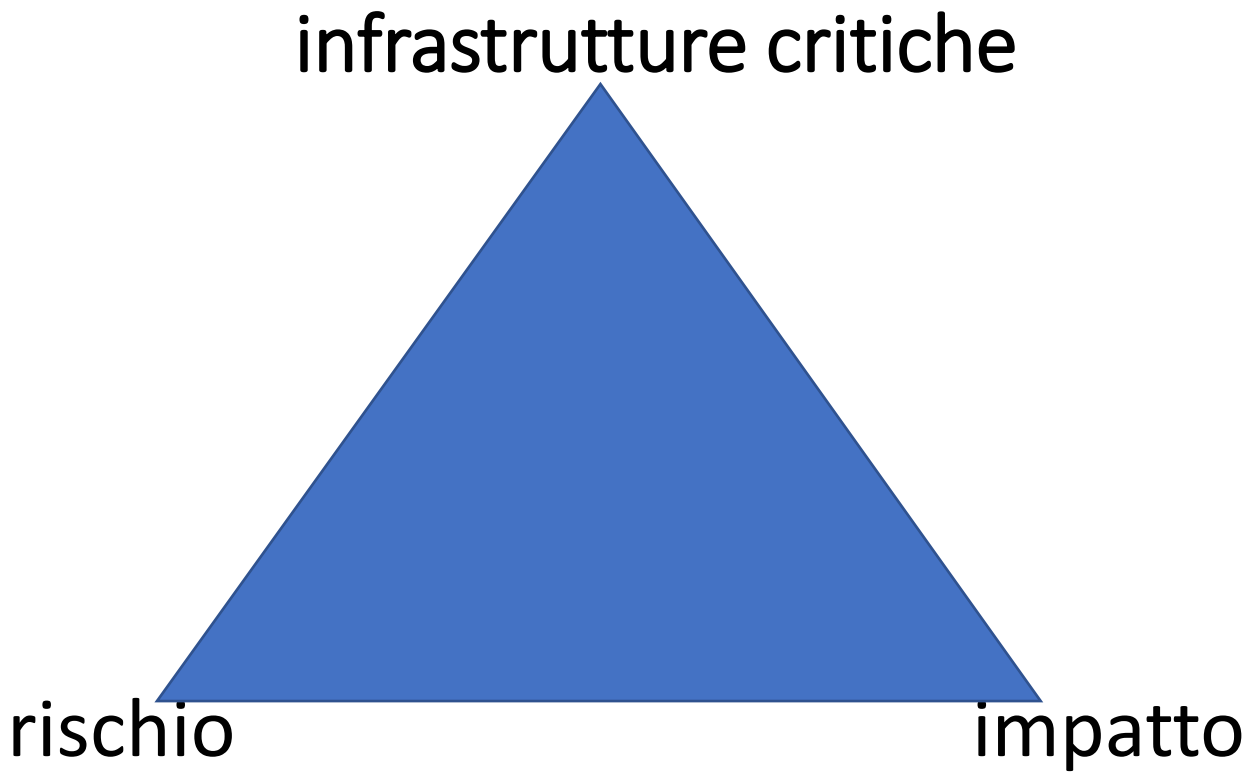
Cybersecurity e protezione dei dati: tra rischio, impatto e sistema

Elisabetta Zuanelli

Presidente CReSEC/Università degli Studi di Roma “Tor Vergata”

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


infrastrutture critiche
rischio
impatto

Norme, comportamenti, risorse e tecnologie della sicurezza

GDPR

D.Leg. vo 65/2018 (Recepimento Direttiva NIS)

CYBERACT

PSD2

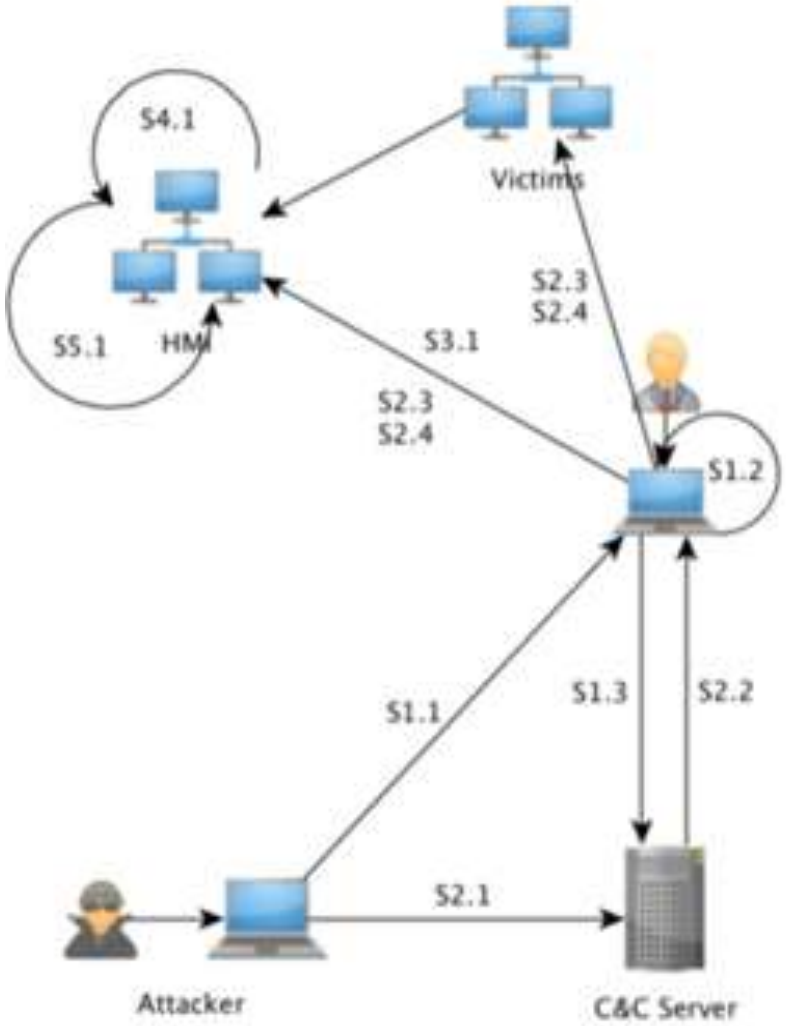
D.L. 105/2019

Infrastrutture critiche: l'incidente ucraino

The Ukraine's Power Grid Incident (Knownsec Security Team, Malicious Code Analysis on Ukraine's Power Grid Incident, 2016)

"At the end of December 2015, the network system of Ukrainian power companies was attacked by hackers, leaving most areas of western Ukraine in the dark…security teams overseas claimed that this incident was related to the Black Energy trojan and some malicious code samples had been acquired and analysed"

La ricostruzione della ‘kill chain’ parziale



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.

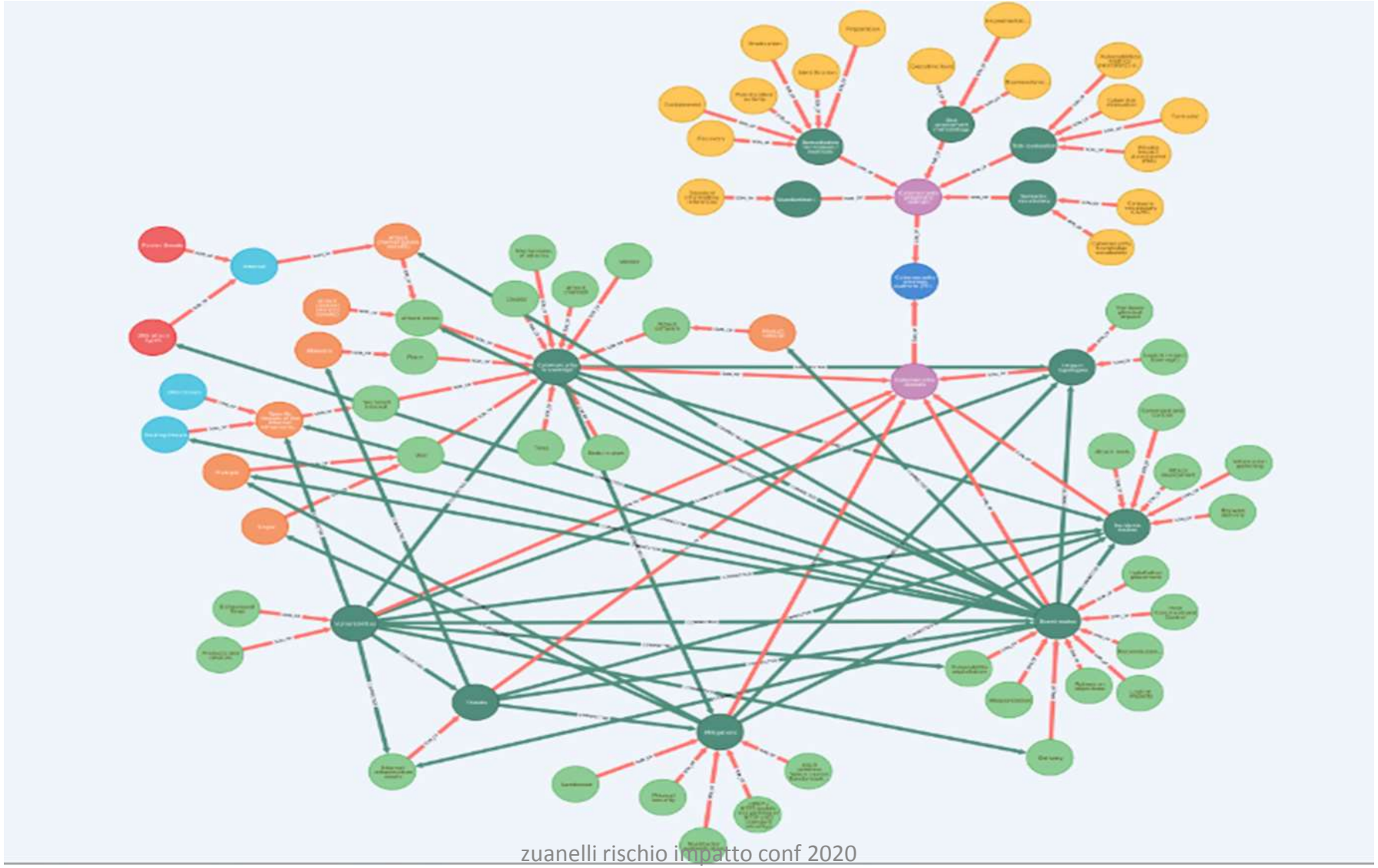
5.1 Attackers load Kill Disk components whenever possible to destroy host disks, causing the paralysis of the entire system.

I quesiti

Avranno valutato il rischio e se sì, come?

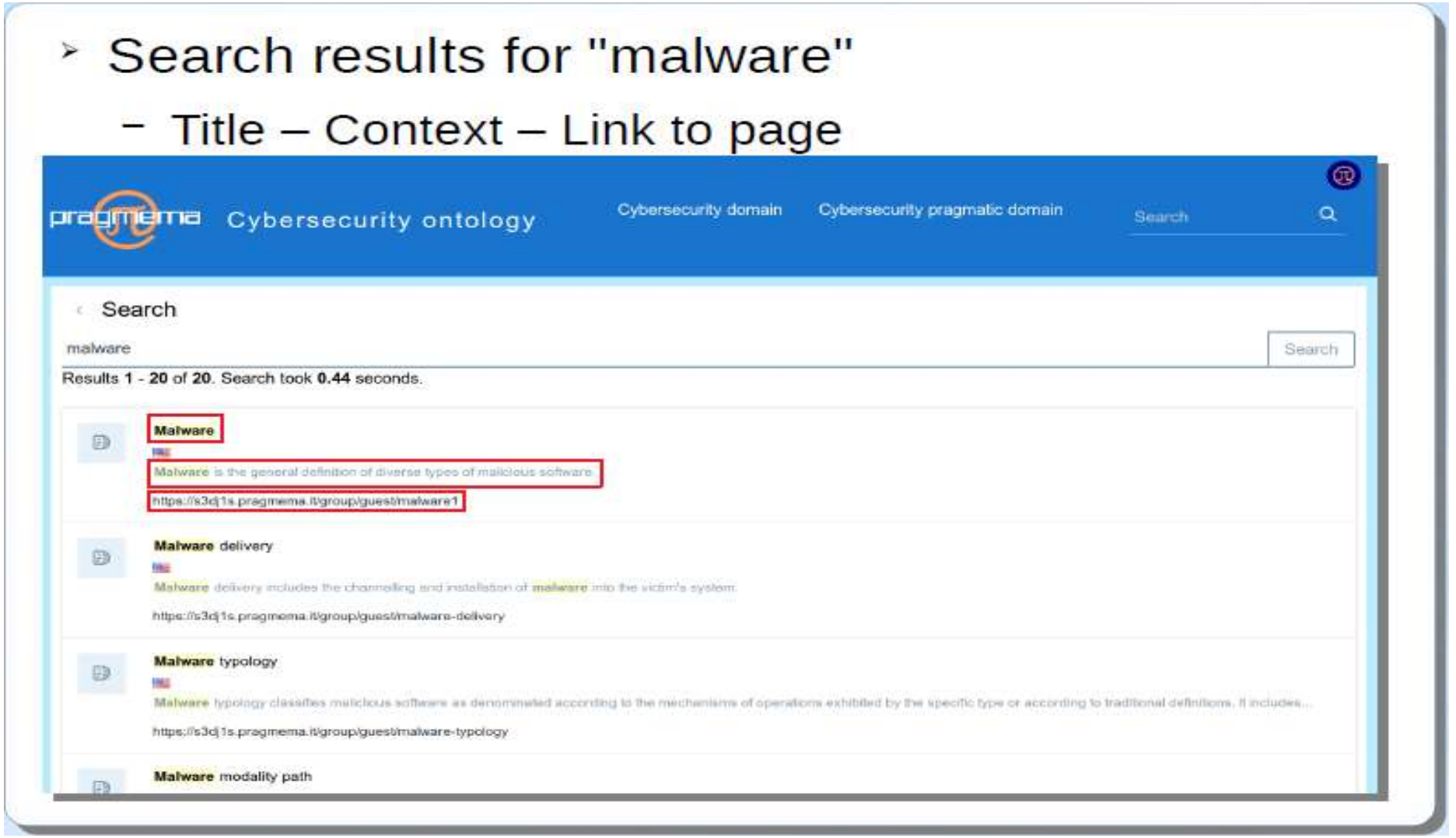
Necessarie le norme?
Necessari i comportamenti?
Necessarie le competenze?
Necessarie le capacità previsionali tecnologiche?

La piattaforma ontologica POC: la predittività logico-semantica

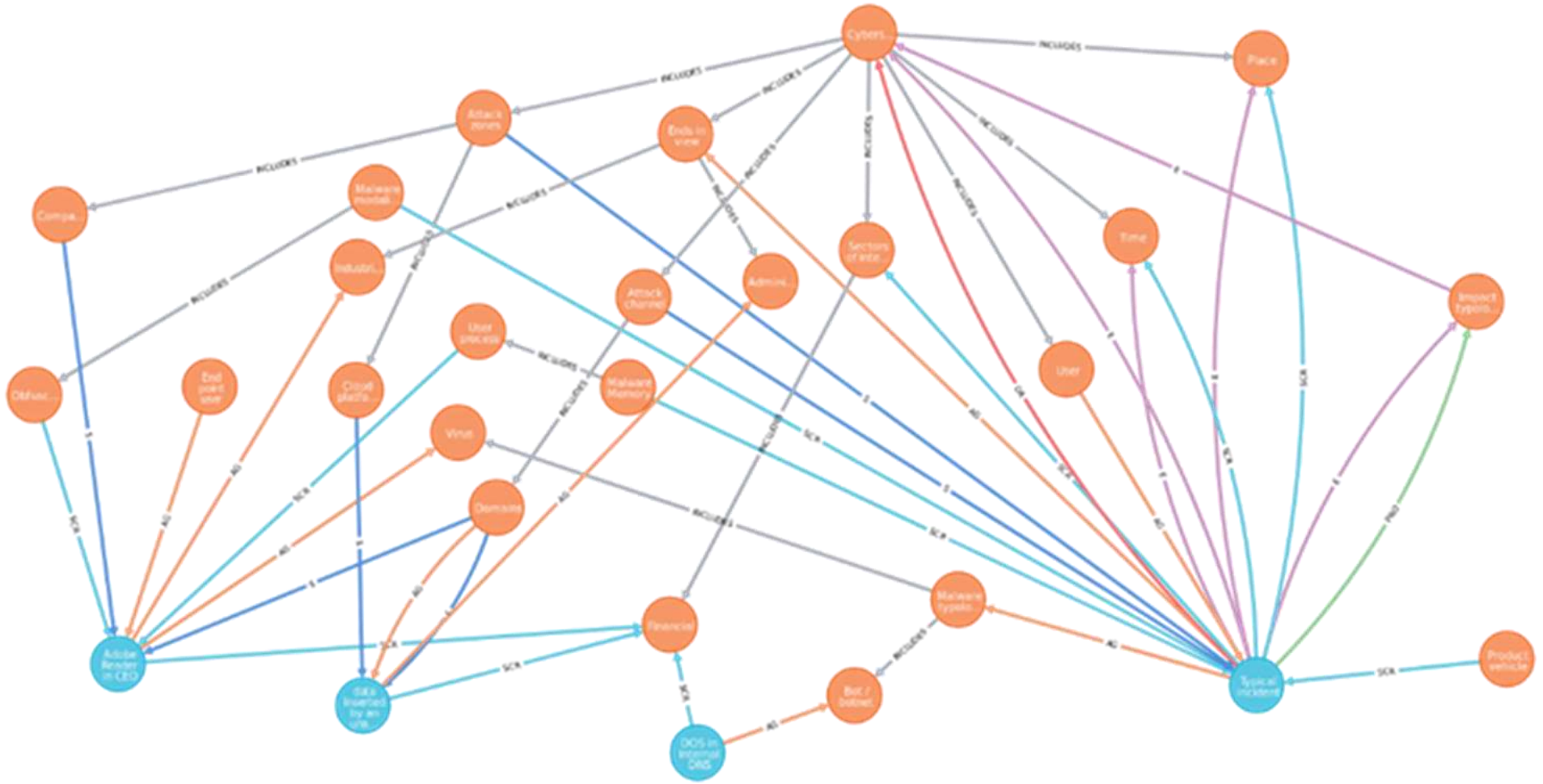


Le entità e il Vocabolario semantico controllato POC

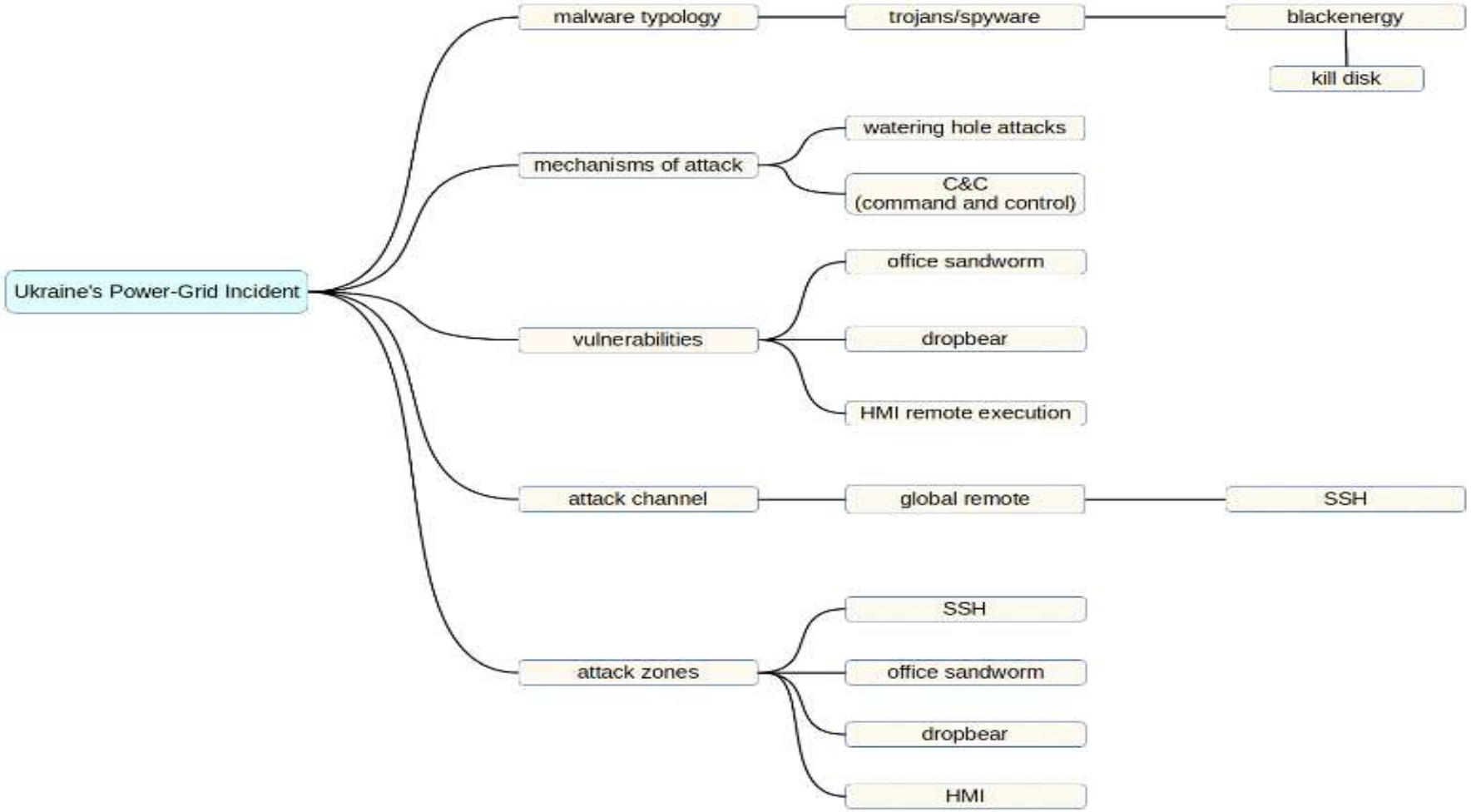
- Search results for "malware"
  - Title – Context – Link to page



Analisi logico-semantica POC della *kill chain* parziale nell'incidente ucraino



L’analisi tassonomico-ontologica POC dell’incidente ucraino



Il perimetro : DL 105/2019
3 decreti e 1 regolamento Art. 1

L'individuazione dei soggetti pubblici e privati tenuti alla sicurezza

Con Decreto DPCM CISR

Le procedure per le notifiche (Decreto DPCM)

CSIRT ---- a DIS---- a Min Interno/PCM/Mise

Elaborazione delle misure di sicurezza

Soggetti attuatori: PCM, Mise, Difesa, Interno, MEF, DIS e MAE

Comunicazione e valutazione per l'affidamento di forniture di beni, sistemi e servizi ICT

- Centri di valutazione CVCN e Interno e Difesa
- Schemi di certificazione
- Collaborazione dei fornitori

Sanzioni

Pecuniarie e al personale amministrativo

Il Decreto Legge 105/2019 e le **norme di contesto** Artt. 1,2,3

Entro un massimo di 10 mesi 3 decreti e 1 regolamento

- Interazione e integrazione con le norme contenute nel Decreto Leg. vo 65/ 2018

Notifica, responsabilità, criteri, laboratori di valutazione

La L. 155/2005, il DL 144/2005,il D.Leg.vo 82/2005, il CAD 2005, la L231/2001, la L. 208/2015,

Art. 2 Sul personale CVCN e PCM

Il D Leg.vo 165/2001, ill D.Leg.vo 66/2010 , la L. 244/2007, la L 127/1997, il D. Leg.vo 303/1999, il DL 101/2013, la L 125/2013, la L. 56/2019

Art. 3 Reti banda larga e 5 g

L 56/2012, DL 21/2012

Individuazione dei soggetti pubblici e privati tenuti al rispetto delle misure e degli obblighi: **criterio di gradualità**???Art. 1 co. 2 a 2 bis

Art.4 Modifiche alla disciplina dei **poteri speciali** nei settori di rilevanza strategica

Al Governo sono estesi i **poteri di controllo** mediante poteri speciali (cd. “golden power”) a nuovi ambiti:

- con particolare riferimento a quanto previsto dal decreto-legge 15 marzo 2012, n. 21
- scopo: coordinare l’attuazione del Regolamento (UE) 2019/452, sul **controllo degli investimenti esteri**
- apprestare idonee misure di **tutela di infrastrutture o tecnologie critiche** che ad oggi non ricadono nel campo di applicazione del decreto-legge 15 marzo 2012, n. 21

In tale nuovo ambito d’applicazione **entrano ora a far parte anche le società quotate nella Borsa Italiana.** L’obiettivo? La protezione dei comparti sopracitati e delle aziende operanti in essi.

I poteri speciali

- La possibilità di **introdurre veti** all'adozione di decisioni societarie o all'acquisto di partecipazioni in società di tali ambiti

- La facoltà di **imporre prescrizioni e condizioni nell'ambito dell'affidamento di forniture di beni e servizi** di *information and communication technology* (ICT) destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti

L’ **adeguatezza concettuale** dei contenuti normativi

- Una fragile definizione: *adequacy*
- L’adeguatezza dei sistemi di valutazione del rischio
- Chi effettua i controlli: controllore e controllato (i *vendor* **collaborano alla valutazione del rischio**…)
- La correlazione tra le strutture: Difesa, Interno, Mise, AgID, Autorità (Protezione dei dati, AgCOM e le 5 attivate dal Decreto Leg.vo 65/2018 di recepimento della NIS)
- Sanzioni ??? Potere dissuasivo? *Compliance* è sicurezza?
- I centri di valutazione: risorse quantitative e qualitative
- I ruoli dei *vendor*

Innovazione tecnologica e sicurezza: **temi e problemi**

- Applicazioni tecnologiche travolgenti e canali di attacco crescenti: satellitari, droni, ecc.
- Le internet parallele: la Russia… ma anche, ad esempio, il finanziario sottomarino
- Il moltiplicarsi dei servizi digitali e delle app, IoT
- La competizione USA, CINA nell'AI
- La competizione, europea e non nel 5G
- Lo *slicing* e il controllo planetario delle informazioni: la dimensione economica (sorvoliamo sul sociale e l'etico) e l'indifferenza soggettiva
- Il ritardo nelle soluzioni tecnologiche di sicurezza
- Formazione e ricerca / skills shortage e upskilling)

Soluzioni di sistema

- Autoregolazione dei *vendor*: tra competizione, etica e mercato
- La *cyberdiplomacy* globale ?
- L'intensificazione del contrasto alla committenza e ai beneficiari del *cybercrime*
- Il controllo operativo e i partenariati parziali

E’ tutto Grazie!!!