Zuanelli, E., (2025). J Inform Techn Int, 3(1): 106
https://doi.org/10.33790/jiti1100106

Journal of Information Technology and Integrity

AI Military Satellites Security in Aerospace: The POC Solution

Elisabetta Zuanelli
Professor Emeritus, Department of Management-Computing Sciences, School of Economy and Finance, University Rome "Tor Vergata", Italy.

Article Details
Article Type: Research Article
Received date: 04th March, 2025
Accepted date: 25th March, 2025
Published date: 03rd April, 2025

***Corresponding Author:** Elisabetta Zuanelli, Professor Emeritus, Department of Management-Computing Sciences, School of Economy and Finance, University Rome "Tor Vergata", Italy.

Citation: Zuanelli, E., (2025). AI Military Satellites Security in Aerospace: The POC Solution. *J Inform Techn Int, 3*(1): 106. doi: https://doi.org/10.33790/jiti1100106

Abstract

The purpose of the paper is to illustrate the specific AI satellites security domain issues and to propose the first AI ontological-taxonomic knowledge representation of partial components of the satellites security domain, with specific attention to the military field. The components of the satellites domain are investigated as for entities, classes, logical semantic relationships according to the Pragmema POC, Platform Ontology of Cybersecurity for cybersecurity defense*. The approach is based on the use of linguistic cognitive axioms implied by the semantic cognitive analysis of classes, entities and relationships. A new approach to the configuration analysis of properties and attributes involves the articulation structure into semantic, operative and episodic memory layers of architecture by means of a controlled semantic vocabulary.

Key words: Satellites Defense Ontology, Satellites Attacks, Satellites Impacts, Satellites Functionalities, Satellites Threats, Satellites Defense Solutions.

Aerospace power and satellite security systems: context analyses

The literature on satellites security [1], threats, risks, incidents, attacks to the satellites systems informs of the accentuated rising concern on these topics. According to Zhang, Zhao, He, et al. [2] "the current states of security technology development" … imply the analysis of "the areas of node access authentication, link secure transmission, and network security routing". Therefore, "the development trends of Satellite Internet security technology highlight the importance of endogenous, systematic, and intelligent Satellite Internet techniques" [3].

Specific proposals to prefigure preventive and predictive understanding of the evolution of satellites security ask for a knowledge representation of the domain. In this perspective, knowledge representation of the domain requires an ontological taxonomic approach to 'data', to be interpreted in an AI context correlation and processing. The satellites security ontology in the paper is grounded on the use of linguistic cognitive axioms implied by the semantic cognitive analysis of classes, entities and relationships of the specific domain.

A new approach to the configuration analysis of properties and attributes is added. This involves the articulation structuring of data into semantic, operative and episodic memory layers of the architecture, extracted from a controlled semantic vocabulary.

The purpose of the paper is to illustrate specific AI military satellites security domain issues and to propose the first knowledge representation of partial components of a satellite security domain ontology.

On the subject, I recall and take for assumed a previous paper of mine on the Pragmema POC of cybersecurity defense systems, as presented at a NATO Conference in 2022 [4].

General background and problems in the Pragmema POC's approach

AI knowledge representation for threat intelligence, info sharing, and incidents reports for satellites security aims at detection, prevention and prediction of cybersecurity attacks and incidents. The first conceptual framework of a cybersecurity ontology by MITRE in 2010 [5] proposed the definition of semantic and structural interoperability of data as specified in the following scheme.

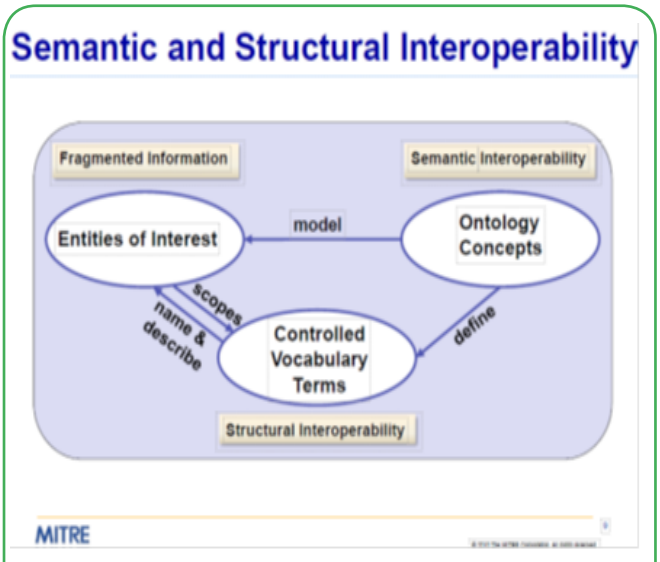

Fig. 1 The semantic and structural interoperability for ontologies

At the same time, MITRE [6] proposed a foundational model of a cybersecurity ontology where entities, logical semantic relationships and the elaboration of a controlled vocabulary for the definition of unambigous entities were illustrated.

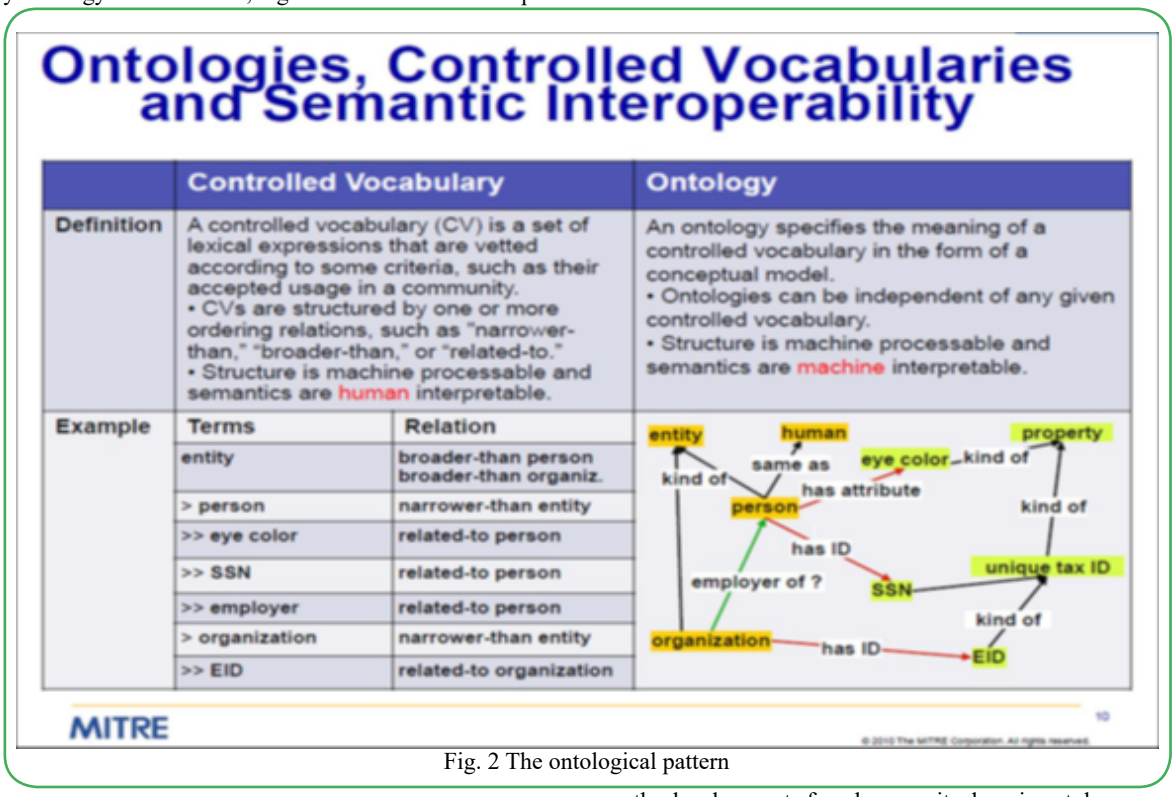

Fig. 2 The ontological pattern

From that time on, a number of cybersecurity platforms was developed and in 2016 NIST released the first vulnerability ontology [7].

The main repositories/platforms developed include [8]:

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

STIX: Structured Threat Information Expression

CAPEC: Common Attack Pattern Enumeration and Configuration

OWASP: Open Web Application Security Project

SIX/TAXII: Structured Threat Information Expression

MISP: Malware Information Sharing Project

In a comparative analysis of the diverse repositories and models, I specified the major flaws of these proposals:

- the lack of an upper-level ontology definition of entities and relationships
- the intuitive listings of cybersecurity entities and their logical semantic relationships
- the lack of a formal motivation and structuring of taxonomies and ontologies
- the quality of controlled vocabularies for entities definitions (if any).

One of the main problems as related to the operational capability of the various models, concerned the lack of IoCs/IoAs data correlation, classification and integration to describe attacks/incidents.

The problems faced by the POC approach were:

- the definition of abstract upper-level concepts and knowledge representation
- the development of a cybersecurity domain ontology, a pragmatic ontology for cybersecurity services and the specification of subdomain ontologies such as the financial, the automotive, and the shipping fields
- the univocal definition of entities and logical semantic relationships by means of a semantic controlled vocabulary
- the IoCs integration and correlation for incidents reporting and analytics
- the technological framework

The ontological representation of cybersecurity knowledge in the cybersecurity domain faces the definition of entities and their correlation by means of a knowledge ontology (upper-level domain ontology) and the specific domain ontology by means of procedural classes: threats, vulnerabilities, events, incidents, impact, resilience.

POC's scope as for services includes:

- detection and prevention of cyber events and incidents
- methods and technologies for risk assessment and risk evaluation
- frameworks for remedial, technological and behavioral systems
- standards for safety automation
- the constituent elements/fields of cybersecurity events and incidents, necessary for data reporting
- the automatic analysis of typological variables that define events and incidents.

The knowledge representation model, briefly summarized, illustrates the starting issues for the present preliminary analysis of the satellites security domain, entities and logical semantic relationships as for communication channels, threats, attacks, etc.

The satellites ontology of security: preliminary analysis

The specific literature on the subject [9] highlights the following synthetic considerations on the state of the art of satellites security. General satellites security problems concern:

- satellite communication between civilian and military uses
- satellites overcrowding

- interferences
- the absence of standards.

If we extend the analysis to the military satellites security context, the main issues to be defined may be summed up as follows:

- the analysis of technological configurations of the military satellites domain
- the definition of vulnerabilities, risks, threats, incidents, attacks, impacts, defenses
- the typology of attackers in the military field
- the typology of attacks in the military field.

The semantic specification of data related to the listed topics should be acquired and inserted into a correlational knowledge base to be used for threat intelligence, infosharing, and vulnerability/incidents reporting, having to do with preventive and predictive security activities.

Context analysis of civilian satellites systems

In an inspiring paper on satellites security in the LEO satellites civilian context [1], we can appreciate the presentation of potential vulnerabilities in communication channels and attackers' capabilities as related to threats.

As regards the typology of satellites orbits and communication channels, the analysis should face distinct representations for Geostationary Earth orbit (GEO) (satellites that are positioned around 36,000 kilometers above the Earth's surface); medium Earth orbit (MEO) (satellites that occupy altitudes ranging from approximately 2,000 to 36,000 kilometers); and low Earth orbit (LEO) (satellites situated at altitudes ranging from approximately 160 to 2,000 kilometers above the Earth's surface).

A first systematization should lead to the interpretation of different communication systems orbits and related implications for communication links and interfaces in the military context.

COM SAT satellites presentation: segments and user interface

According to NIST [10] , SATCOM analysis of components includes ground stations, space segments, communication segments and user segments.

Ground segments relate ground to ground relationships on one side and ground segment GSaaS on the other as implied, this second, in Internet communication between users and cloud platforms (communicating in turn through Internet with network operators).

The ground segment interacts with the space segment satellite and satellite with satellite ground system; whereas intersatellites links connect satellite to satellite in a biunivocal relationship.

The satellite to user and user to satellite links represent a twofold relationship; the user segment is furtherly linked to the ground system.

This complex network of interactions in SATCOM imply a wide range of different vulnerabilities in civilian satellites systems.

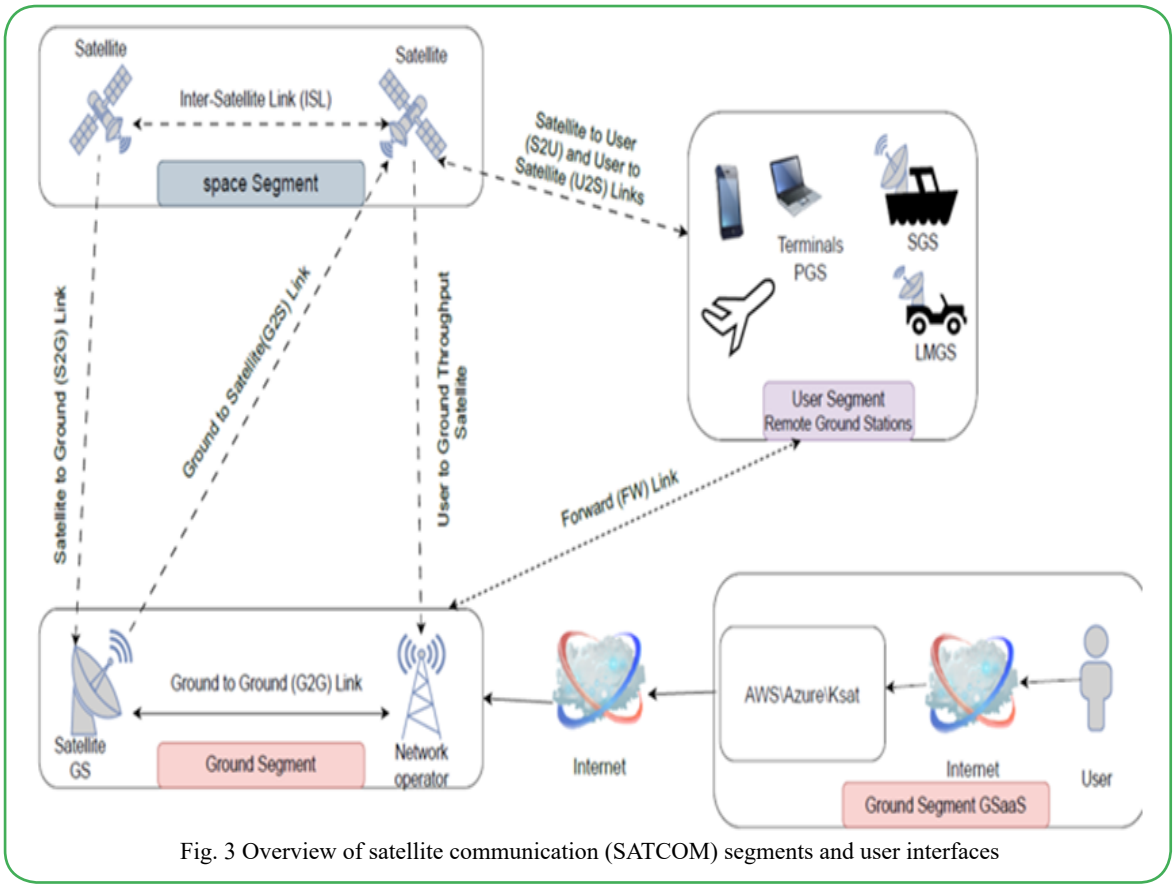

Fig. 3 Overview of satellite communication (SATCOM) segments and user interfaces

The threats to LEO satellites has been analyzed in connection with adversaries' capabilities. These can be extended to the military field.

The adversaries' capabilities in LEO

The following scheme [1] sketches partially the adversaries' resources for the compromise of the system.

We can observe that capabilities involve typologically different resources as related to the RF, tools, infrastructures, positioning and insider operators. These should be managed in specific contexts.

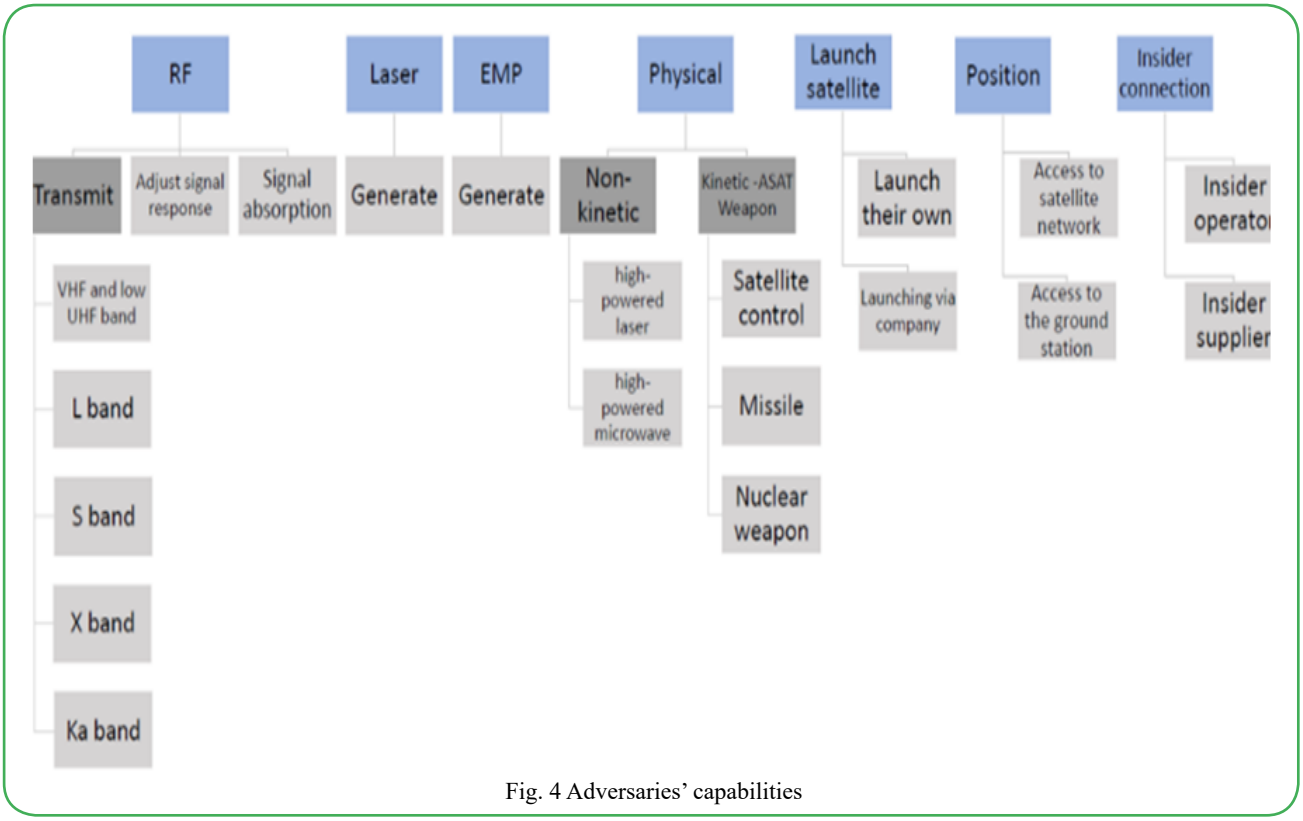

Fig. 4 Adversaries' capabilities

MITRE taxonomy for LEO satellites

In the analysis of satellites vulnerabilities and attacks, MITRE proposes [11] an extension and application of the kill chain descriptive approach that includes specific tactics and techniques in a 'taxonomic' structuring that might be partially included in our description of the domain incidents' procedures.

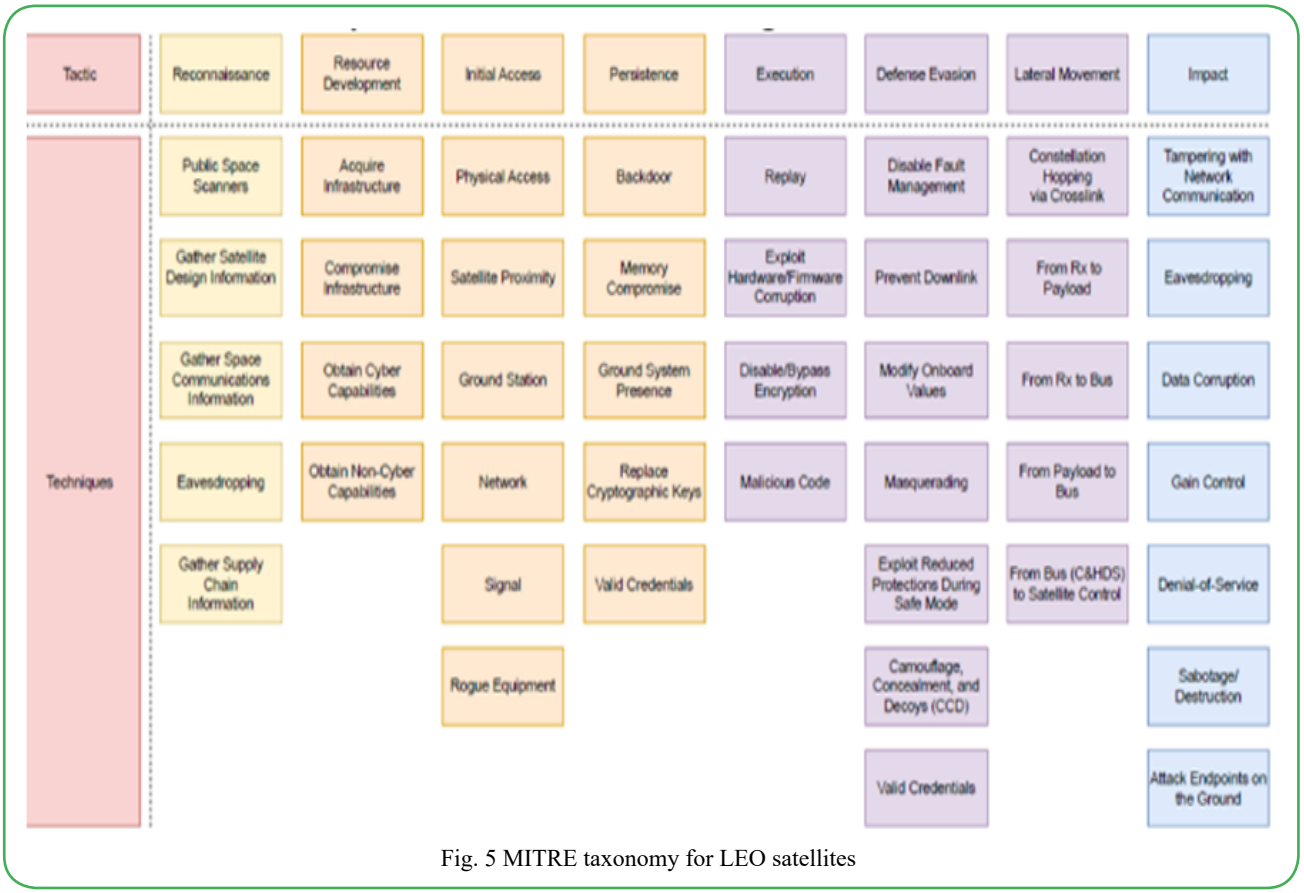

Fig. 5 MITRE taxonomy for LEO satellites

MITRE taxonomy attack analysis

An application of the MITRE taxonomy to a VIASAT attack is represented in the following scheme [1].

As we can see, the taxonomy is related to different phases of an attack and imply the correlation of the taxonomic entities listed as techniques. Each tactic and technique, if considered as entities,

should therefore be defined and related vertically and transversally, according to specific properties and attributes.

Coming to the Pragmema POC model I shall start to outline the process of definition of the domain components and the vunerability assessment (VA), to begin with.

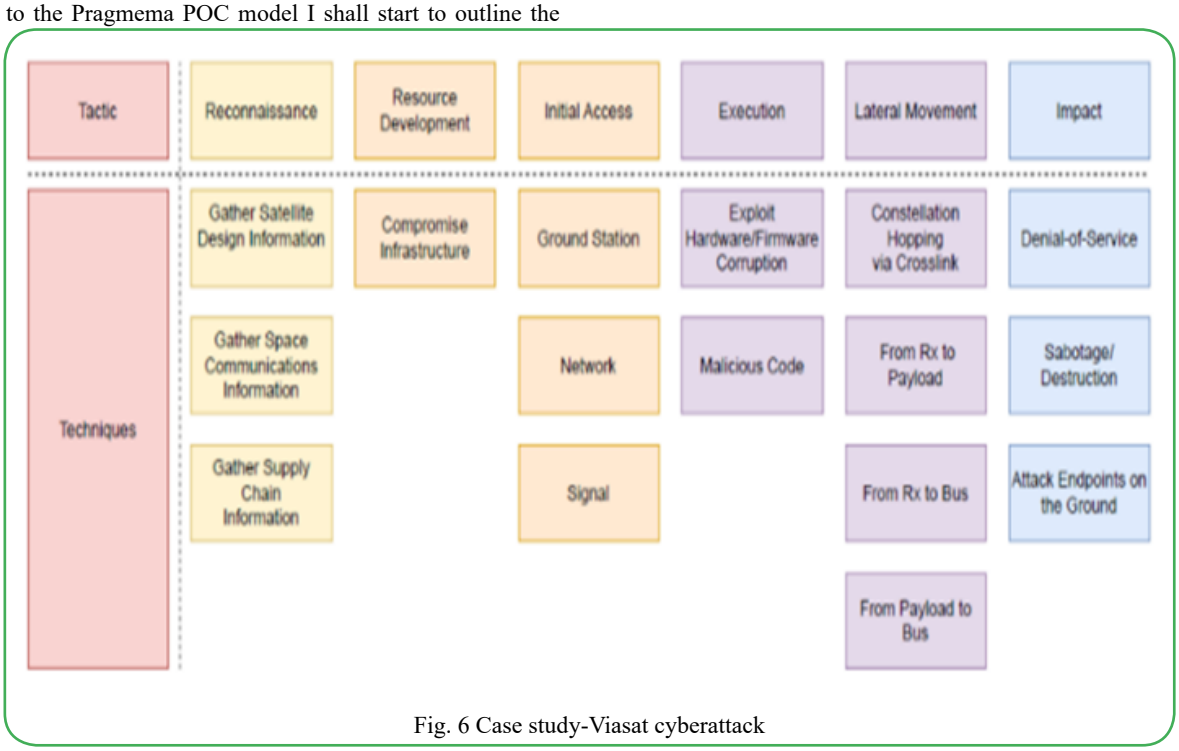

Fig. 6 Case study-Viasat cyberattack

Threat intelligence, information sharing, incident reporting: the POC AI military satellites defense solution

A basic question has to do with methodological criteria for an AI approach to satellites security defense solutions.

As far as theoretical and methodological assets to be pursued, we need to develop:

- satellites security knowledge bases through AI models and representation standards. These to be fed with data learned and tested through advanced machine learning
- satellites domain and subdomain military satellites security representation of entities, relationships, interactions in military satellite communication channels, defense systems and defense protocols
- analysis of system functionalities, vulnerabilities, threats, attacks, impacts, current defense solutions

AI development for the analysis ovulnerabilities: IoCs and IoAs analysis and integration

The analysis of vulnerabilities (VA) in the satellites cybersecurity context should allow for a preventive and predictive application, taking into consideration the whole of common technological defense tools as presented below. These release IoCs and IoAs that need classification, rules and integration solutions.

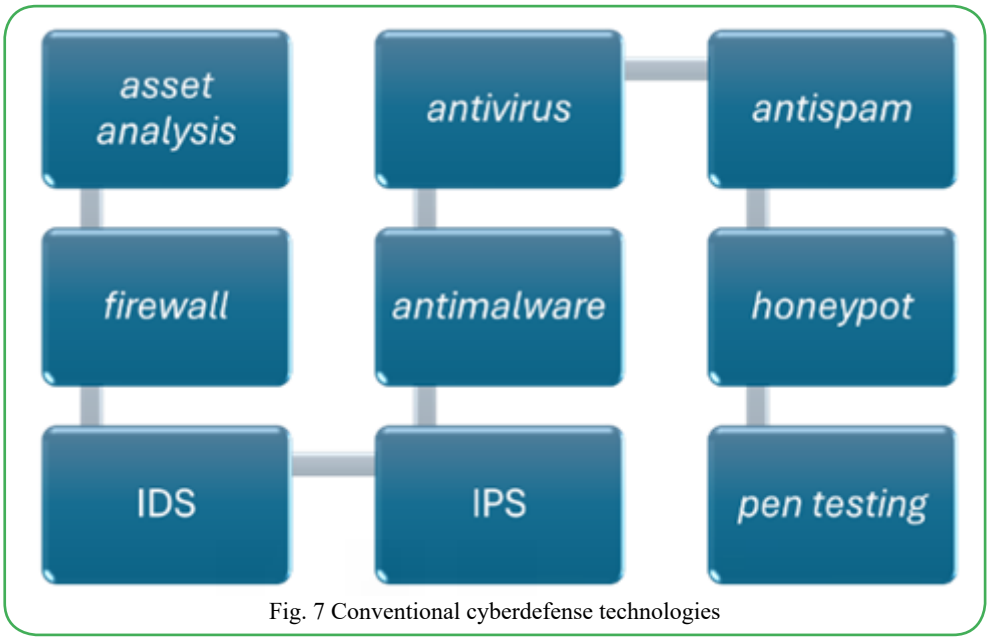

Fig. 7 Conventional cyberdefense technologies

The scheme below recalls the application in the Pragmema POC of a first IoCs integration model [4] in the cybersecurity domain representation for incidents.

The perspective of the methodological application of integration rules must be specifically customised for the satellites vulnerability sub-domain.

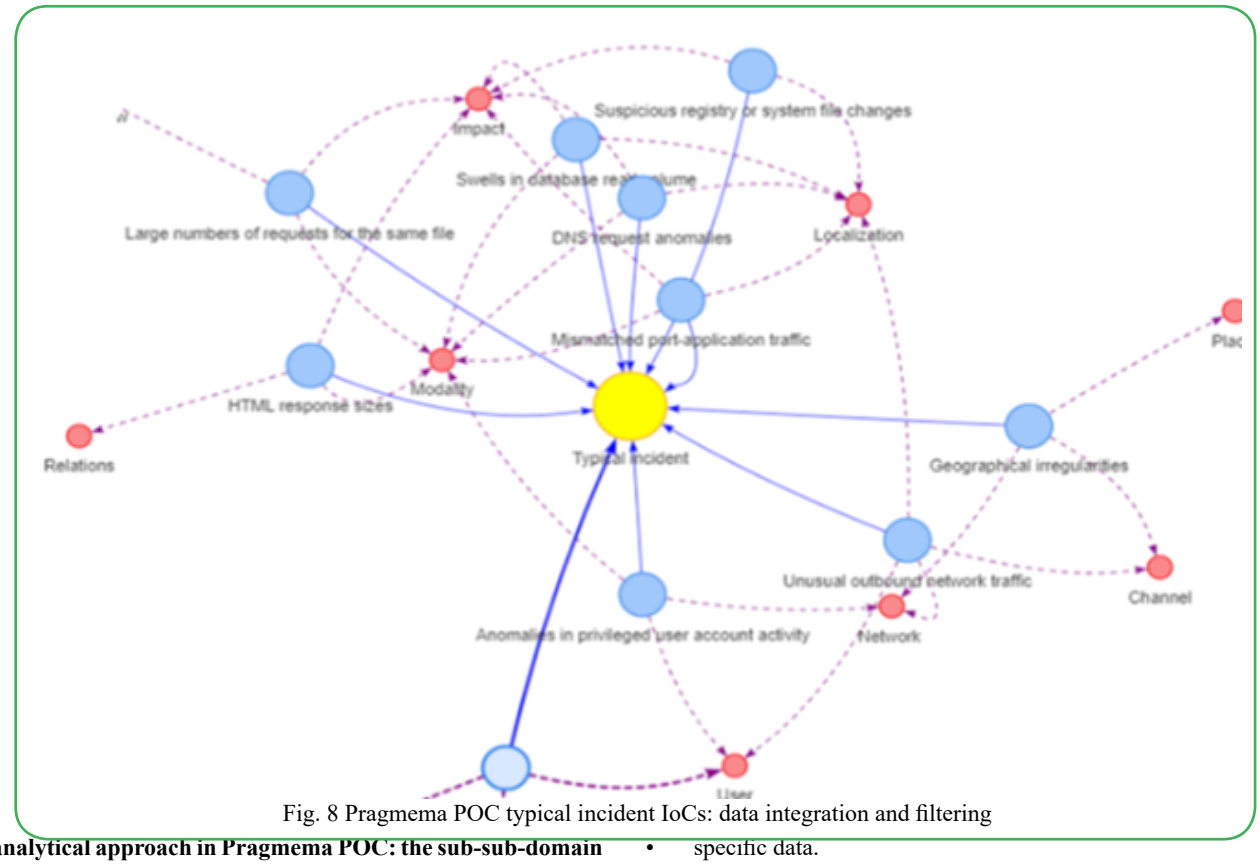

Fig. 8 Pragmema POC typical incident IoCs: data integration and filtering

The analytical approach in Pragmema POC: the sub-sub-domain of vulnerability pentesting in the satellites domain

The analysis of dynamic incoming data as related to satellites security can refer to two data sources: data related to the range of technological defense systems and data related to vulnerability assessment (VA) in pentesting and similar checks.

The mandatory application of VA techniques to cybersecurity such as pentesting and redteaming, for insstance, according to recent European legislation, allows for a preliminary representation of vulnerabilities in the cybsescurity context.

The representation requires:

- the definition of the sub-subdomain entities of the penetration testing
- the organization of logical-semantic relationships of the entities
- the machine memorization/ acquisition of pentesting nodes and links of pentesting
- specific data.

The prospective development of a longitudinal platform of pentesting data requires further definition of fields to be used for the preliminary manual data acquisition.

A longitudinal check-board on the evolution of vulnerability flaws in satellites cybersecurity should then be related to the range of cybersecurity platforms and devices such as the ones mentioned above: firewall, IDS, IPS, antimalware, antivirus, etc.

Finally, the vulnerability assessment deriving from the processing of data related to defense devices would benefit of an advanced machine learning model such as a DNNML for the automatic interpretation of data in a preventive predictive fashion.

What follows is the graph representation taxonomy of the VA subdomain.

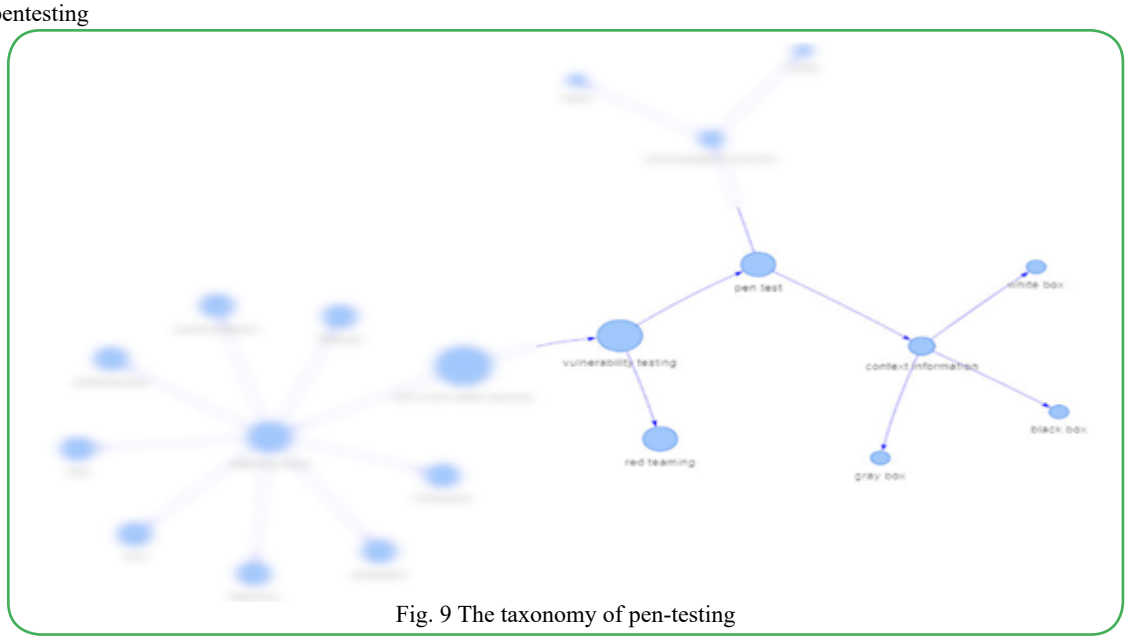

Fig. 9 The taxonomy of pen-testing

The graph relates VA to two taxonomic suites of entities corresponding to two methodological approaches: pentesting and redteaming, on one side; on the other, VA is related to the range of security devices of the system and implied IoCs, IoAs.

Entities of the methodological approach correspond to variables such as black box, white box, gray box and preliminary information in pentesting, for instance. As applied to satellites security, what is specifically interesting is the elaboration of a structured analytical check-list derived from preliminary analysis of the system: groundsystems, payload, satellites technology, satellites interactions, etc. The specification of the pentesting variables is then related to data deriving from the technological tools used for pentesting and records as data sources.

Penetration testing, as a component of a wide range of vulnerability assessment methods, can be related to other VA methodologies. The pen-testing activity as vulnerability analysis is related to the domain of satellites security.

The satellites security domain representation as developed preliminarly by Pragmema POC includes the analysis of threats, attacks and impacts confronted with present solutions in defense systems.

Security systems in military satellites

The need for a functional representation of security systems in the military context is strongly solicited by cyber and non cyber-related missile and satellites incidents.

In a specific reconstruction of cyber-related missile and satellite incidents [12], the typology of causes is articulated into human errors, system malfunctioning and intentional targeting, as synthesized by the following table.

Year	Human error	System malfunction	International targeting
1962	Moorestown missile false alarm		
1979	Exercise tape insertion and false missile warning		
1980		Typographical computer errors and false missile reading	
1983		Oko early-warning radar malfunction	
1997/98			ROSAT satellite failure
2010		Computer hardware failure at Warren Air Force Base	
2018	Hawaii false missile alert		US satellite network infiltration
2022			Viasat KA-SAT cyberattack Cyberattacks and missile strikes on infrastructure in Ukraine Roscosmos satellite compromise Starlink jamming and disruption
2023			Russian media false missile alerts Dozor-Teleport cyberattack

Table 1. Cyber-related missile and gsatellite incidents,1962-2023

The table reports incidents in a time lapse extending from 1962 to 2023. The availability of data would allow for a structured analysis of attacks-incidents.

Coming to the architectural solution proposed by the POC platform for the definition of the military domain of satellites security, our approach has required the following specifications:

- satellites typologies: the missions, the objects (vehicles, ground stations, etc.)
- the orbits
- the analysis of the functionalities in the military satellite communication systems
- the analysis of threats
- the analysis of attacks
- the impacts of attacks
- the analysis of the current technological solutions of the military aerospace defense in the satellite domain.

I shall briefly outline the main entities of the domain of the satellites security system, starting with defense functionalities in the use of the military satellites communication.

Defense functionalities

Defense functionalities in military satellites security may be summed up as follows:

- satellites operations continuity
- satellites physical protection
- satellites communication protection
- satellites data protection.

These are the taxonomic graph representations of the four variables.

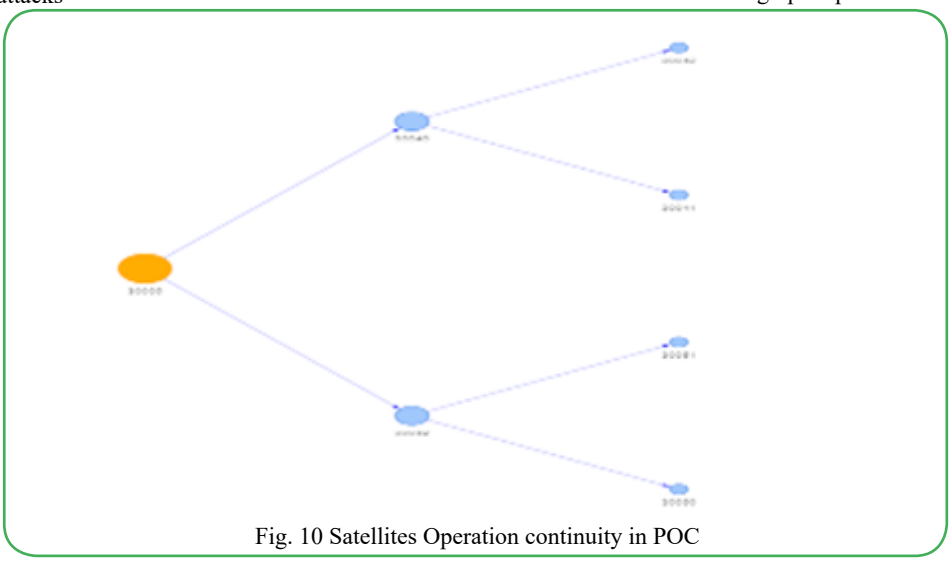

Fig. 10 Satellites Operation continuity in POC

Fig. 11 Satellites Communication protection in POC

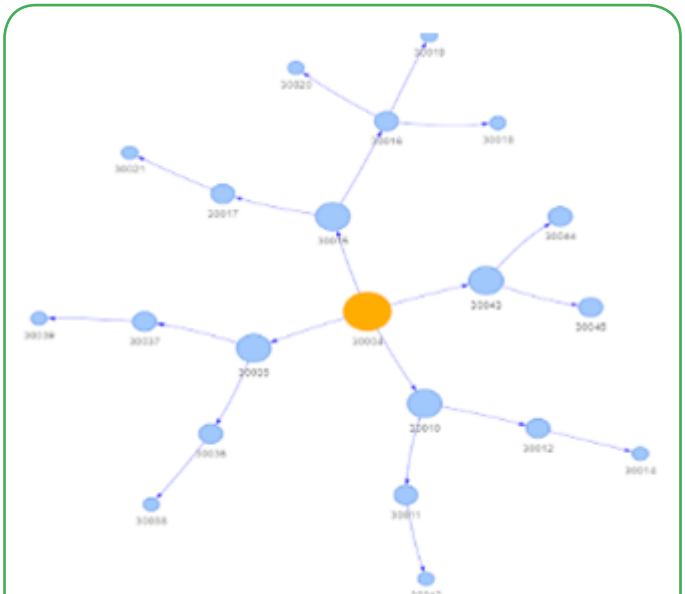

Fig. 12 Satellites Data protection in POC

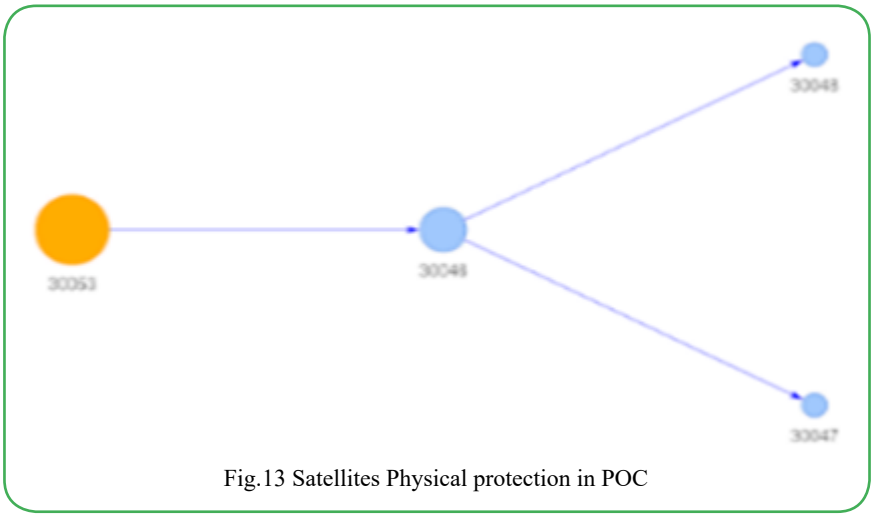

Fig.13 Satellites Physical protection in POC

Satellites defense functionalities and the security system

The analysis of the security system related to the above mentioned functionalities is as follows.

As we can see, the ontological taxonomic structure of the graph representation of the satellite security system includes different classes/entities articulated into the four levels of satellites functionalities (F).

Fig.14 Satellites security system

The second level entities of the four general functionalities of the security system contain third and fourth level entities defined according to three conceptual specifications of entities as derived from a semantic vocabulary: in particular, three properties are specified according to logical semantic criteria. The properties concern: the functions of the communication system (F), the security activity (W) and the operational tool (H).

As an istance, the communication protection (F4), 2nd level class, includes COMSEC (f1), satellites transmission security (f2) and antijamming (f3).

COMSEC (f1) includes two types of activity: secure voice/secure data (W1) and redundancy failover (W2).

Secure voice/secure data (W1) includes end to end cryptography (w1H1) while redundancy failover (W2) includes redundancy systems (H2a) and failover mechanisms (H2b).

These taxonomic links are furtherly related to transversal entities such as threats and incidents, in particular.

The second component of the ontology/taxonomy: threats.

The threats representation

The typology of threats includes a basic distinction between cyberattacks and electronic warfare entities on one side and non cybersecurity entities such as physical and environmental entities on the other.

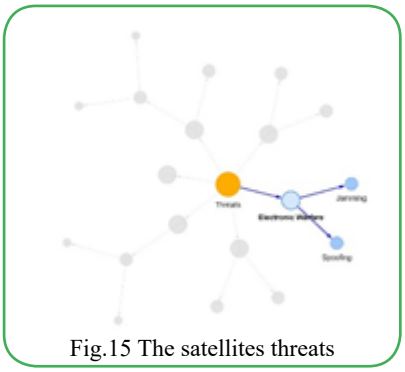

Fig.15 The satellites threats

As an instance, 2nd level class threats include the entity 'electronic warfare' as a third level. Electronic warfare includes two specific entities: jamming and spoofing. Threats are then related to attacks impacts.

A comparative analysis of attacks variables and attacks impacts

According to Brandon Bailey, in the Aerospace Report prepared in 2021 for the U.S. Government Agency, "Attacks can occur from the mission's own ground infrastructure, adversaries' ground infrastructure, a spacecraft, or via a hardware or software supply chain implant. While the likelihood of each attack path varies depending on adversaries' capabilities, intent, and engineering difficulty, using defense-in-depth principles alongside risk management strategies will aid in countering threats" [13].

Translated operationally, the question of management strategies implies some sort of knowledge representation. In my perspective, the correlation of the security system with attacks impact is contextualized into a general attack variables presentation. In order to appreciate the data correlation, we are to analyse the comparison of attack variables.

A first specification of variables would include modality of attacks, typology of cyberattacks and RF attacks such as jamming and spoofing.

Modality	Cyber-Attacks	Jamming	Spoofing
Target	Software, networks, data, control systems	Radio frequency(RF) communication signals	Rf communication signals
Layer of Attack	Digital/software layer	Physical/radio frequency layer	Physical/radio frequency layer
Method	Hacking, malware, DoS attacks, phishing	Broadcasting disruptive signals on RF band	Sending false signals mimicking legit ones
Primary Objective	Compromise system integrity, steal data	Disrupt communication, cause signal loss	Deceive system by faking data or signals
Impact	Data corruption, unauthorized access, control	Loss of service, degraded signal quality	Misleading data, navigation errors
Defense Mechanisms	Encryption, firewalls, multi-factor authentication	Frequency hopping, directional antennas	Signal authentication, encryption
Scope of Disruption	Potentially broad(system-wide disruption)	Limited to the communication link	Limited to specific communication links

Table 2. Attacks variables

The listed entities are related in the overall security and threats analysis.

In the following graph, satellites attacks impacts are represented as follows.

Fig.16 Satellites attacks impact

To conclude this complex partial ontological analysis of the satellites attacks sub-domain we can include components such as threat actors, attacks techniques, attack vectors as implied in the POC cybersecurity Platform.

The preliminary ontology of satellites security appears as follows.

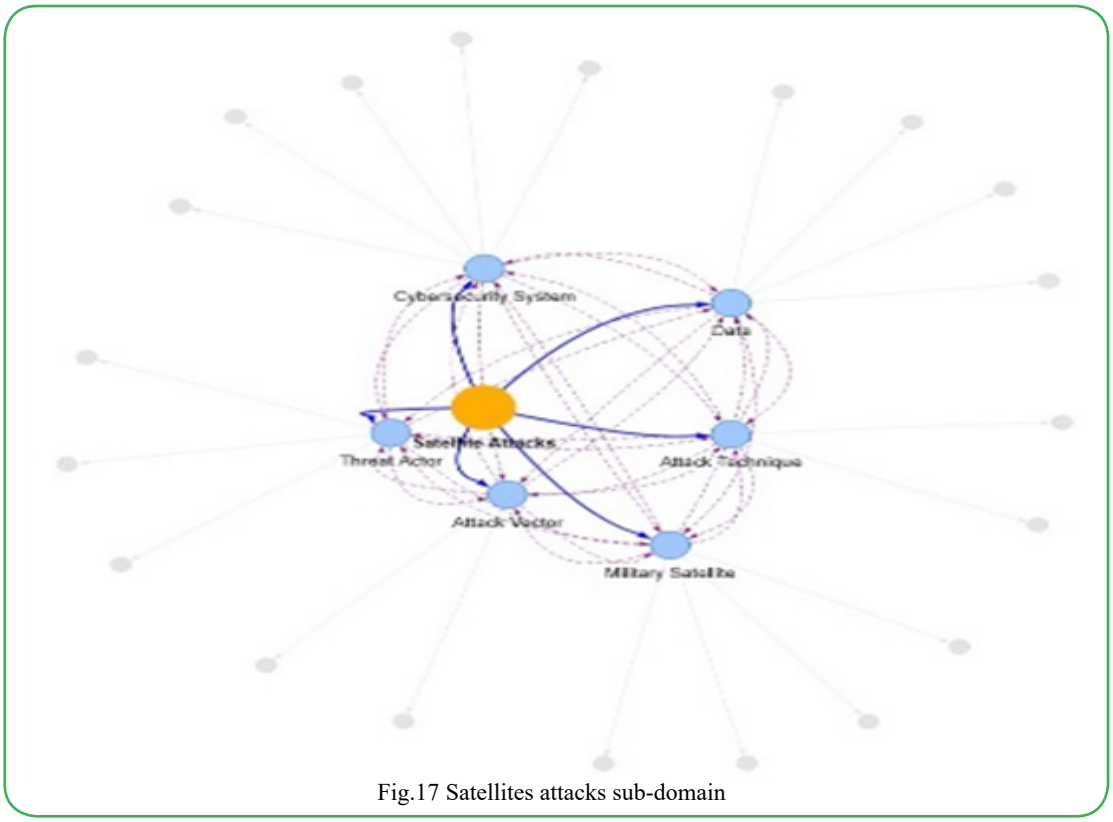

Fig.17 Satellites attacks sub-domain

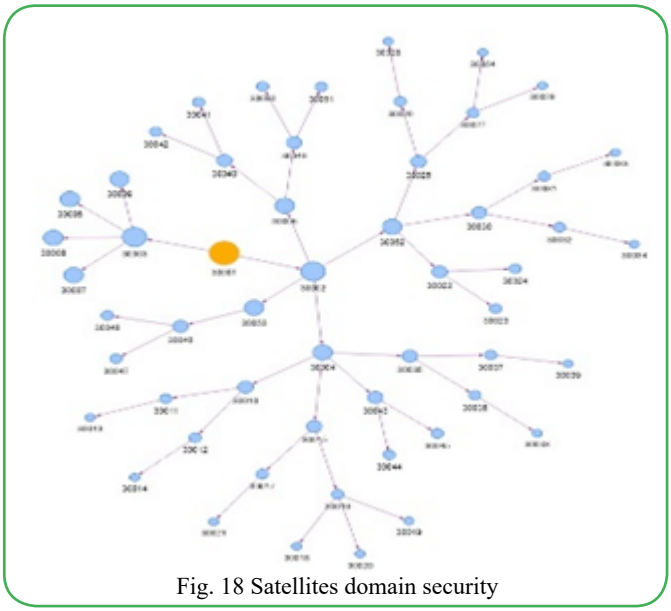

Fig. 18 Satellites domain security

Conclusion

The AI ontology of military satellites security will be implemented by analytical data as specified by the diverse security components and furtherly related to the general ontology specifications at the upper, middle and domain levels of the POC platform.

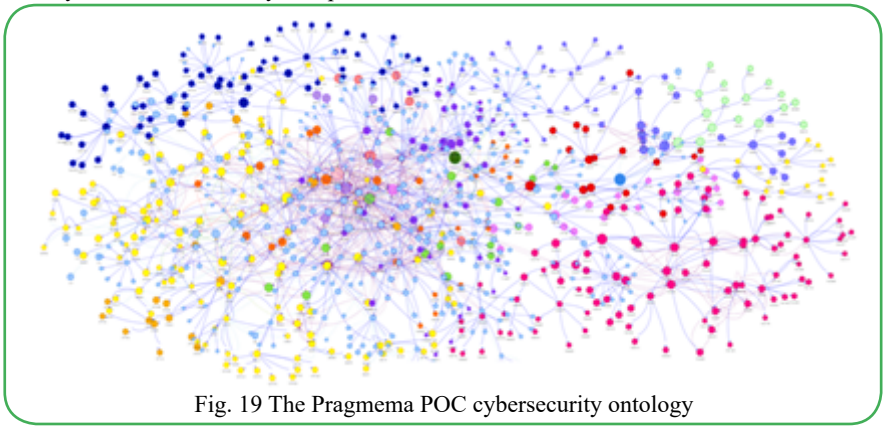

Fig. 19 The Pragmema POC cybersecurity ontology

The POC satellites security domain can represent an overall container for diverse taxonomies and ontologies in an AI frame.

Conflict of Interests: The author declares that there are no conflicts of interest.

Reference

1. Peled, R., E. Aizikovich, E. Habler, Y. Elovici, A. Shabtai, (2023). 'SoK: Evaluating the Security of Satellite Systems'. https://arxiv.org/abs/2312.01330, 2023
2. Zhang, Y, S., & Zhao, J. He, et al., (2024). 'Satellite Internet security: requirement, current status and trends'. *Journal of Cybersecurity, 2024, 2*(4): 2-17 https://doi.org/10.20172/j.issn.2097-3136.240401
3. Yue, P., J. An, J. Zhang, J. Ye, G. Pan, S. Wang, P. Xiao, and L. Hanzo,(2023).“Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead”. arXiv:2201.03063v3 [eess.SP] 19 Jul 2023
4. Zuanelli, E., (2022). 'Cybersecurity ontology and defense solutions: the POC platform'. Science Direct, Procedia. *Computer Science, 205*. 300–309
5. Parmalee, M. C., (2010).'Toward an Ontology Architecture for Cyber-Security Standards', STIDS, MITRE
6. Obrst, L., P. Chase, R. & Markeloff, (2012). 'Developing an ontology of the cyber security
7. Booth, H. and C. Turner, (2016). 'Vulnerability Description Ontology (VDO)', Draft NISTIR 8138
8. http://oval.mitre.org/repository/,http://measurablesecurity.mitre.org/
9. Harrison, J., Y. Wood, Goessler, et al., (2022). 'Space threat Assessment', Center for Strategic&InternationalStudies. https://newspaceeconomy.ca/wpcontent/uploads/2022/11/harrison_spacethreatassessment2022_web_v3-compressed-1.pdf
10. Scholl, M., T. Suloway, 2023. NIST IR 8270. 'Introduction to Cybersecurity for Commercial Satellite Operations'. https://csrc.nist.gov/News/2023/cyber-for-commercial-satellite-operations
11. E. Blake, A. Strom, D. Applebaum, et alii, (2018). 'Mitre att&ck: Design and Philosophy”, *Technical report*, The MITRE Corporation.https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy
12. Saalman, L., L. Saveleva Dovgal and S. Fei, (2023). 'Mapping cyber-related Missile and satellite incidents and confidence-building measures'. *SIPRI*, Insights on Peace and Security
13. B. Bailey, (2021). Cybersecurity Protections for Spacecraft: A Threat Based Approach, AEROSPACE REPORT NO. TOR-2021-01333-REV A