WACREN CONFERENCE 2018
Togo, Lomè

CYBERSECURITY AS A SERVICE: THE POC TOOL/PLATFORM FOR DESIGN AND IMPLEMENTATION

ELISABETTA ZUANELLI

UNIVERSITY OF ROME "TOR VERGATA"

PRESIDENT OF CRESEC (WWW.CRESEC.COM)

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 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**.

The content parameters

Typological lists of **cybersecurity variables** such as domains of attacks, mechanisms of attack, incidents lists, etc.

Cybersecurity analytics tools such as cybersecurity domain ontologies and pragmatic domain platforms capable of control of technological assets, vulnerabilities, threats, events, incidents, etc.

An ASREN/WACREN knowledge cybersecurity platform

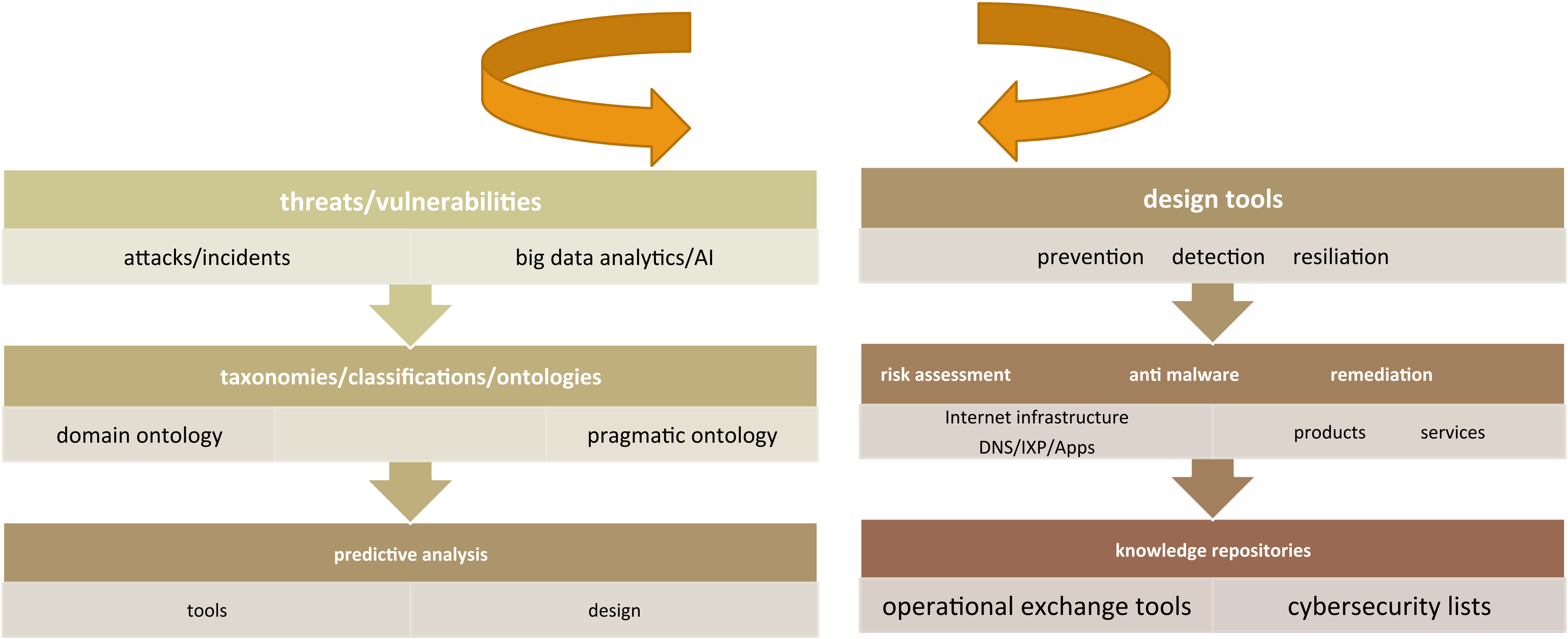
a synthesis of the state of the art in cybersecurity as a structured data base for collaboration and interpretation

- **vendors (cybersecurity by design in the development of devices) : i.e. OOSS, programs, applications in different domains: i.e. cloud, IoT, platforms, mobile apps**
- **IXP, DNS,Routers, etc.;**
- **cybersecurity antimalware suppliers/vendors: i.e. Kaspersky, Symantec, etc.;**
- **cybersecurity assessment for analysts companies (SIEM SOC, Csirts, etc.);**

and

- a shared ontology of **cybersecurity as a service** implying **semantic controlled vocabularies, lists and enumerations of conceptual entities of the phenomena, etc.;**
- the **sharing knowledge and automation tools for big data analytics** as provided by AI and machine learning;

cybersecurity as a service



threats/vulnerabilities

attacks/incidents | big data analytics/AI

taxonomies/classifications/ontologies

domain ontology | pragmatic ontology

predictive analysis

tools | design

design tools

prevention detection resiliation

risk assessment | anti malware | remediation

Internet infrastructure
DNS/IXP/Apps

products services

knowledge repositories

operational exchange tools | cybersecurity lists

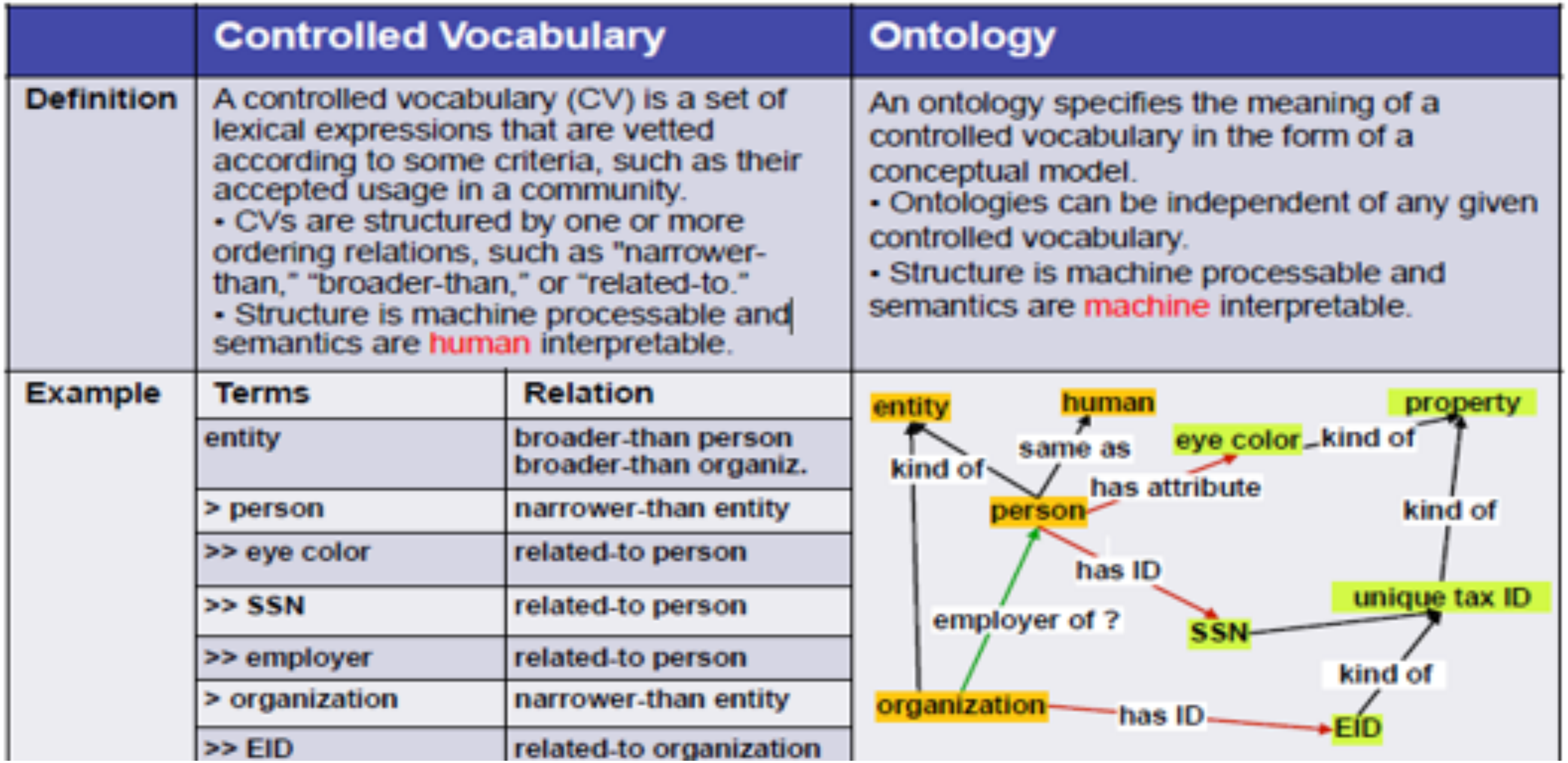
Cybersecurity ontology: Big data and AI technologies

“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, 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	

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

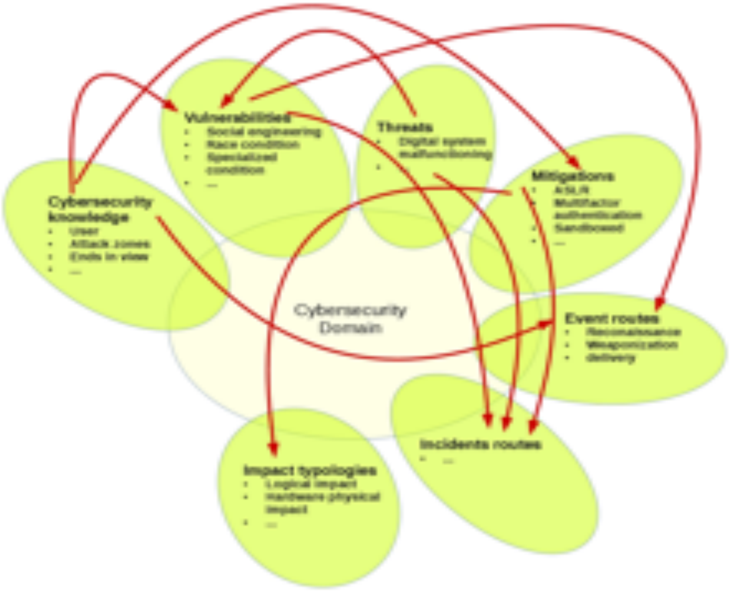
)

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)	<font size=+2><b>Name: CVE-2018-7580</b></font><p> <p><b>Description:</b> ** 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><b>Status:</b> Candidate<br> <b>Phase:</b> Assigned (20180301)<br> <p><b>Votes:</b> <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)	<font size=+2><b>Name: CVE-2018-7581</b></font><p> <p><b>Description:</b> ** 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><b>Status:</b> Candidate<br> <b>Phase:</b> Assigned (20180301)<br> <p> <b>Votes:</b> <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>

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



Vulnerabilities
- Social engineering
- Race condition
- Specialized condition
- ...

Threats
- Digital system malfunctioning
-

Mitigations
- ASLR
- Multifactor authentication
- Sandboxed
- ...

Cybersecurity knowledge
- User
- Attack zones
- Ends in view
- ...

Cybersecurity Domain

Event routes
- Reconnaissance
- Weaponization
- delivery

Incidents routes
- ...

Impact typologies
- Logical impact
- Hardware physical impact
- ...

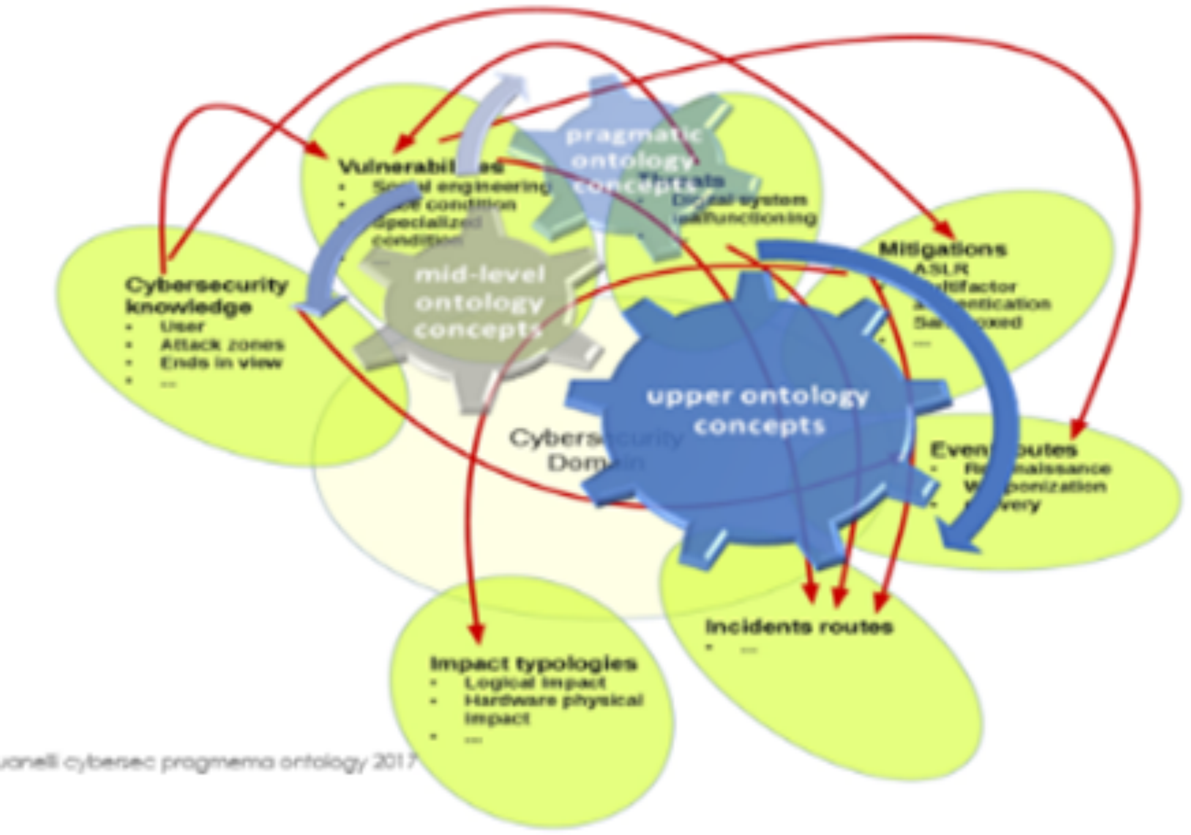
Definitions:

- Univocal
- Unequivocal

Structure:

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

The logical semantic relations network: cybersecurity domain ontology and pragmatic ontology

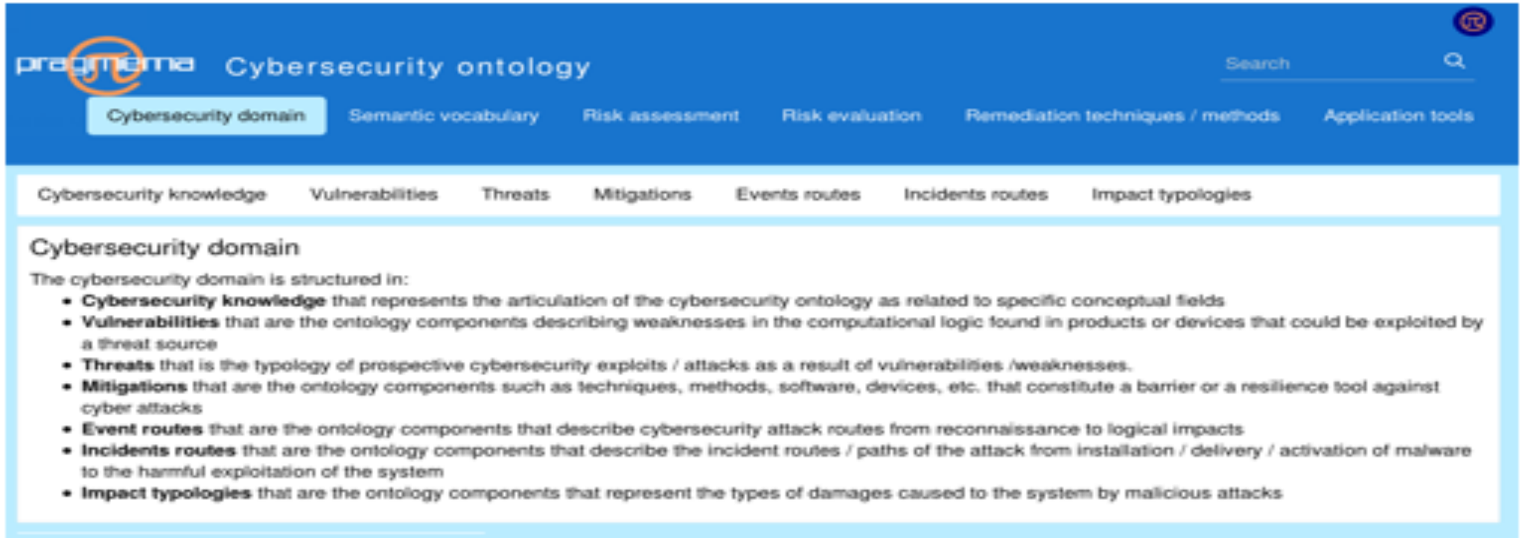


zuanelli cybersec pragmema ontology 2017

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.



Cybersecurity domain

The cybersecurity domain is structured in:

- **Cybersecurity knowledge** that represents the articulation of the cybersecurity ontology as related to specific conceptual fields
- **Vulnerabilities** that are the ontology components describing weaknesses in the computational logic found in products or devices that could be exploited by a threat source
- **Threats** that is the typology of prospective cybersecurity exploits / attacks as a result of vulnerabilities /weaknesses.
- **Mitigations** that are the ontology components such as techniques, methods, software, devices, etc. that constitute a barrier or a resilience tool against cyber attacks
- **Event routes** that are the ontology components that describe cybersecurity attack routes from reconnaissance to logical impacts
- **Incidents routes** that are the ontology components that describe the incident routes / paths of the attack from installation / delivery / activation of malware to the harmful exploitation of the system
- **Impact typologies** that are the ontology components that represent the types of damages caused to the system by malicious attacks

applications
in the cybersecurity domain

Cybersecurity as a service

A long way to go…