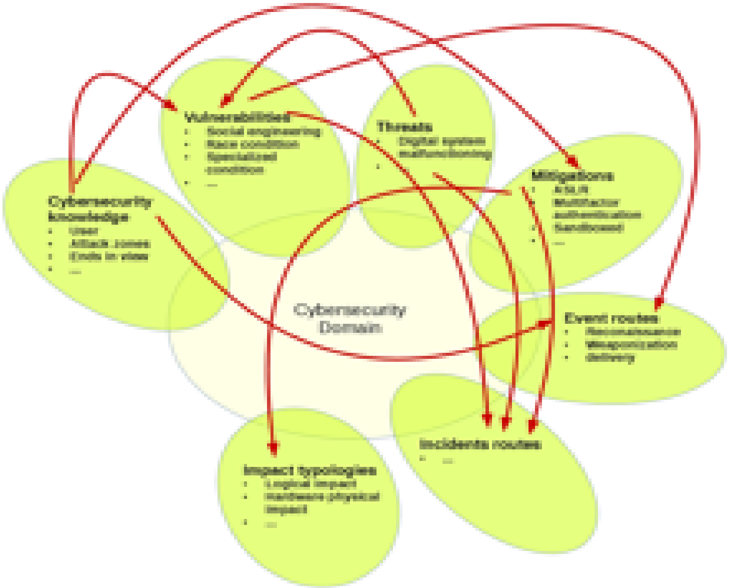
TABLE I
CTI EVALUATION: TAXONOMIES, SHARING STANDARDS, AND ONTOLOGIES

		Identity	Motivation	Goal	Strategy	TTP	Tool	IOC	Atomic Indicator	Target	COA
Taxonomies	TAL [8]	*									
	Threat Agent Motivation [5]	*	*								
	CVE [9]								*		
	NVD [10]								*		
	CPE [11]								*		
	CWE [12]					*			*		*
	CAPEC [13]					*		*			*
	ATT&CK [14]	*				*	*				
	CVSS [15]								*		
	CWSS [16]								*		
Sharing Standards	STIX 1 [18]	*	*	* (Intended Effect:taxonomy)	*	*	*	*	*	*	*
	STIX 2 [36]	*	*	* (Objectives:string)	*	*	*	*	*	*	*
	MAEC [19]							*			
	OpenIOC [37]					*	*	*	*		
Ontologies	Fenz & Ekelhat (2009) [21]								*		
	Wang & Guo (2009) - OVM [22]					*			*		*
	Orbst et al. (2012) [23]	*					*		*	*	
	More et al. (2012) [26]					*			*		
	Oltramari et al. (2014) - CRATELO [27]	*				*			*	*	
	Gregio et al. (2014) [28]						* (malware)		*		
	Salem & Wacek (2015) - ICAS [29]					*			*		
	Iannacone et al. (2015) - STUCCO [30]	*				*	*		*		
	Gregio et al. (2016) - MBO [31]						* (malware)	*	* (it may provide)		
	Fusun et al. (2015) - ASR [32]					*			*	*	
	Pendelton et al. (2016) - Security Metrics Ontology [34]					*					*
	Syed et al. (2016) - UCO [35]	*	*	*	*	*	*	*	*		*
	Unified Cyber Ontology (2016) - UCO [38]	*	*	*	*	*	*	*	*	*	*

The Pragmema cybersecurity ontology: POC

- the **univocal application** of the representation concepts, entities and relations as conceived in upper and mid-level ontology
- **constituents**: cybersecurity domain ontology, cybersecurity pragmatic ontology, cybersecurity knowledge, semantic vocabulary
- **different level entities**, **semantic** and **pragmatic relations**

The domain ontology



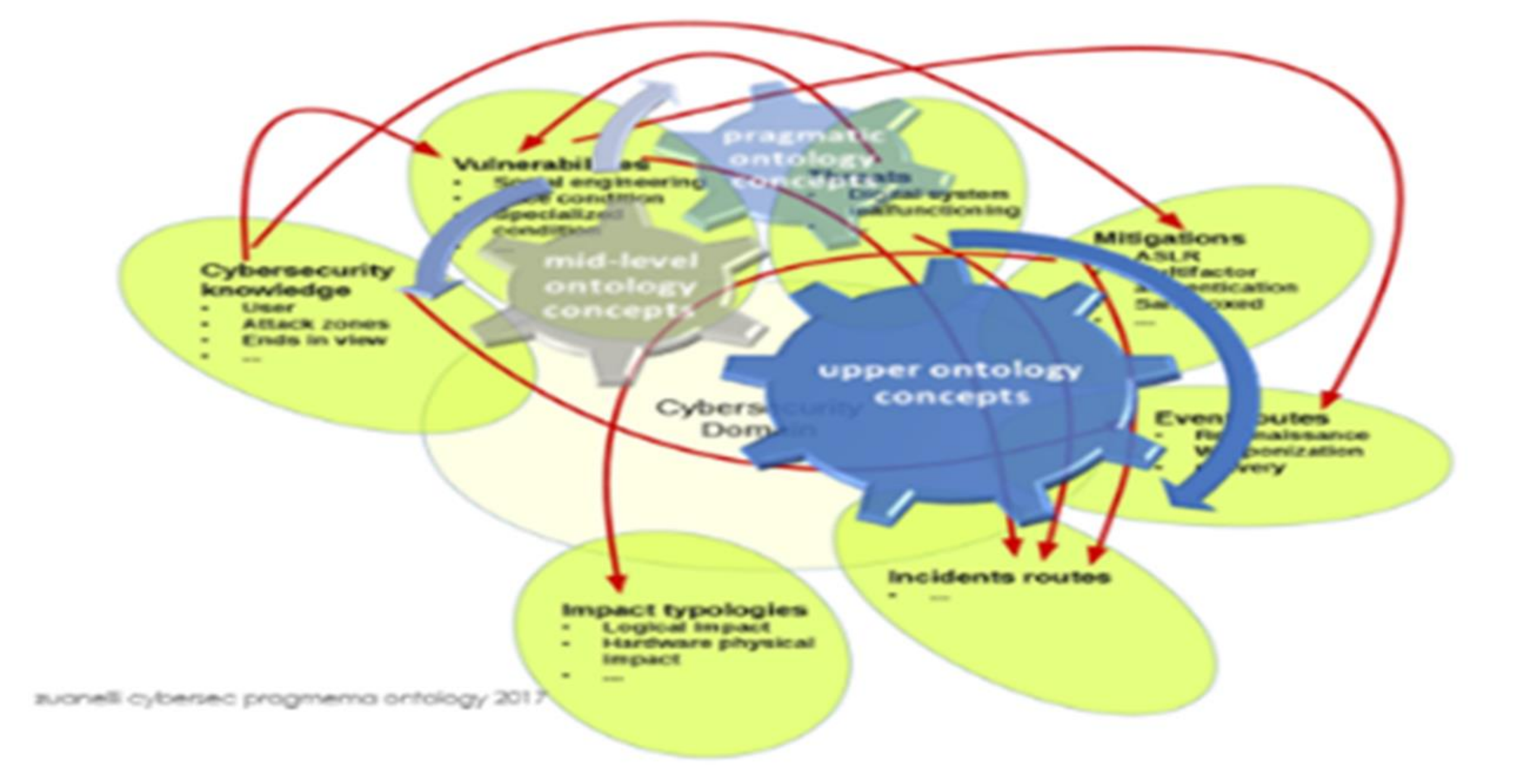
Definitions:

- Univocal
- Unequivocal

Structure:

- Taxonomy
- Hierarchic relations from broader to detailed
- Ontology: reticular multiple relations

The Poc ontology: domain ontology and pragmatic ontology

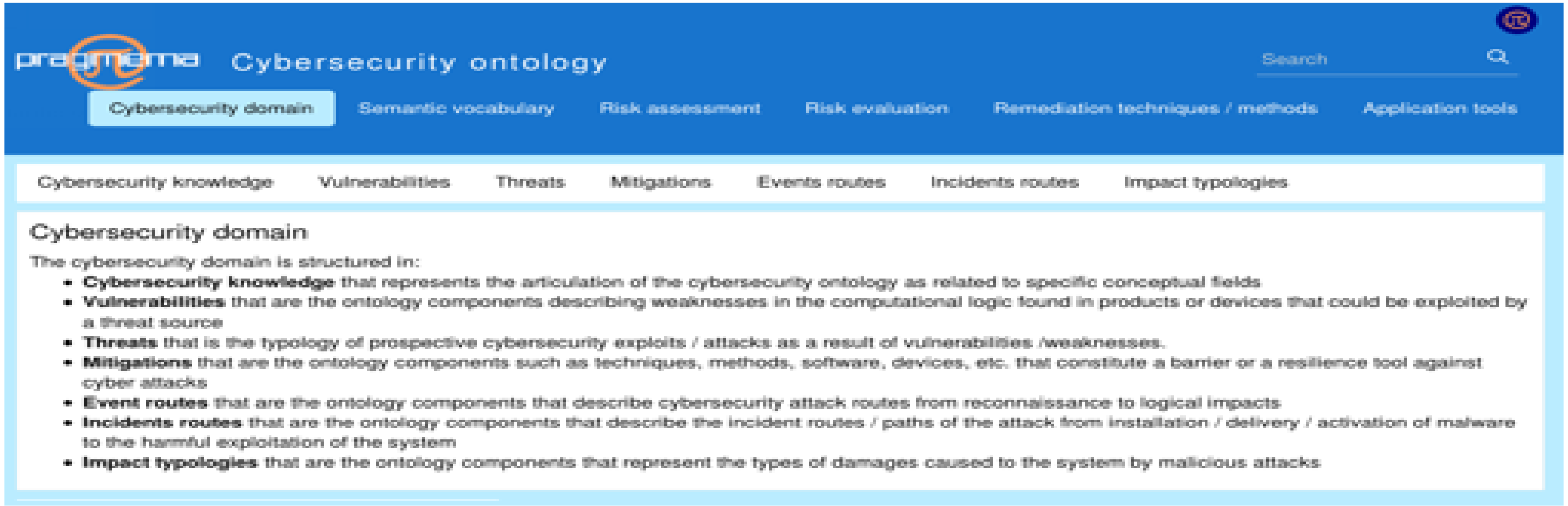


cybsec as a service zuanelli eage 18

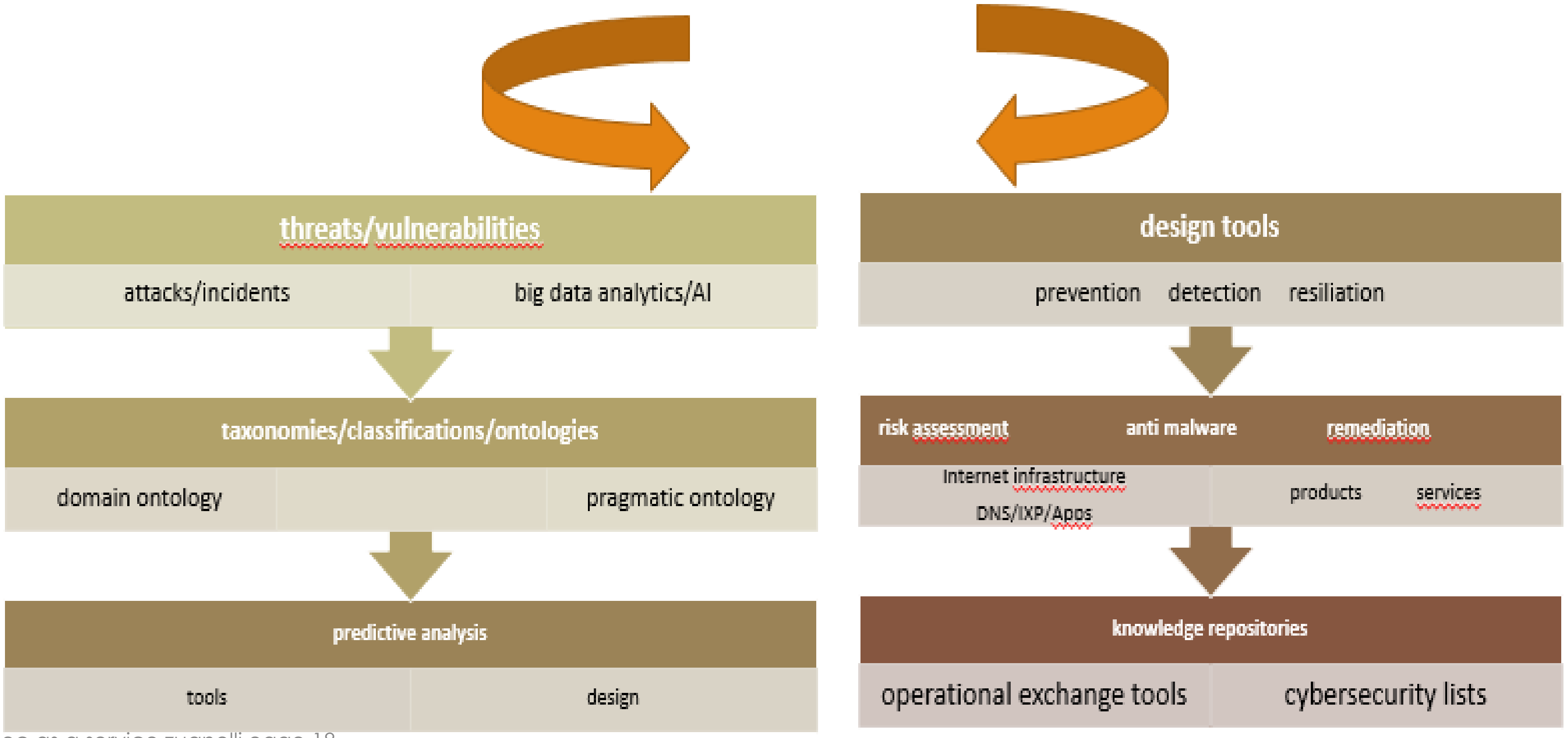
The POC PLATFORM: a cybersecurity ontology for big data analytics and services

POC: a complete platform

- Seven analytics areas for specific cybersecurity services
- A tools area for risk assessment, risk evaluation, remediation techniques, specific applications: data recording and incident reporting, statistics, metrics, standards, etc.



An integrated platform for cybersecurity as a service



cybsec as a service zuanelli eage 18

Cybersecurity as a service: towards enabling collaborative platforms

Thanks …