VII CONFERENZA NAZIONALE

Sicurezza cibernetica e aerospaziale

Conferenza connessa al Master

«Competenze digitali per la Protezione dei Dati, la Cybersecurity e la Privacy»

Università degli Studi di Roma «Tor Vergata»

Roma, Palazzo Wedekind, Piazza Colonna 366

7 aprile 2025

La ‘nuova sicurezza’ tra *cybersecurity* e *aerospace security*

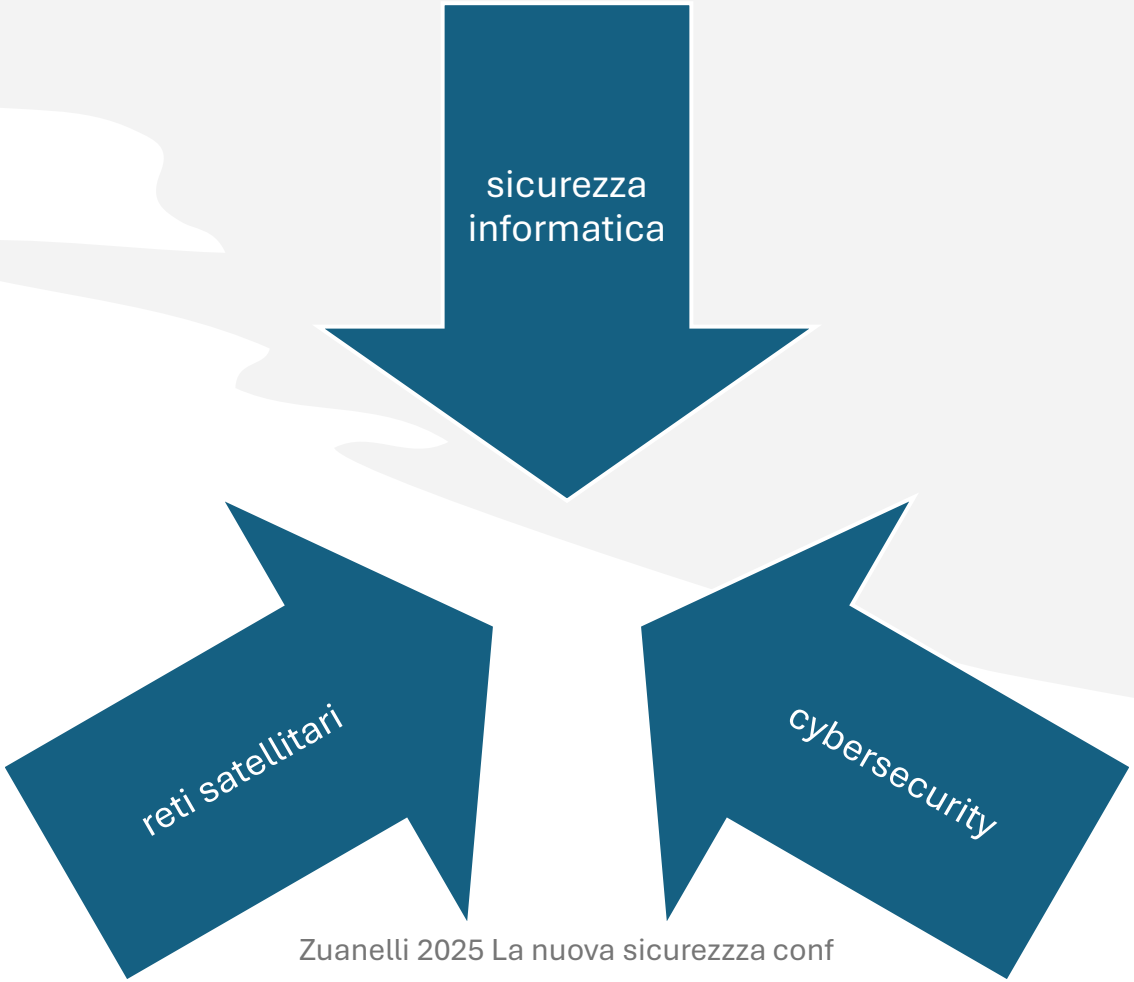
Elisabetta Zuanelli

Coordinatore del Partenariato per il Piano di formazione in Cybersecurity, Cyberthreat e Privacy

Professore Emerito, Università degli Studi di Roma «Tor Vergata»

Esperto ONU e NATO di Intelligenza artificiale

Dal ‘vecchio’ al ‘nuovo’: dalla sicurezza informatica, alla *cybersecurity*, alla sicurezza aerospaziale



Le cause dell'insicurezza

innovazione tecnologica (intelligenza artificiale, reti 5g, quantum)

proliferazione delle **app**

moltiplicazione delle piattaforme (istituzionali, aziendali, *business*, *ecommerce*, *educational*, politiche, **social**, etc.)

motori di ricerca, app e **gestione dati personali e istituzionali**

reti e sistemi di rete

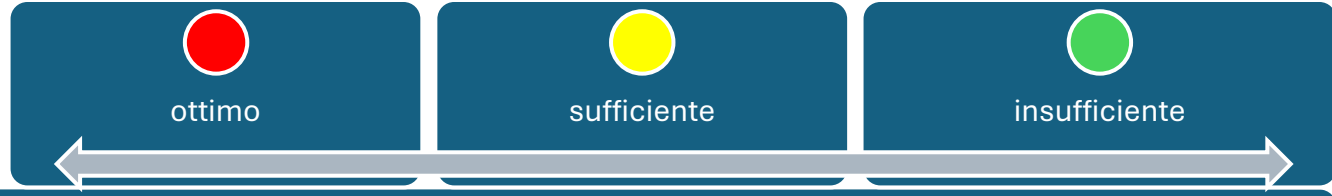
piattaforme di servizi: **cloud**

tecnologie *mobile*

crescita esponenziale delle **masse di dati** che circolano

le finalità **economiche, sociali e geopolitiche** (inclusa la ***cyberwarfare***)

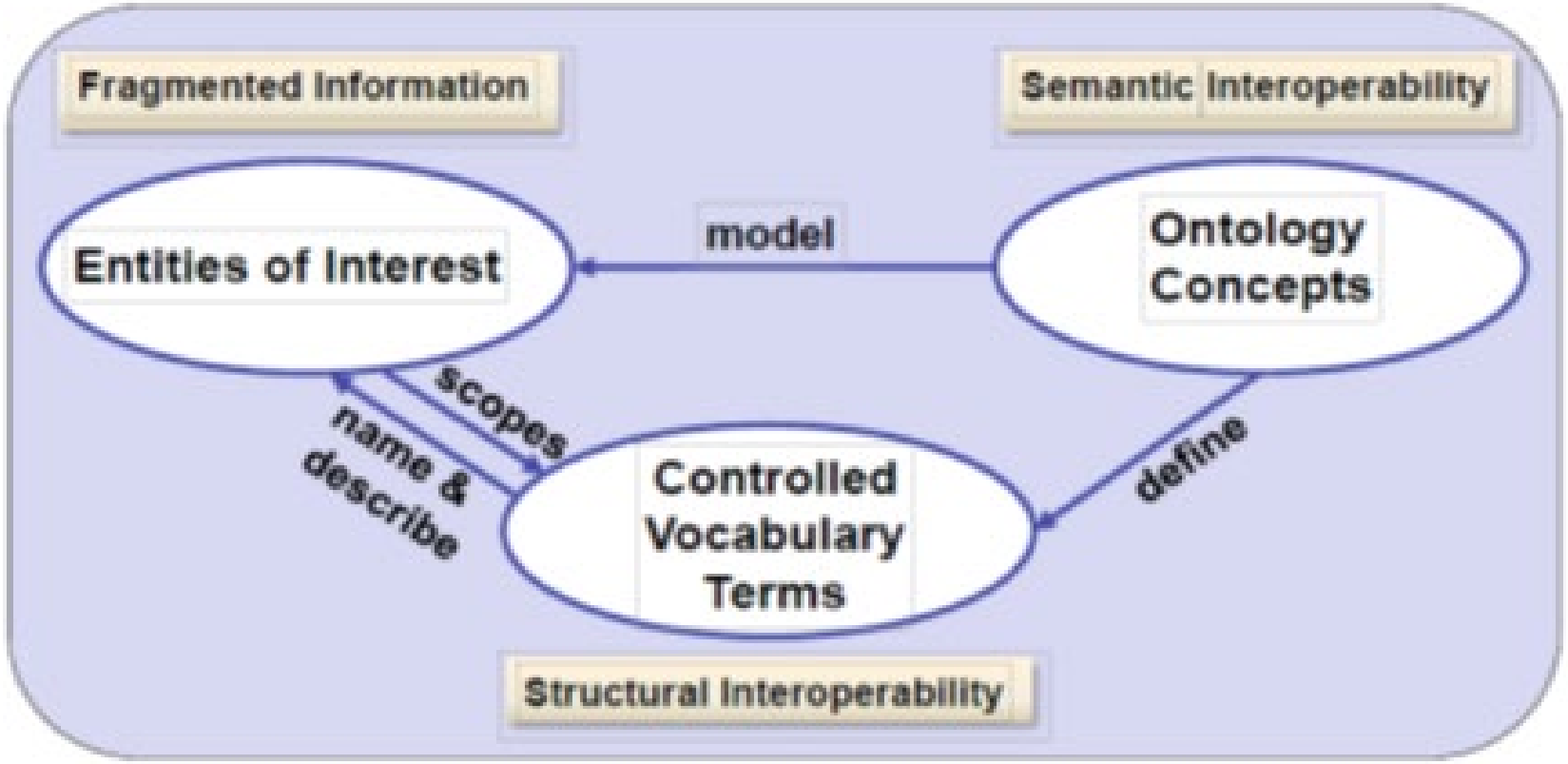
La difesa: i soggetti



I *vendor* di prodotti e servizi digitali	+	+/-	
I *vendor* di connettività	?	?	?
Le aziende della sicurezza		+/-	
Le aziende enti istituzioni soggetti pubblici e privati utenti			-
I sistemi di difesa -		+/-	
Le tecnologie di difesa		+/-	
I soggetti istituzionali: agenzie, autorità, board, etc.		+/-	
Le norme		+/-	
Gli standard		?	

2010: lo scetticismo *cybersecurity* MITRE e la ‘nuova proposta’di analitica dei dati

Semantic and Structural Interoperability



MITRE

Concettualizzazione, terminologie, entità, relazioni logico-semantiche, rete di entità

- dati
- basi di dati
- informazioni
- concettualizzazione e algoritmi
- corpora di dati/ informazioni/concetti
- contestualizzazione dei dati: dominio, entità, relazioni logico-semantiche
- classificazioni e tecnologie (*data set*, *embedding*, *layer*)
- modelli di classificazioni: tassonomie/ontologie
- modelli di intelligenza artificiale
- tecnologie mach*ine learning*: modelli inferenziali

Le piattaforme/*repository* e i modelli di ontologia e tassonomia dei dati della ‘sicurezza’ cibernetica: ma come si costruisce un’ ontologia o una tassonomia? Cos’è una classificazione?

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

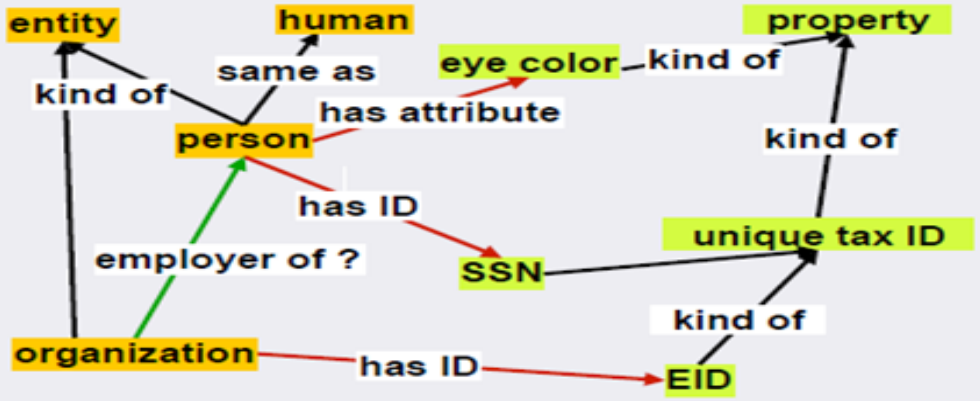
MISP: Malware Information Sharing Project

http://nvd.nist.gov/,

http://oval.mitre.org/repository/, http://measurablesecurity.mitre.org/

Threat intelligence, *information sharing*, *incidents reporting*: lo storico modello ontologico per analizzare il dominio *cybersecurity* (2010)

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	

MITRE

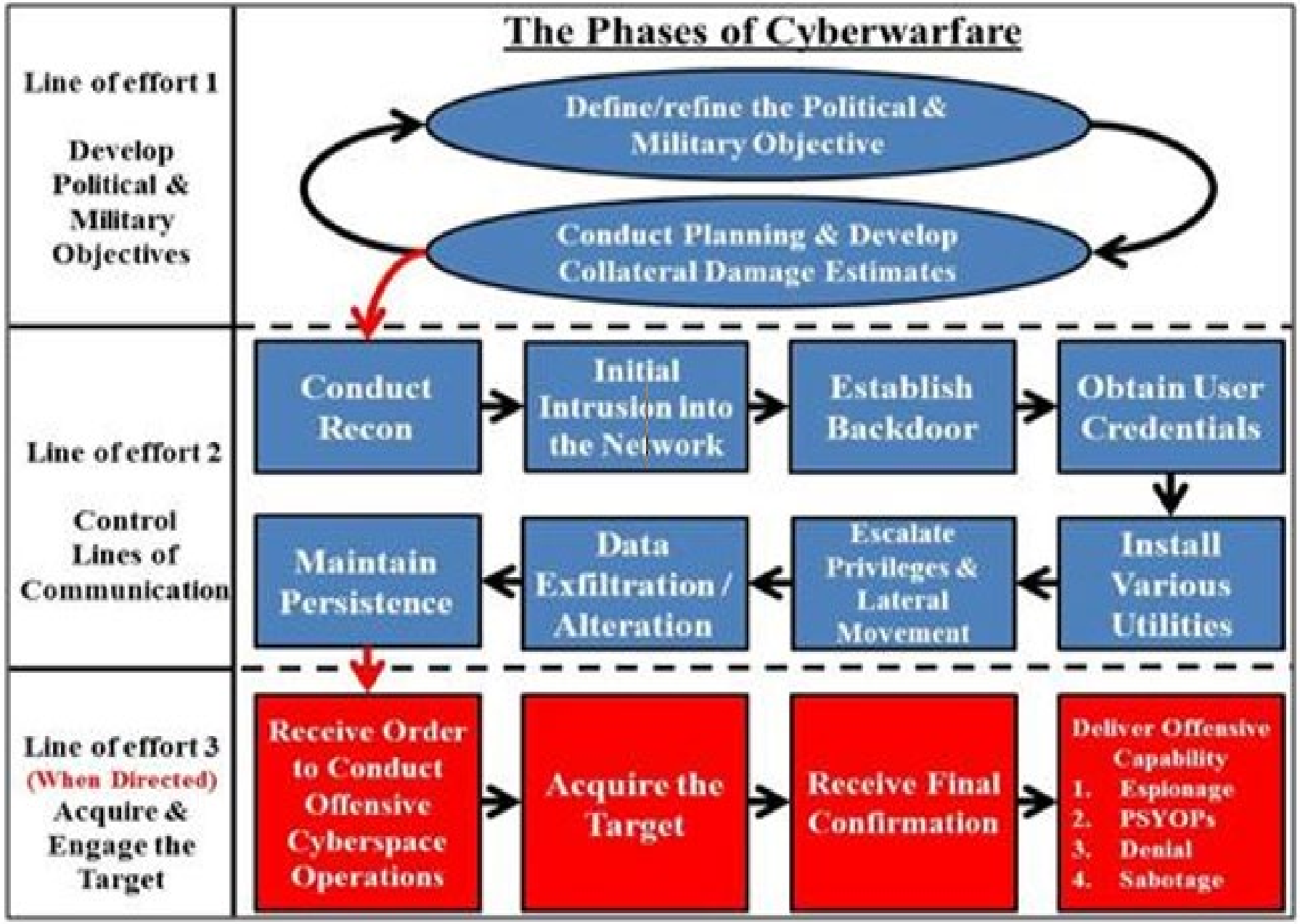
Gli attacchi e le descrizioni analitiche

la Babele terminologica

il *phishing* non è un tipo di attacco, né lo è un *ransom* o un Trojan

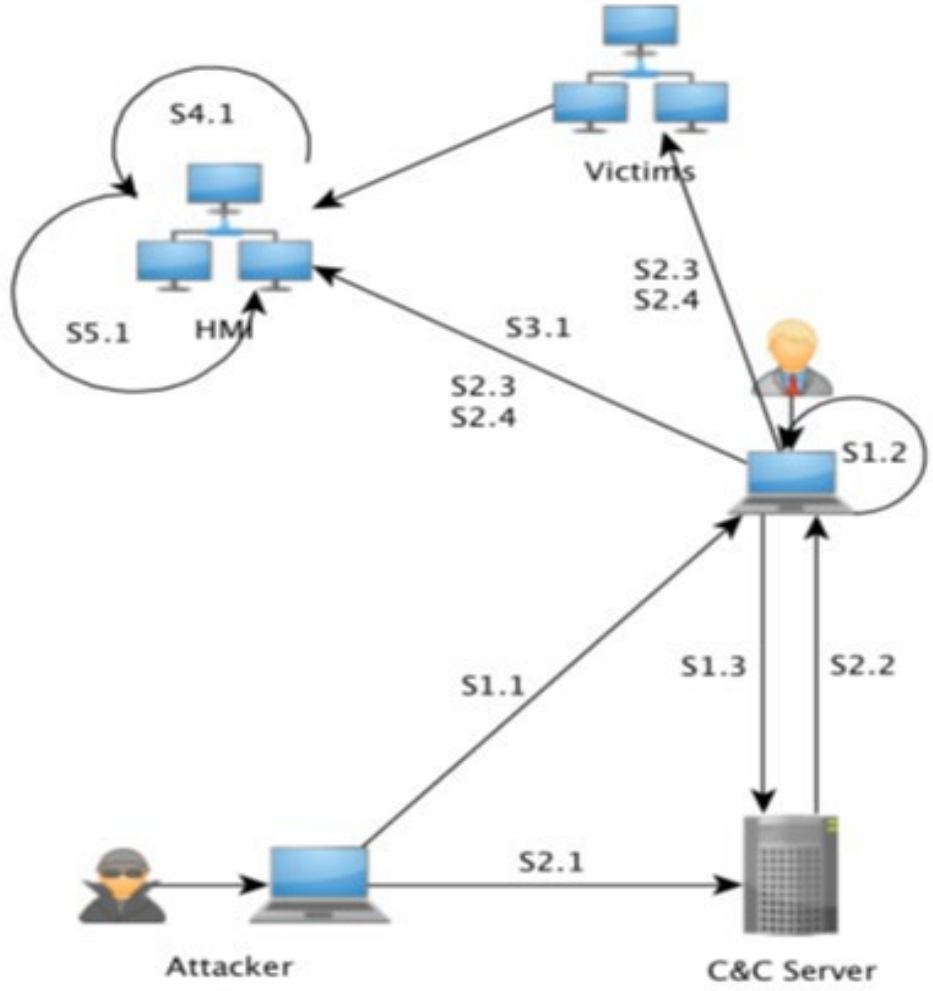
cos'è un 'attacco' come si deve analizzare e come si analizzano e classificano i dati

La storica *kill chain* ovvero l'analisi delle fasi di un 'attacco'



The Ukraine's Power Grid Incident(2015): the 'killchain' reconstruction.

The BejjngKnownsecSecurity Team analysed26 samples acquired by Tencent PC Manager Team



1.1 Attackers use Office SandWorm to carry out watering hole attacks.
1.2 Victims open the malicious file to release and execute the malicious code.
1.3 Victim hosts send basic system information to C&C servers.

2.1 Attackers control victim hosts by sending commands through C&C servers.
2.2 C&C servers take control over victim hosts to scan the internal network.
2.3 Victim hosts scan the targeted HMI devices.
2.4 Attackers use HMI remote execution vulnerability to achieve expansion within the internal network and control HMI devices.

3.1 Attackers implant BlackEnergy into HMI devices or victim hosts.

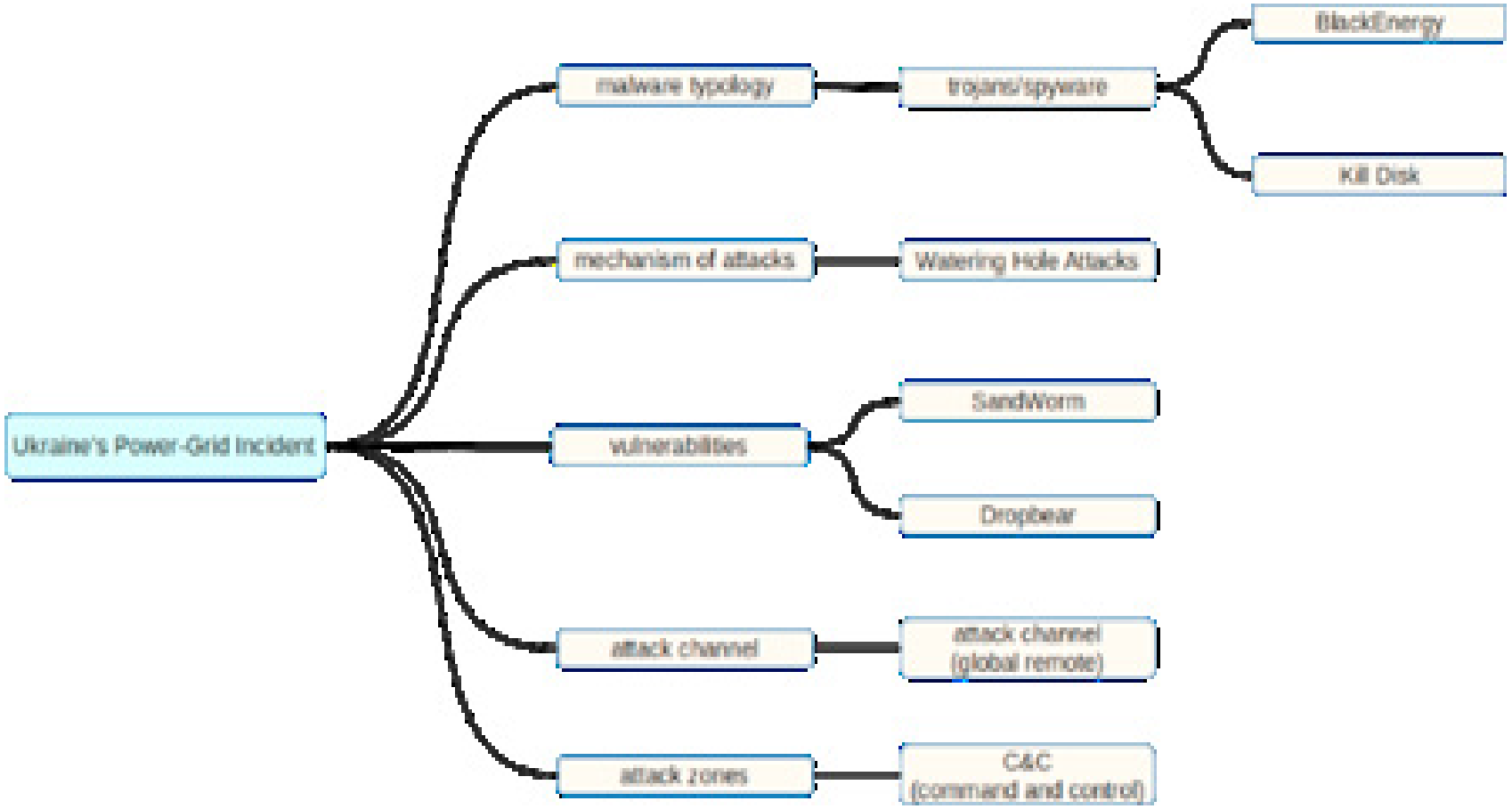
4.1 BlackEnergy loads components and starts light-weighted SSHD Dropbear, listening port 6789.

5.1 Attackers load Kill Disk components whenever possible to destroy host disks, causing the paralysis of the entire system.

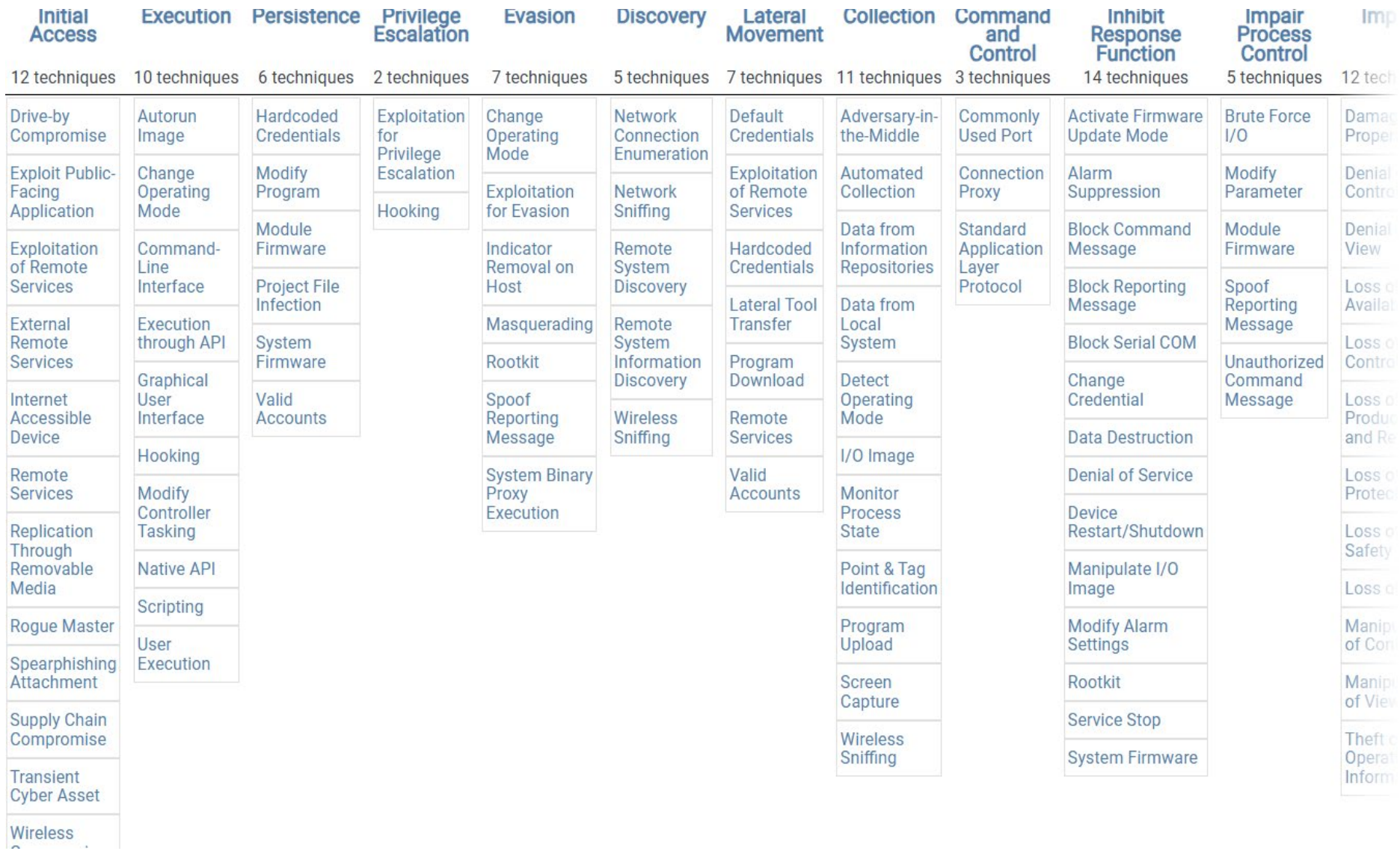
The samples

No.	SHA-1 Value of Samples	Sample Type (Main Purpose)
1	aa67ca4fb712374f5301d1d2bab0ac66107a4df1	Excel (containing macro virus)
2	166d71c63d0eb609c4f77499112965db7d9a51bb	PE32 (Dropbear server program)
3	72d0b326410e1d0705281fde83cb7c33c67bc8ca	VBS (starting Dropbear)
4	4c424d5c8cfedf8d2164b9f833f7c631f94c5a4c	PE32 (vba_macro.exe released by macro virus)
5	6d6ba221da5b1ae1e910bbeaa07bd44aff26a7c0	PE32 (damaging code)
6	8ad6f88c5813c2b4cd7abab1d6c056d95d6ac569	PE32 (damaging code)
7	16f44fac7e8bc94eccd7ad9692e6665ef540eec4	PE32 (KillDisk component)
8	f3e41eb94c4d72a98cd743bbb02d248f510ad925	PE32 (LocalServer)
9	896fcacff6310bbe5335677e99e4c3d370f73d96	PE32 (malicious program)
10	1a86f7ef10849da7d36ca27d0c9b1d686768e177	PE32 (malicious driver)
11	1cbe4e22b034ee8ea8567e3f8eb9426b30d4affe	PE32 (malicious driver)
12	4bc2bbd1809c8b66eecd7c28ac319b948577de7b	PE32 (malicious driver)
13	502bd7662a553397bbdcfa27b585d740a20c49fc	PE32 (malicious driver)
14	069163e1fb606c6178e23066e0ac7b7f0e18506b	PE32 (malicious driver)
15	84248bc0ac1f2f42a41cfffa70b21b347ddc70e9	PE32 (malicious driver)
16	be319672a87d0dd1f055ad1221b6ffd8c226a6e2	PE32 (malicious driver)
17	cd07036416b3a344a34f4571ce6a1df3cbb5783f	PE32 (malicious driver)
18	e1c2b28e6a35aeadb508c60a9d09ab7b1041afb8	PE32 (malicious driver)
19	0b4be96ada3b54453bd37130087618ea90168d72	PE32+ (malicious driver)
20	1a716bf5532c13fa0dc407d00acdc4a457fa87cd	PE32+ (malicious driver)
21	2c1260fd5ceaef3b5cb11d702edc4cdd1610c2ed	PE32+ (malicious driver)
22	2d805bca41aa0eb1fc7ec3bd944efd7dba686ae1	PE32+ (malicious driver)
23	20901cc767055f29ca3b676550164a66f85e2a42	PE32+ (malicious driver)
24	bd87cf5b66e36506f1d6774fd40c2c92a196e278	PE32+ (malicious driver)
25	c7e919622d6d8ea2491ed392a0f8457e4483eae9	PE32+ (malicious driver)
26	e40f0d402fdcba6dd7467c1366d040b02a44628c	PE32+ (malicious driver)

L’analisi tassonomica POC



MITRE ATT&CK®: il Repository tassonomico



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Imp
12 techniques	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 tech
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damag Proper
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial Contro
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss o Availa
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss o Contro
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss o Produc and Re
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss o Protec
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss o Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss o
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manip of Con
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manip of Vie
Wireless									Rootkit		Theft Operat Inform
									Service Stop		
									System Firmware		

Le tecnologie Quantum e AI e la *cybersecurity*

Quantum/AI *attacks* e Quantum /AI *defense*: il doppio vincolo

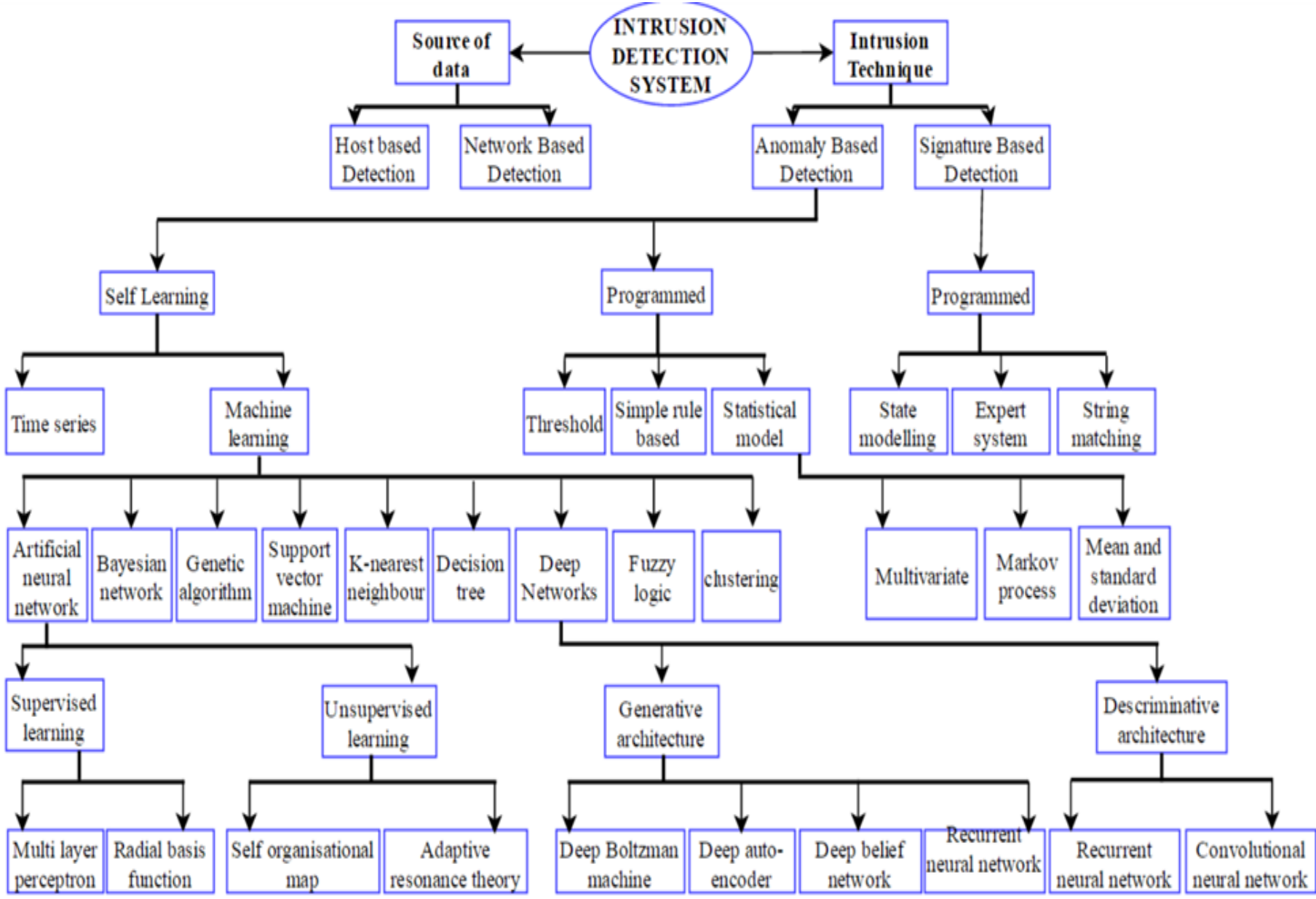
minacce

- compromissione algoritmi di crittazione
- AI *adversarial attacks*

soluzioni di difesa

- algoritmi di crittazione avanzati per la comunicazione e lo *storage*
- piattaforme AI preventive e predittive

IDS attack e AI analytics? Il *gap: i dati*



La sicurezza nel cyberspazio: il satellitare civile e militare

"Global Navigation Satellite Systems are critical to our safety on land, at sea and in the air,"
said **ITU Secretary-General Doreen Bogdan-Martin.**
"Member States should ensure the uninterrupted operation of these systems for everyone's safety and the resilience of essential services that our lives depend on."

la comunicazione satellitare tra civile e militare

il sovraffollamento satellitare

le interferenze

l’assenza di standard

tipologia di attaccanti nel militare

tipologie d’attacco nel militare

minacce, attacchi, impatti, difese

L’aerospazio e i sistemi satellitari: temi e problemi di sicurezza

Threat intelligence, *information sharing*, *incident reporting*: soluzioni algoritmiche di sicurezza AI per l'aerospazio

basi di conoscenza con modelli AI e standard di rappresentazione

rappresentazione del **dominio aeronautica, e dei sub-domini: entità, relazioni, interazioni**: canali di comunicazione satellitare militari, sistemi di difesa e protocolli di difesa

analisi delle **funzionalità del sistema**, **minacce** e **attacchi**, **impatti**, **soluzioni attuali di difesa**

Zhang, Zhao, He, et al.

Y. Zhang, 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

"the current states of security technology development" … imply the analysis of

- the **areas of node access authentication**
- **link secure transmission**
- **network security routing**.

Therefore, "the development trends of Satellite Internet security technology highlight the importance of endogenous, systematic, and **intelligent Satellite Internet techniques"**

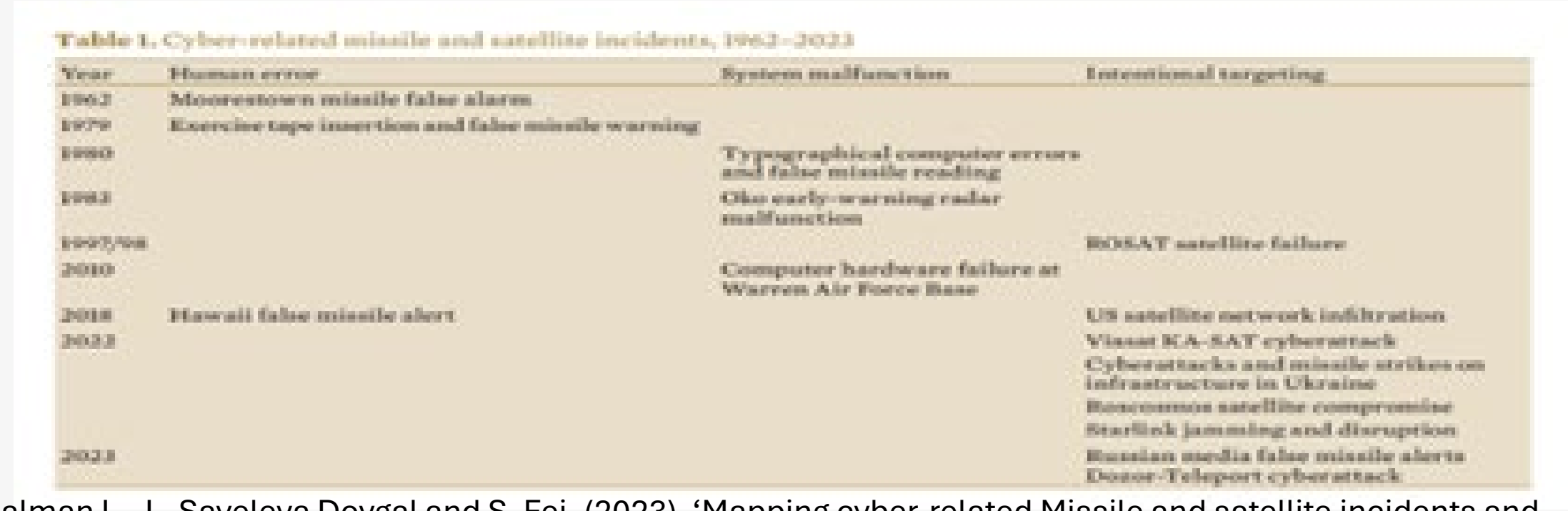


Table 1. Cyber-related missile and satellite incidents, 1962–2023

Year	Human error	System malfunction	Intentional 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
			Russian satellite compromise
			Starlink jamming and disruption
2023			Russian media false missile alerts
			Dozor-Teleport cyberattack

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

Gli incidenti e gli attacchi a missili e satelliti: errori umani, malfunzionamento di sistema, ***targeting*** intenzionale

Comunicazioni satellitari: *link*

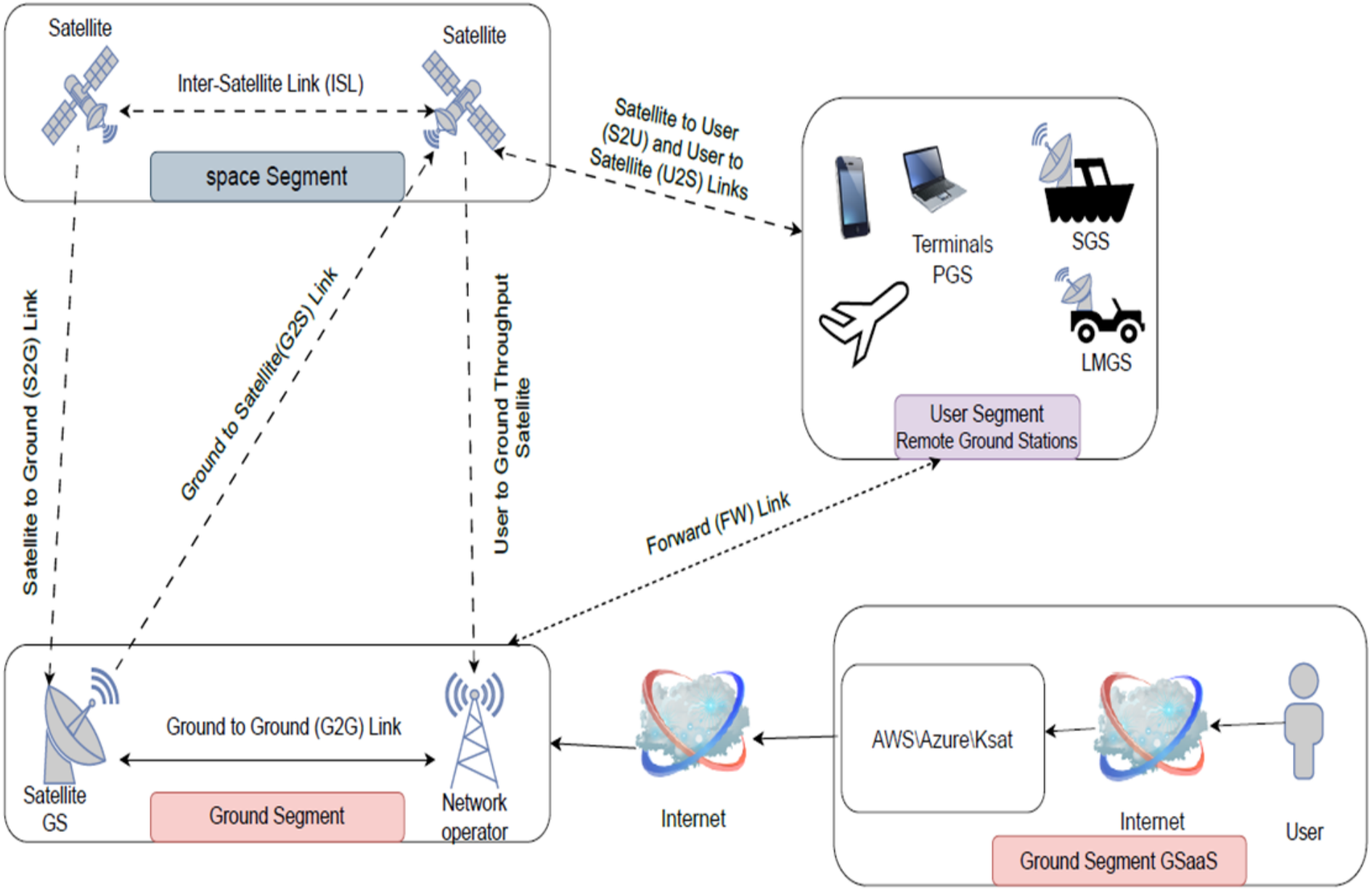


Figure 1: Overview of satellite communication (SATCOM) segments and user interfaces.

Le variabili degli attacchi: ***cyber* e non *cyber***

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

Le capacità degli avversari

R. Peled, E. Aizikovich, E. Habler, Y. Elovici, A. Shab, (2023) 'SoK:Evaluating the Security of Satellite Systems', https://arxiv.org/abs/2312.01330, 2023

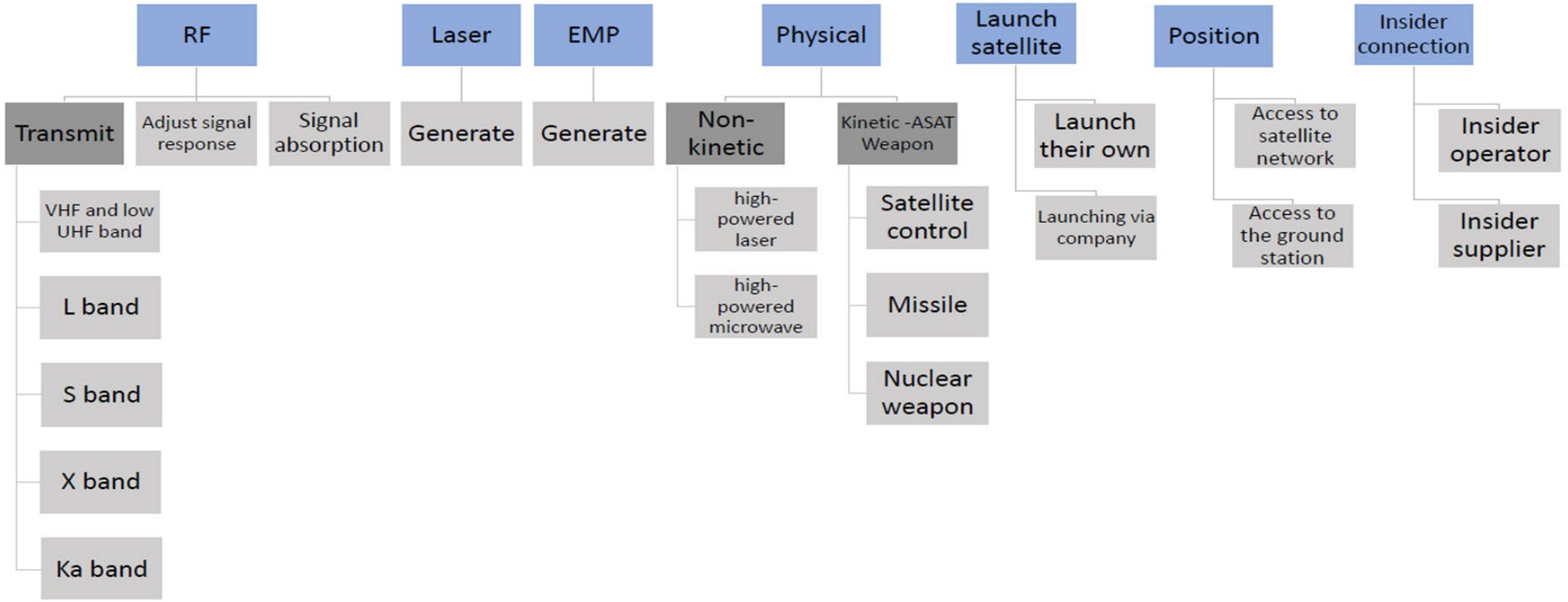
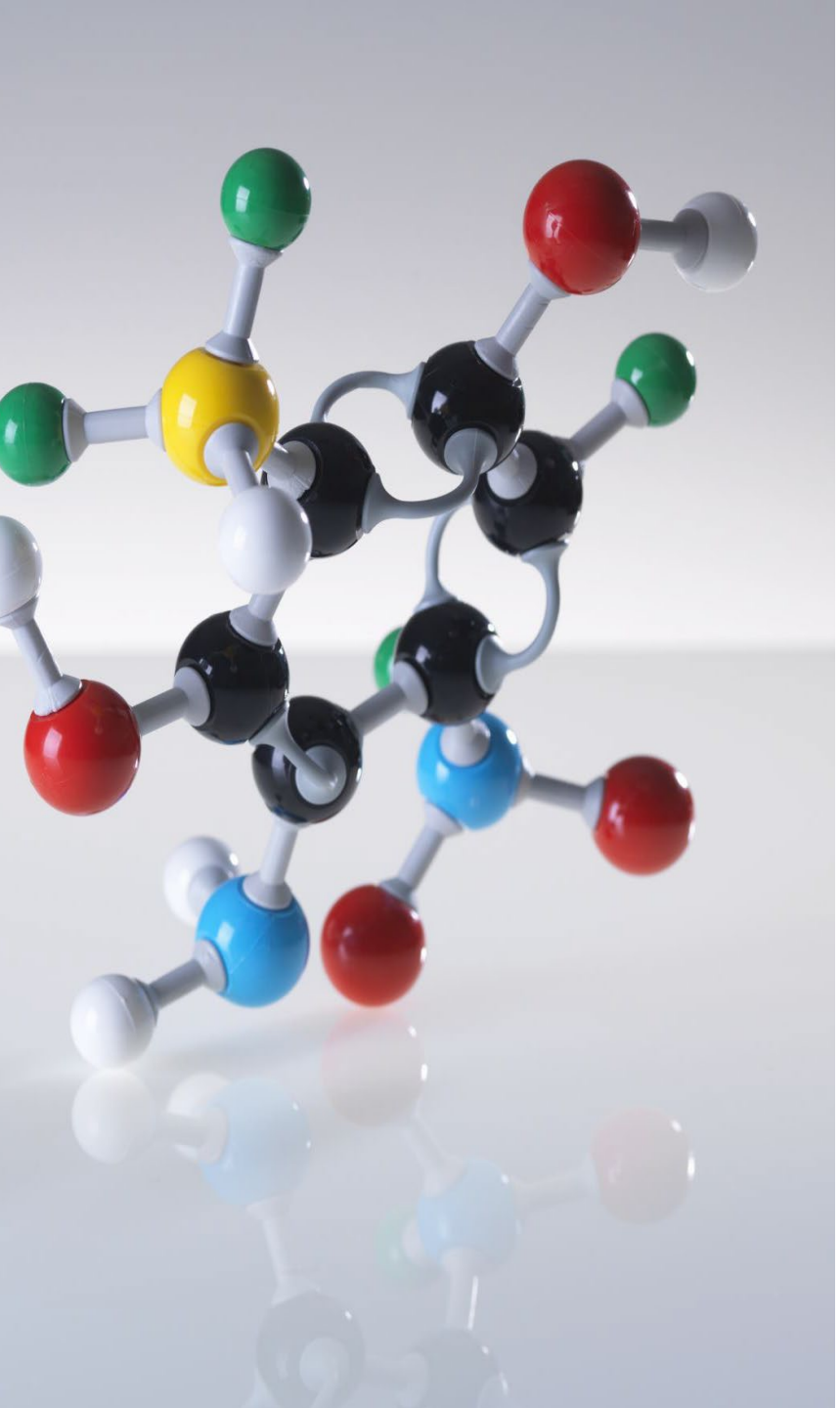


Figure 2: Adversaries' capabilities.



La metodologia AI per la sicurezza satellitare: obiettivi

- **le funzioni interpretativa, preventiva e predittiva**
- le rappresentazioni di conoscenza: le *knowledge bases*
- analisi e rappresentazione delle vulnerabilità
- analisi e rappresentazione delle minacce
- analisi e rappresentazione degli attacchi
- gli impatti
- modelli specifici di classificazione tassonomica e ontologica

La tassonomia LEO della MITRE

Zuanelli 2025 La nuova sicurezzza conf

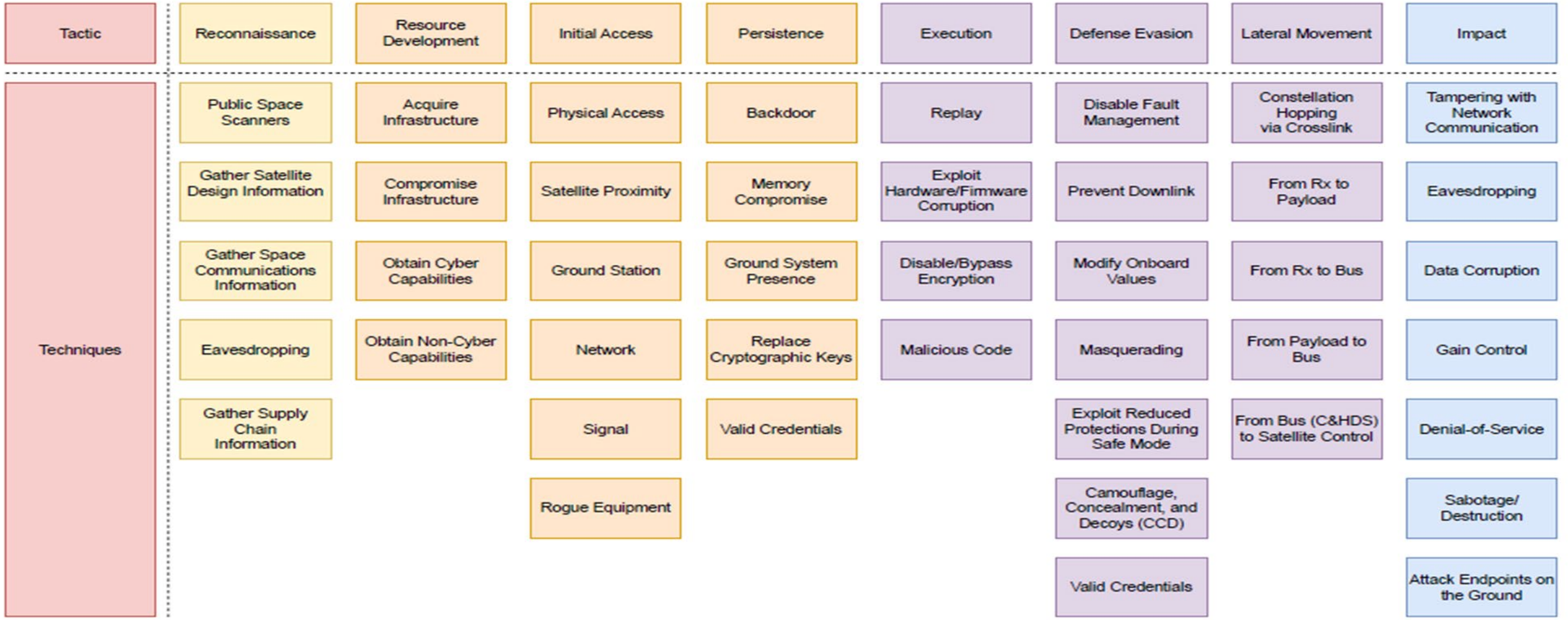


Figure 4: MITRE taxonomy for LEO satellites.

Dominio, minacce e difesa nel satellitare militare: le soluzioni architetturali Pragmema POC

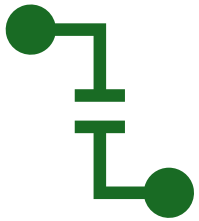
Satelliti: tipologie, orbite, canali di comunicazione, *mission*, *payload*, tecnologie

- l'analisi delle funzionalità nel satellitare civile e militare
- l'analisi delle soluzioni tecnologiche attuali della difesa aerospaziale nel satellitare
- l'analisi delle funzionalità del sistema di comunicazione satellitare
- l'analisi delle vulnerabilità
- l'analisi delle minacce
- l'analisi degli attacchi
- l'analisi degli impatti

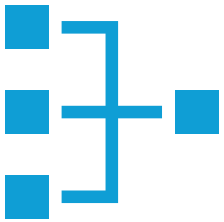
Pragmema POC *analytics* nella difesa satellitare militare: la componente **functionalities**

Il modello Pragmema POC di componenti di un sistema di sicurezza satellitare: le **funzionalità**

il nodo apicale: le 4 funzionalità



le 4 funzionalità: *operations continuity*, *physical protection*, *communication protection*, *data protection*



i nodi classi/entità tassonomiche di livello

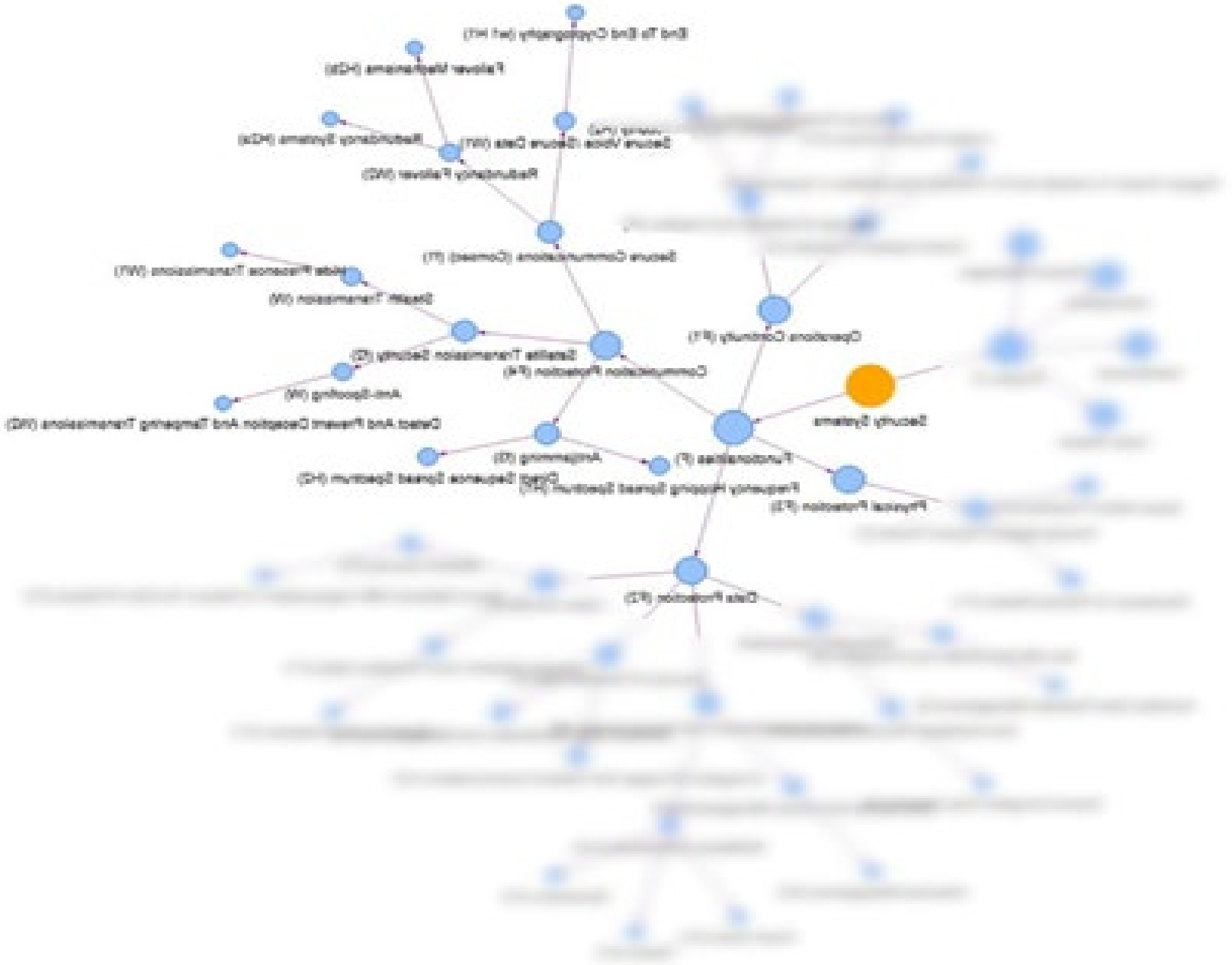
Le funzionalità nel sistema Pragmema POC di sicurezza

Le entità di **secondo livello** ovvero le **quattro funzionalità generali** della comunicazione nel sistema di sicurezza (operations continuity, *physical protection*, *communication protection*, *data protection*)

contengono entità di **terzo, quarto e quinto livello** definite secondo tre specifiche concettuali di ciascuna entità derivate da un **vocabolario semantico controllato**: in particolare, **tre proprietà delle funzionalità** sono specificate secondo criteri logico-semantici

Le proprietà riguardano: le **funzioni del sistema di comunicazione** (F), l'**attività di sicurezza** (W) e lo **strumento operativo** (H)

Pragmema POC: il sistema di sicurezza satellitare



Esempio di relazioni tassonomiche dal nodo funzionalità, 1° livello, al nodo di 2° livello: **protezione delle comunicazioni**

la protezione delle comunicazioni (F4) nodo/classe di 2° livello, comprende tre nodi di 3° livello:

COMSEC (f1)

sicurezza della trasmissione satellitare (f2)

antijamming (f3)

Nodi di 3° 4° 5° livello

COMSEC (f1), nodo di 3° livello, include due nodi di 4°livello:

- voce sicura/dati protetti (W1)
- *failover* di ridondanza (W2)

Voce sicura /dati protetti (W1) include un nodo di 5° livello:

- crittografia end-to-end (w1H1)

il *failover* di ridondanza (W2) include due nodi di 5° livello:

- sistemi di ridondanza (H2a)
- meccanismi di *failover* (H2b).

La rete relazionale

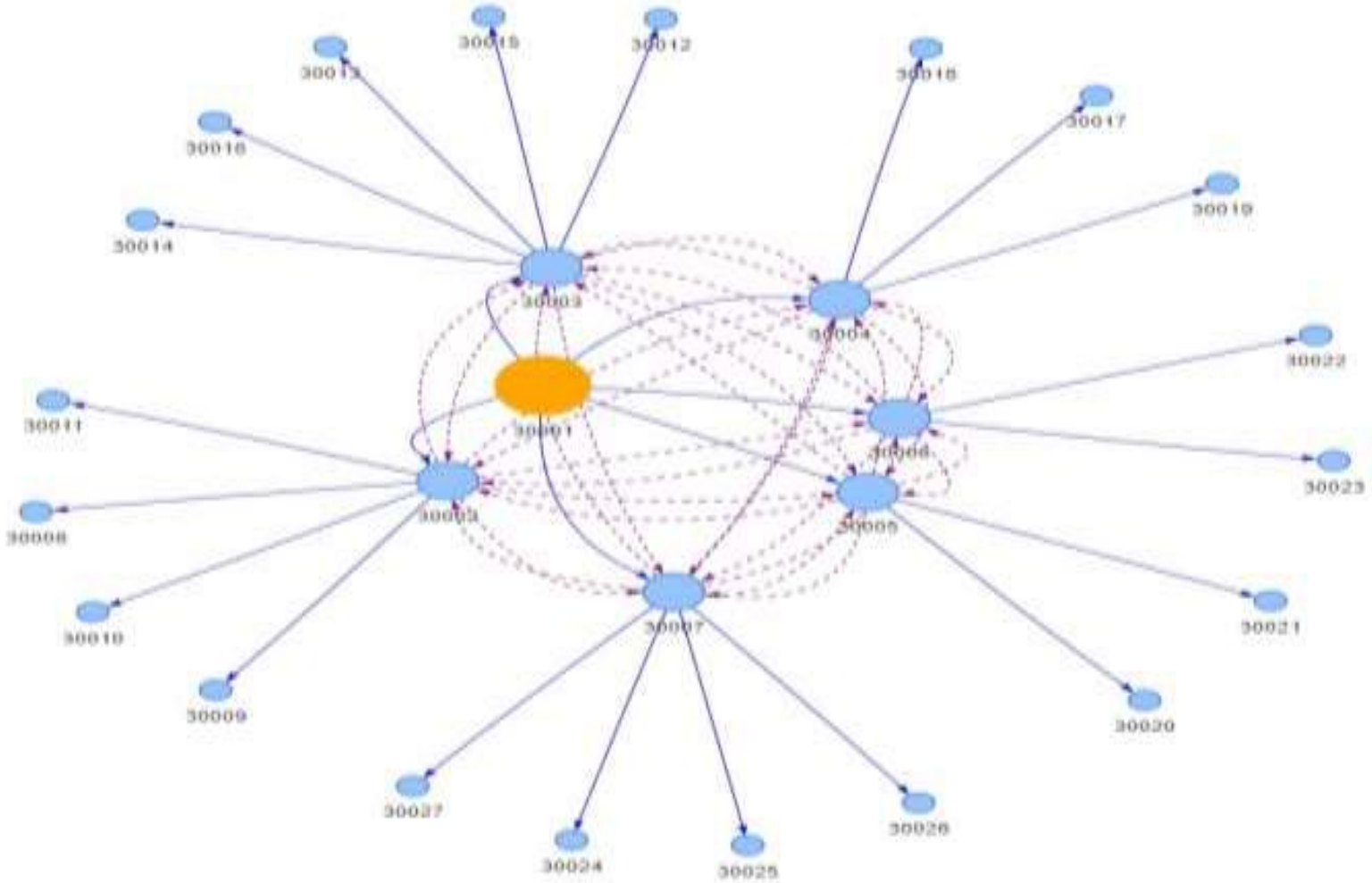
Entità/ nodi tassonomici delle funzionalità sono correlati trasversalmente a componenti di sistema, nodi di primo livello quali:

- **minacce**
- **attacchi**
- **impatto**

Pragmema POC: un modello tassonomico ontologico parziale degli attacchi, nodi di 2° livello

- *cybersecurity system*
- *military satellites*
- *data*
- *threat actors*
- *attack techniques*
- *attack vectors*

Pragmema POC: ontologia degli attacchi



Lo sviluppo ontologico del sub-dominio sicurezza satellitare e le prospettive preventive e predittive

La possibilità di uno sviluppo ontologico del dominio (sub-) della sicurezza satellitare, articolato in **‘civile’** e **‘militare’** prevede una sequenza complessa di fasi di analisi e definizione di entità e relazioni atte a rappresentare e acquisire:

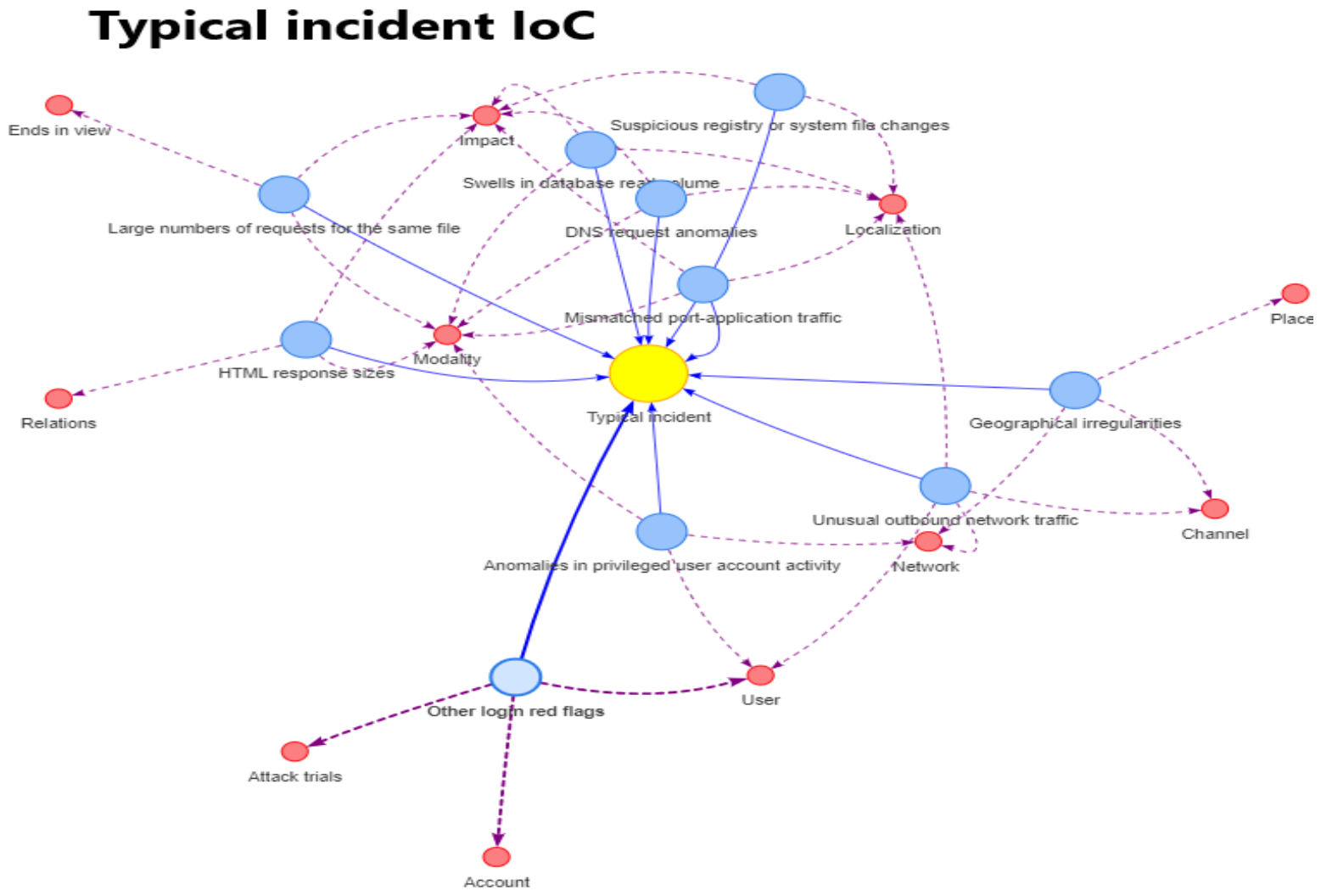
- **i nodi/entità nucleari** corrispondenti ai **dati tecnologici** delle diverse classi di entità rappresentate
- la definizione di **campi manuali di inserimento dati**
- il **modello tecnologico architetturale** di apprendimento
- l’ **apprendimento AI *supervised***
- il testaggio delle **funzionalità analitiche preventive**
- lo **sviluppo inferenziale** AI *unsupervised*
- possibili sviluppi **predittivi** di attacchi

- l’apprendimento deidati nucleari e ‘integrazione con l’intologia della cybersecurity

Infine

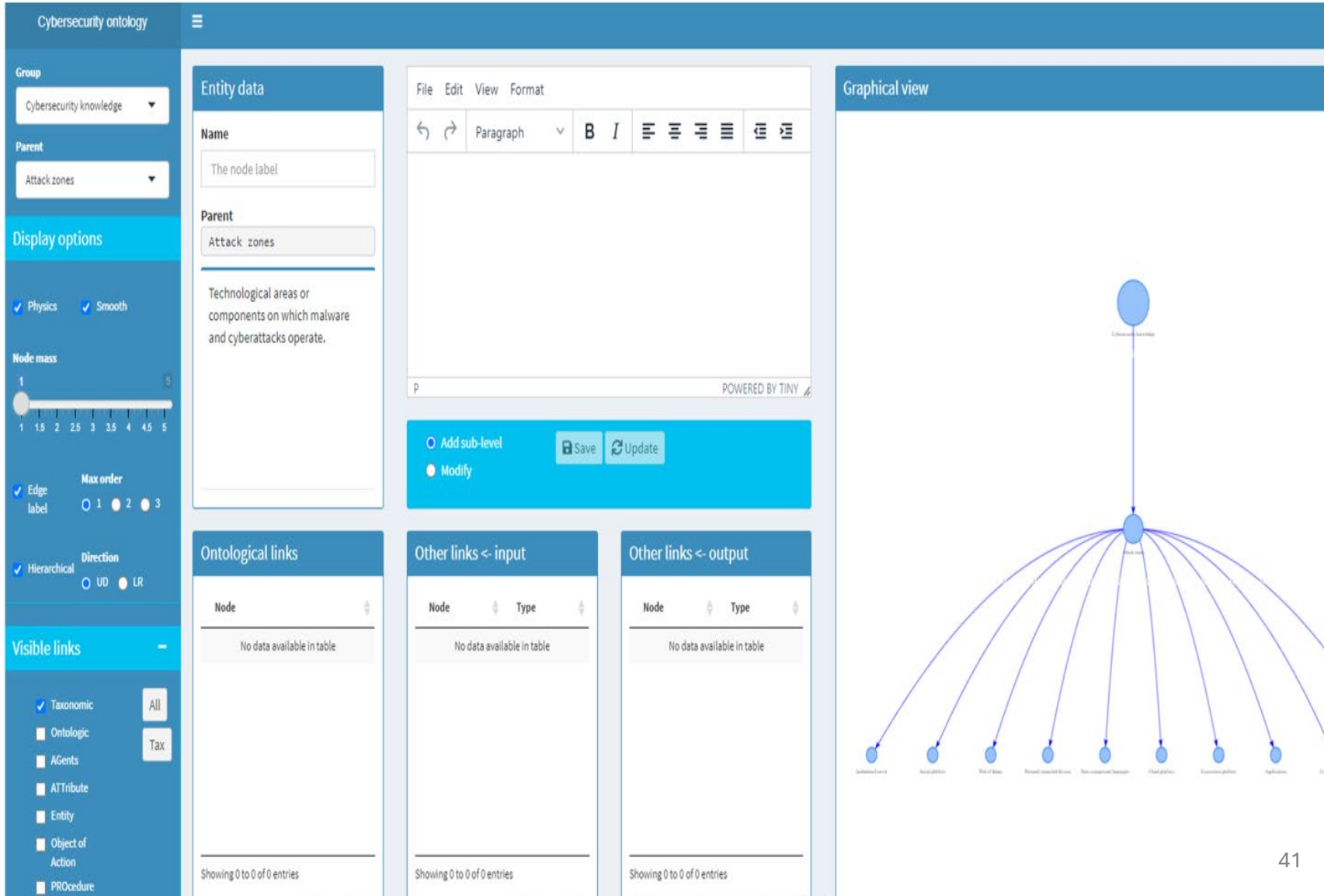
L’integrazione della ontologia del sub-dominio satellitare nella *cybersecurity ontology* ovvero nella AI cybersecurity *knowledge base*

L’integrazione IoCs nella POC ontology

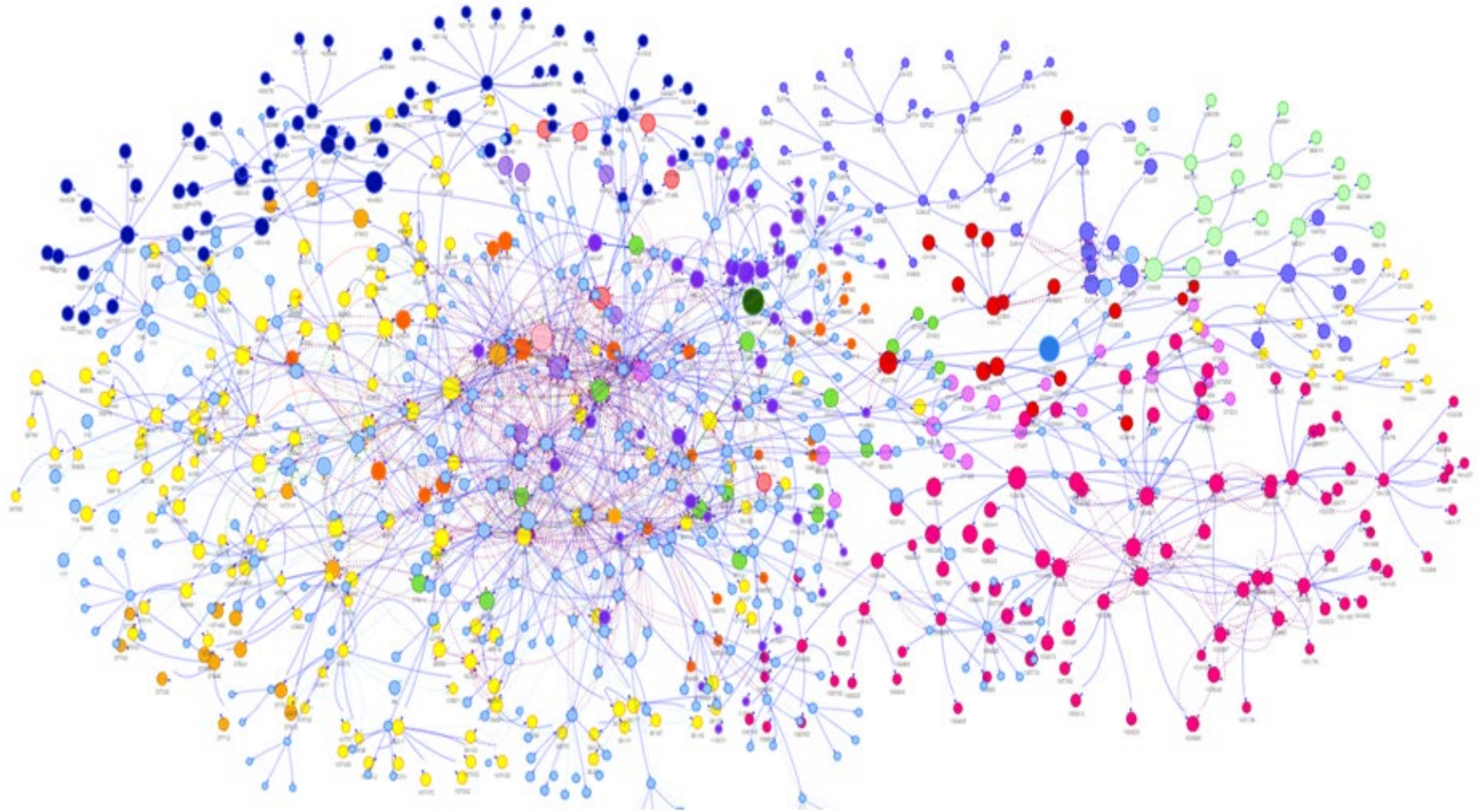


Le zone d'attacco nella *knowledge base* Pragmema POC

POC: attack zones



Pragmema POC cybersecurity knowledge ontology



Un percorso complesso.
Un' **ontologia della *cybersecurity* che integri** i dati di sicurezza dei **sistemi informativi informatici,** delle **reti,** dei **sistemi e tecnologie di difesa (IoCs e IoAs), dei canali di connessione** e degli **attacchi!**

Una nuova sicurezza?
Forse…

Zuanelli 2025 La nuova sicurezzza conf