Relational Modelling of Cyberattacks: A Taxonomy for the Analysis of Threat Interactions in Digital Environments

Mikel Ferrer-Oliva, José-Amelio Medina-Merodio, José-Javier Martínez-Herraiz, Carlos Cilleruelo-Rodríguez

Departamento de Ciencias de la Computación, Universidad de Alcalá, España

Alcalá de Henares, España

{mikel.ferrer, josea.medina, josej.martinez, carlos.cilleruelo}@uah.es

Abstract. *Cyberattacks have evolved into coordinated operations that combine multiple techniques to disrupt digital infrastructures. Existing classification methods often overlook the interdependence between attack vectors, limiting early detection and strategic response. This study introduces a relational taxonomy composed of eight attack groups and twenty connections, enabling a non-hierarchical understanding of how threats interact and escalate.*
The model captures dynamic relationships across multiple attack phases and supports the integration of emerging techniques. Its open structure enhances adaptability and analytical depth, offering practical value for cybersecurity operations within corporate and critical environments. This contribution addresses key limitations in static threat classification frameworks.

Keywords. Cybersecurity, taxonomy, threats, risk modelling, cyber defence.

1 Introduction

Digital transformation has significantly redefined the landscape of technological infrastructures, exposing organizations and institutions to a broader spectrum of advanced cyber threats. These threats have evolved from isolated actions into complex operations where diverse techniques are orchestrated to maximize impact and compromise resilience across interconnected systems.

Although current cybersecurity frameworks provide valuable mechanisms for classifying and exchanging threat information, such as MITRE ATT&CK (MITRE, 2025), STIX2 (TC, 2025a), TAXII 2.1 (TC, 2025b), and MISP (CIRCL, 2025), their descriptive nature tends to focus on individual tactics. These approaches frequently fail to convey how techniques interact within attack sequences, thereby limiting their predictive capacity and response effectiveness.

Documented analyses of real incidents demonstrate that attacks typically unfold as a chain of events, where an initial intrusion enables successive steps, including privilege escalation, long-term access, and lateral expansion across digital environments (ENISA, 2021). This progression highlights the necessity of a relational understanding of how attack vectors reinforce one another throughout the adversarial lifecycle.

For example, social engineering continues to serve as a catalyst for compromising credentials and delivering malware, granting unauthorized access to high-value environments (Bhardwaj & Sapra, 2020; Hellemann, 2023). In parallel, the exploitation of software vulnerabilities remains a prevalent mechanism for maintaining persistence and infiltrating sensitive systems (Clavijo Mesa et al., 2024; Connolly et al., 2023). However, the prevailing classification models lack the structural capacity to reflect these strategic interactions. This paper introduces a relational taxonomy that groups cyber threats according to shared tactical and operational characteristics, while mapping the connections that enable their interaction. Unlike rigid categorizations, the model is designed as a non-hierarchical system capable of representing complex relationships among diverse offensive techniques. Its purpose is to support more accurate threat analysis, informed risk assessment, and adaptive response strategies in dynamically evolving cybersecurity environments.

The manuscript is structured as follows: Section 2 presents a review of existing taxonomies and their limitations. Section 3 details the proposed model, including its categories and relational links. Section 4 discusses practical implications and real-world applications. Section 5 concludes with a summary and future lines of research.

2 Theoretical Framework

Cyber threats evolve constantly, prompting the creation of taxonomies to structure and classify

malicious behaviours. Ontology-driven efforts like CASE formalise events but show limited adoption, while platforms like MISP facilitate sharing yet do not model the strategic interplay among vectors (CIRCL, 2025; C. Community, 2025). Most systems remain static: even MITRE ATT&CK—despite its granularity—cannot depict the dynamic sequences observed in real incidents (MITRE, 2025). In practice, attacks unfold through chained techniques that escalate access or maintain persistence, underscoring the need for taxonomies that capture interdependencies and progression (ENISA, 2021). Empirical patterns—watering hole leveraging trusted sites (Alrwais et al., 2016), coordinated ransomware + DDoS in industrial/maritime contexts (Clavijo Mesa et al., 2024; Ivanov et al., 2021), and the surge of ransomware amid remote work and credential leaks—reinforce this need (Beaman et al., 2021; Rauf et al., 2023; Salim et al., 2019).

2.1 Limitations of Static Taxonomies

Frameworks like MITRE ATT&CK (MITRE, 2025) catalogue techniques in rigid categories. Although informative, they overlook how tactics combine across stages. This limits their capacity to model threat progression.

Attackers adapt their strategies based on the environment, chaining actions that static models fail to capture (Connolly et al., 2023). Watering hole attacks, for instance, involve multiple phases of deception and exploitation (Alrwais et al., 2016). In industrial and maritime settings, coordinated ransomware and DDoS incidents underline the need for models that reflect overlapping behaviours (Clavijo Mesa et al., 2024; Ivanov et al., 2021). The surge in ransomware due to remote work and credential leaks reinforces this urgency (Beaman et al., 2021).

Without accounting for technique interrelations, traditional taxonomies struggle to support predictive analysis or adaptive defence (Rauf et al., 2023; Salim et al., 2019).

2.2 Intrusion Chains and Implications for Risk Assessment and Incident Response

Cyberattacks typically evolve as ordered sequences, where each step enables the next (Hutchins et al., 2011; Javeed et al., 2020). Frequent entry vectors—phishing and vishing—lead to credential theft or malware deployment (Álvarez et al., 2024; Bhardwaj & Sapra, 2020; CISA & FBI, 2021). Campaigns such as Lucifer combine cryptojacking, DDoS, and exploitation in a single flow, while IoT botnets assemble large-scale infrastructures (Gelgi et al., 2024; Networks, 2025; Niño, 2023; Wu et al., 2021). Static frameworks often obscure these dependencies, reducing their usefulness for anticipatory defence. Standards like STIX 2.1 and TAXII 2.1 enable structured sharing but, by design, do not impose relational semantics; MISP aids classification and exchange yet lacks native constructs for stage transitions (CIRCL, 2025; TC, 2025a, 2025b). As emerging vectors—e.g., supply chain attacks—demand models that capture coordination (ENISA, 2021), prior proposals such as the Diamond Model and VERIS acknowledge links but remain limited in operational use (Caltagirone et al., 2013; V. Community, 2025; Sedano Pinzón, 2024). A relational taxonomy aligns classification with how real attacks unfold, making explicit the enabling role of each stage and strengthening both risk assessment and incident response (Clavijo Mesa et al., 2024; Hutchins et al., 2011; Javeed et al., 2020).

3 Proposed Cyberattack Taxonomy

The dynamic nature of cyber threats requires models capable of representing the interconnection between offensive techniques, rather than viewing them as isolated events. In adversarial contexts, attacks frequently manifest as interrelated actions, where each tactic contributes to achieving broader strategic goals. Recognizing this complexity is essential for improving the accuracy of threat analysis and the responsiveness of cybersecurity frameworks.

This section introduces a relational taxonomy of cyberattacks designed to map the functional role and interdependencies of each technique within an evolving threat environment. The model comprises eight distinct attack groups, each representing a set of behaviours or tactics commonly observed in real incidents. These groups are not organized in hierarchical order, but rather positioned within a network of relationships that reflects how they interact and reinforce one another.

The proposed structure captures both direct and indirect connections between attack groups. This approach enables analysts to identify common escalation paths, detect potential facilitators of advanced threats, and understand how certain techniques may contribute to system-wide compromise. By incorporating twenty well-defined relationships, the taxonomy supports a non-linear representation of attack progression, providing a more realistic basis for scenario-based risk modelling. Rather than introducing isolated categories disconnected from established knowledge, this model recontextualizes existing techniques within a relational framework that emphasises functional interdependence. By focusing on how techniques interact rather than how they are segmented, the approach facilitates the seamless incorporation of new attack modalities while preserving structural integrity. Its adaptability allows the taxonomy to remain operationally consistent as threat landscapes evolve, offering a scalable tool for understanding the convergence of diverse cyber tactics. In the following subsections, each attack group is described in detail

(Section 3.1), followed by an explanation of the strategic relationships that connect them (Section 3.2), and finally, a visual representation of these connections through a non-hierarchical diagram (Section 3.3).

3.1 Classification of Attacks Groups

This model facilitates the identification of recurring patterns in threat evolution, supporting the anticipation of escalation strategies commonly observed in complex cyber incidents. Table 1 presents the eight attack groups proposed in the taxonomy, each defined by the nature of the techniques involved and their role in documented cases. The classification does not follow a sequential or hierarchical structure but reflects distinct operational behaviours. Social engineering (such as phishing and vishing) exploits human factors to obtain credentials or trigger malicious actions (Bhardwaj & Sapra, 2020; Hellemann, 2023). These tactics often precede malware-based attacks involving ransomware, trojans or botnets used to disrupt systems or enable lateral movement (Ivanov et al., 2021).

Many incidents also involve exploiting software vulnerabilities in applications or firmware to gain privileged access (Networks, 2025; Wu et al., 2021). These are frequently combined with identity and authentication attacks based on credential stuffing or brute-force methods (Hellemann, 2023).

Other vectors include attacks on network infrastructure, which affect routers or internal devices to degrade services or bypass segmentation (Gelgi et al., 2024), and protocol-based attacks that intercept or manipulate data flows (Javeed et al., 2020).

In operational environments, threats against IT/OT infrastructure may compromise industrial processes (Clavijo Mesa et al., 2024). Advanced persistent threats and cyberespionage campaigns combine several tactics to maintain long-term access to strategic systems (Connolly et al., 2023; Rauf et al., 2023).

Table 1. Attack Groups in the Proposed Taxonomy

Strike Group	Description
Social Engineering (SE)	Use of psychological manipulation to gain access to credentials or resources. Phishing attacks have been identified as one of the leading causes of security breaches in companies (Bhardwaj & Sapra, 2020).
Malware-based attacks (MBA)	Use of malware to compromise systems, facilitating attacks such as ransomware, Trojans, and botnets. The analysis of new malware variants has proven its adaptability to evade detections (Ivanov et al., 2021).
Network Infrastructure Attacks (NIA)	Attacks targeting network devices, servers, and interconnected systems to disrupt services or facilitate unauthorized access. Recent research has looked at the impact of IoT botnets on massive DDoS attacks (Gelgi et al., 2024).
Exploiting Software Vulnerabilities (ESV)	Exploiting flaws in software to escalate privileges, install malware, or compromise critical systems. The persistence of unpatched vulnerabilities has been a key factor in multiple attack campaigns (Wu et al., 2021).
Attacks on Protocols and Communications (APC)	Compromise of communication protocols through techniques such as Man in the Middle attacks and DNS hijacking, facilitating the interception of sensitive data. Studies have shown the vulnerability of industrial protocols to targeted attacks (Javeed et al., 2020).
Identity and Authentication Attacks (IAA)	Compromise of credentials and authentication systems through attacks such as credential stuffing, brute force, and dictionary attacks. Exploiting credentials in corporate environments remains one of the main initial access tactics (Hellemann, 2023).
Attacks on critical IT/OT infrastructure (CIIA)	Attacks targeting industrial networks and SCADA systems for sabotage and espionage. Device tampering in critical environments has been documented as a significant risk to operational safety (Clavijo Mesa et al., 2024).
APTs and Cyberespionage (APT)	Persistent infiltration and espionage operations that combine multiple attack vectors to maintain longtermly access to strategic government and enterprise networks. Cyberespionage continues to evolve with more sophisticated persistence tactics (Connolly & Wall, 2019).

3.2 Relationships Between Attack Groups

A central strength of the proposed taxonomy lies in its capacity to model how attack groups interact strategically throughout the lifecycle of cyber incidents. Rather than depicting static or isolated behaviours, the taxonomy captures how techniques from different domains reinforce each other, forming interconnected sequences that reflect the operational logic observed in real-world threats.

Table 2 outlines twenty directional relationships supported by case-based evidence and intelligence reports. These links describe how the use of one type

of technique often enables, amplifies or conditions the success of others within multi-stage campaigns.

Initial compromise frequently involves social engineering tactics such as phishing or vishing (Álvarez et al., 2024; Bhardwaj & Sapra, 2020), which often lead to the extraction of access credentials (Hellemann, 2023; Ivanov et al., 2021). With these credentials, attackers can bypass authentication mechanisms, escalate privileges or deploy malware components tailored to specific targets (Clavijo Mesa et al., 2024; Gelgi et al., 2024). Malware, in turn, operates as a pivot between multiple attack vectors, supporting system manipulation, network disruption or covert persistence.

Exploitation of software vulnerabilities plays a complementary role, allowing unauthorized modifications in services and applications to establish control over critical assets (Networks, 2025; Wu et al., 2021). This technique is commonly associated with identity-based intrusions, particularly when authentication protocols are weak or reused credentials are exposed (Connolly et al., 2023; Rauf et al., 2023).

Attacks targeting communication protocols and network infrastructure add another layer of complexity, enabling packet interception, redirection or disruption of legitimate traffic flows (Javeed et al., 2020; Salim et al., 2019). When these same techniques are directed toward operational environments, they can severely impact critical IT/OT infrastructure, compromising industrial processes and degrading service continuity (Clavijo Mesa et al., 2024).

These diverse vectors converge in advanced persistent threats and cyberespionage operations, where multiple techniques are orchestrated to maintain long-term access and extract strategic information (Connolly et al., 2023; Rauf et al., 2023)).

By mapping these interdependencies, the taxonomy offers a relational view of attack progression that supports predictive modelling, improves early detection and enhances threat intelligence capabilities.

Table 2. Relationships between Attack Groups in Taxonomy

Initial Attack	Facilitated Attack	Description
Identity and Authentication Attacks	Social Engineering	Credentials access aids manipulation, increasing deception effectiveness for successful attacks (Bhardwaj & Sapra, 2020; Hellemann, 2023).
Identity and Authentication Attacks	Malware based attacks	Compromised systems via stolen credentials allow running unauthorized software, bypassing security to spread malware (Beaman et al., 2021; Ivanov et al., 2021).
Identity and Authentication Attacks	Exploiting Software Vulnerabilities	Improper auth/privileged access helps attackers find flaws, increasing compromise risk (Rauf et al., 2023; Wu et al., 2021).
Identity and Authentication Attacks	Attacks on Protocols and Communications	Exposed credentials allow channel access for data interception/alteration without needing vulnerability exploits (Javeed et al., 2020; Wu et al., 2021).
Identity and Authentication Attacks	Network Infrastructure Attacks	Improper admin access aids network manipulation for persistence or undetected info flow modification (Gelgi et al., 2024; Salim et al., 2019).
Social Engineering	Malware based attacks	Persuasive deception effectively induces users to run unsafe programs, enabling harmful actions (Álvarez et al., 2024; Bhardwaj & Sapra, 2020).
Social Engineering	Exploiting Software Vulnerabilities	Personalized persuasion leads victims to insecure platforms, risking unauthorized code execution (Alrwais et al., 2016; Rauf et al., 2023).
Malware based attacks	Attacks on Protocols and Communications	Some malware uses system communication for data manipulation/exfiltration without needing credentials (Javeed et al., 2020; Wu et al., 2021).
Malware based attacks	Network Infrastructure Attacks	Compromised devices can degrade networks and enable unauthorized internal access without human interaction (Clavijo Mesa et al., 2024; Gelgi et al., 2024).
Malware based attacks	Attacks on critical IT/OT infrastructure	Harmful software exploited to affect essential control systems, interrupting operations strategically (Clavijo Mesa et al., 2024; Niño, 2023).
Malware based attacks	Exploiting Software Vulnerabilities	Automated access helps find flaws in compromised environments, increasing persistence ability (Rauf et al., 2023; Wu et al., 2021).

Exploiting Software Vulnerabilities	Attacks on Protocols and Communications	Altering apps/services enables communication manipulation for data access without user intervention (Javeed et al., 2020; Wu et al., 2021).
Exploiting Software Vulnerabilities	Network Infrastructure Attacks	Software protection flaws allow compromising key network devices, affecting stability and enabling unauthorized access (Salim et al., 2019; Wu et al., 2021).
Exploiting Software Vulnerabilities	APTs and Cyberespionage	Persistent attacks use software flaws to infiltrate sensitive areas, allowing prolonged undetected access (Connolly & Wall, 2019; Rauf et al., 2023).
Attacks on Protocols and Communications	APTs and Cyberespionage	Manipulating device communication aids info exfiltration without needing credentials, creating high risks (Rauf et al., 2023; Wu et al., 2021).
Attacks on Protocols and Communications	Attacks on critical IT/OT infrastructure	Manipulating industrial communication systems allows remote process control, impacting operational continuity (Clavijo Mesa et al., 2024; Wu et al., 2021).
Attacks on Protocols and Communications	Network Infrastructure Attacks	Compromising communication protocols enables persistent attackers to establish network footholds for undetected data extraction (Connolly & Wall, 2019; Rauf et al., 2023).
Network Infrastructure Attacks	APTs and Cyberespionage	Compromised networks facilitate access to industrial environments, with significant strategic/operational impact (Clavijo Mesa et al., 2024; Niño, 2023).
Network Infrastructure Attacks	Attacks on critical IT/OT infrastructure	Prolonged infiltrations via network compromise enable espionage/process alteration, threatening stability/confidentiality (Connolly & Wall, 2019; Niño, 2023).
APTs and Cyberespionage	Attacks on critical IT/OT infrastructure	Prolonged APT access enables process manipulation and key info theft in globally important infrastructures (Clavijo Mesa et al., 2024; Rauf et al., 2023).

3.3 Taxonomy Framework

Fig. 1 presents a non hierarchical relational diagram. Each attack group is a node with evidence based directed links that indicate tactical enablement.

The view reveals multiple paths from phishing or credential compromise to malware and vulnerability exploitation or unauthorized access and also cyclic patterns typical of APTs. The scheme supports threat correlation and path simulation and predictive risk modelling.

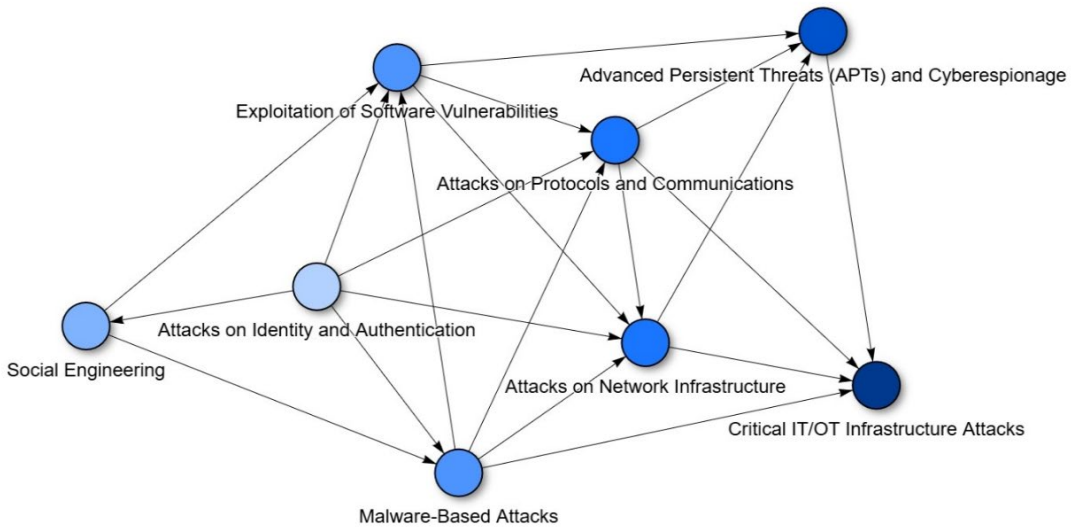

Figure 1. Framework of the Proposed Relational Taxonomy

4 Methodology

The taxonomy is built as a functional partition of eight groups defined by the tactical role they play within real intrusion chains, independent of platform, sector, or malware family. The decision to fix eight groups simultaneously pursues broad functional coverage and clear semantic separation so that the model avoids overlaps and preserves traceability to TTP catalogues and cyber-threat intelligence exchange frameworks (ENISA, 2021; Hutchins et al., 2011; MITRE, 2025).

The twenty directed relationships arise from an iterative refinement that retains only tactical-enablement links repeatedly observed in technical literature and incident reports. Each edge expresses a group's capacity to facilitate or condition the activation of another with causal meaning (not mere chronological succession). The structure supports the incorporation of emerging techniques as instances or, where appropriate, as new edges without reopening the base ontology. The result is directly integrable with STIX 2.1/TAXII 2.1, can be annotated in MISP, and is compatible with VERIS/CASE for operational exchange and correlation (CIRCL, 2025; C. Community, 2025; V. Community, 2025; TC, 2025a, 2025b).

5 Discussion

The increasing sophistication of cyberattacks demands models capable of reflecting the strategic interplay between techniques. Traditional taxonomies, while useful for cataloguing behaviours, often fail to represent how tactics interact during incident progression (Hutchins et al., 2011; MITRE, 2025). Many intrusions follow coordinated chains, where early actions enable more damaging phases (Alrwais et al., 2016; Connolly & Wall, 2019). Social engineering methods such as phishing are frequently used to gain credentials or introduce malicious payloads, which often lead to deeper compromise of critical systems (Bhardwaj & Sapra, 2020; Sedano Pinzón, 2024). Similarly, exploiting software vulnerabilities facilitates privilege escalation and persistence in sensitive environments (Clavijo Mesa et al., 2024; Wu et al., 2021).

The relational taxonomy proposed here addresses these limitations by mapping how one technique facilitates others within multi-stage attacks. It includes eight attack groups and twenty relationships derived from documented cases, enabling flexible representation of complex scenarios.

This adaptability is key when analysing emerging threats such as supply chain compromises or attacks in cloud-based infrastructures. By linking new behaviours to existing groups, the model avoids constant reclassification while maintaining consistency (ENISA, 2021; Hutchins et al., 2011).

Concrete examples reinforce its relevance. Malware like Lucifer combines cryptojacking, denial of service and exploitation in a single campaign (Networks, 2025; Salim et al., 2019). IoT botnets, exploiting protocol and firmware weaknesses, demonstrate how limited-entry vectors can lead to large-scale compromise (Gelgi et al., 2024). Protocol-based threats also support industrial espionage through data interception (Clavijo Mesa et al., 2024; Javeed et al., 2020).

Human factors remain central. Training and awareness have been shown to reduce social engineering effectiveness (Hellemann, 2023; Nassir et al., 2025). Existing frameworks like CASE or MISP offer structural approaches but lack the flexibility to capture threat progression in operational contexts (CIRCL, 2025; C. Community, 2025).

5.1 Case-led validation and scalability

The validity of the approach is evident in Stuxnet, where an APT-type operation established persistence, industrial-environment awareness, and evasion to enable a direct impact on OT infrastructure. The intrusion combined zero-day vulnerabilities, stolen certificates, and stealth techniques to infiltrate SCADA and alter Siemens PLCs, covertly modifying centrifuge process parameters; in the taxonomy, this path is modelled as APTs and Cyberespionage → Attacks on Critical IT/OT Infrastructure, confirming the directionality and causal meaning of the proposed relationship (Shakarian, 2012). The robustness of the network is reinforced by other campaigns that cover distinct edges of the graph: the WannaCry case illustrates Malware-Based Attacks → Attacks on Protocols and Communications by propagating the worm through an SMBv1 exploit (Smart, 2018); additionally, Mirai evidences Malware-Based Attacks → Network Infrastructure Attacks by compromising IoT devices and launching DDoS against network services (Cloudflare, 2022); and Sea Turtle shows Attacks on Protocols and Communications → Network Infrastructure Attacks/APTs via DNS hijacking that sustains covert and persistent access (CISCO, 2019). Maintaining a fixed conceptual base of eight nodes (groups) and twenty edges (relationships) facilitates scalability: operational growth comes from instances and relationship weights as events and sectors are incorporated, preserving structural coherence without relying on specific operational minutiae.

5.2 Integration with Standards and Knowledge Graphs

Each group is modelled as an abstract entity in STIX 2.1 (attack-pattern, malware, intrusion-set, or infrastructure, depending on role) and each of the twenty relationships as a directed enablement link

between entities. Distribution via TAXII 2.1 allows updatable collections where new evidence adds edges or annotations without modifying the base ontology (TC, 2025a, 2025b). In MISP, the taxonomy is annotated via a relational taxonomy/galaxy and coexists with MITRE ATT&CK to maintain TTP ↔ group traceability (CIRCL, 2025; MITRE, 2025). In knowledge graphs, the groups are functional nodes and the edges encode directed enablement with evidence/confidence attributes; this enables queries for probable paths, pivot-node detection, and flow analysis over incidents annotated with VERIS/CASE (C. Community, 2025; V. Community, 2025).

6 Conclusions

This work shows cyberattacks are interrelated sequences enabling escalation, not isolated actions. Addressing prior taxonomy limits, we proposed a relational model (8 groups, 20 relationships) capturing the dynamic complexity of real incidents.

The model contributes to understanding attack organization and progression by explaining technique interdependencies, helping identify patterns across various environments, including critical infrastructures. Organizationally, the model aids early detection and response. Analysing technique interaction helps anticipate attack evolution and mitigate impact, enabling efficient, coordinated responses and resource allocation, fostering preventative cultures.

Socially, the model highlights the human factor in social engineering and credential mismanagement. It underscores investigating human/technical vulnerability interactions and promotes awareness /training programs to foster good practices and reduce susceptibility to manipulation like phishing.

Limitations exist: the theoretical basis continues to be tested in operational threat environments. Constant threat evolution necessitates regular updates for ongoing adaptability. Future research includes (i) modeling the eight identified groups to empirically analyze characteristic attack behaviors, (ii) establishing explicit STIX 2.1 representations by formally defining entities, relationships, and inference rules, and (iii) validating the taxonomy's scalability in high-volume, real-time environments (e.g., SOC operations), where its performance has not yet been fully demonstrated.

Acknowledgments

This work has been developed within the "Recovery, Transformation and Resilience Plan", project C084/23 Ada Byron INCIBE-UAH, funded by the European Union (Next Generation).

References

Alrwais, S., Yuan, K., Alowaisheq, E., Liao, X., Oprea, A., Wang, X., & Li, Z. (2016). *Catching predators at watering holes: finding and understanding strategically compromised websites*. https://doi.org/10.1145/2991079.2991112

Álvarez, A. L., Cruz, J. A., Cruz, S. B., Gallardo, J. d. C., López, I. M., & García, R. E. (2024). El phishing como amenaza en la ciberseguridad corporativa de grandes empresas. *Investigaciones Latinoamericanas en Ingeniería y Arquitectura* (1), 26-33. https://doi.org/10.51378/ilia.vi1.8496

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Comput Secur, 111*, 102490. https://doi.org/10.1016/j.cose.2021.102490

Bhardwaj, A., & Sapra, V. (2020). Why is phishing still successful? *Computer Fraud & Security, 2020*, 15-19. https://doi.org/10.1016/S1361-3723(20)30098-1

Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The Diamond Model of Intrusion Analysis* (ADA586960).

CIRCL. (2025, 2025-03-19). *MISP taxonomies and classification as machine tags.* CIRCL.LU. Retrieved 19-mar-2025 from https://www.misp-project.org/

CISA, & FBI. (2021). *TrickBot Malware* (AA21-076A). https://www.cisa.gov

CISCO. (2019). *Threats of the Year: A look back at the tactics and tools of 2019* (Cisco Cybersecurity Series 2019. Threat Report, Issue. http://www.cisco.com/go/securityreports

Clavijo Mesa, M. V., Patino-Rodriguez, C. E., & Guevara Carazas, F. J. (2024). Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains. *Information*, 15(11). https://doi.org/10.3390/info15110710

Cloudflare. (2022). *DNS and the Threat of DDoS*.

Community, C. (2025, 2025-03-19). *CASE: Cyber-investigation Analysis Standard Expression*. CASE Community. Retrieved 19-mar-2025 from https://caseontology.org/

Community, V. (2025, 2025-03-19). *VERIS: Vocabulary for Event Recording and Incident Sharing*. VERIS Community. https://verisframework.org/

Connolly, K., Klempay, A., McCann, M., & Brenner, P. (2023). Dark Web Marketplaces: Data for Collaborative Threat Intelligence. *ACM Digital*

Threats: Research and Practice, 4(4). https://doi.org/10.1145/3615666

Connolly, L., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security, 87*. https://doi.org/10.1016/j.cose.2019.101568

ENISA. (2021). *ENISA Threat Landscape for Supply Chain Attacks*. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf

Gelgi, M., Guan, Y., Arunachala, S., Samba Siva Rao, M., & Dragoni, N. (2024). Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. *Sensors (Basel),* 24(11). https://doi.org/10.3390/s24113571

Hellemann, N. (2023). *Human Risk Review 2023* [Report]. S. A. GmbH. https://www.sosafe-awareness.com/

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Leading Issues in Information Warfare & Security Research,* 1(1), 80-106. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Ivanov, M. A., Kliuchnikova, B. V., Chugunkov, I. V., & Plaksina, A. M. (2021). *Phishing Attacks and Protection Against Them 2021* IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus),

Javeed, D., MohammedBadamasi, U., Ndubuisi, C. O., Soomro, F., & Asif, M. (2020). Man in the Middle Attacks: Analysis, Motivation and Prevention. *International Journal of Computer Networks and Communications Security*, 8(7), 52-58. https://doi.org/10.13140/RG.2.2.22752.81928

MITRE. (2025). ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge. In: MITRE Corporation.

Nassir, N. F. M., Rauf, U. F. A., Zainol, Z., & Ghani, K. A. (2025). Revealing the multi-perspective factors behind insider threats in cybersecurity. *Journal of Media and Information Warfare*, 17(2), 65-82.

Networks, P. A. (2025). *Lucifer: New Cryptojacking and DDoS Hybrid Malware Exploiting High and Critical Vulnerabilities to Infect Windows Devices*. https://unit42.paloaltonetworks.com

Niño, F. Y. Á. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes,* 24(49). https://doi.org/10.15517/isucr.v24i49

Rauf, U., Mohsen, F., & Wei, Z. (2023). A Taxonomic Classification of Insider Threats: Existing Techniques, Future Directions & Recommendations. *Journal of Cyber Security and Mobility.* https://doi.org/10.13052/jcsm2245-1439.1225

Salim, M. M., Rathore, S., & Park, J. H. (2019). Distributed denial of service attacks and itsdefenses in IoT: a survey. *The Journal of Supercomputing*, 76(7), 5320-5363. https://doi.org/10.1007/s11227-019-02945-z

Sedano Pinzón, J. J. (2024). El contexto actual e histórico de la ingeniería social. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades,* 5(5). https://doi.org/10.56712/latam.v5i5.2691

Shakarian, P. (2012). Stuxnet: Revolución de Ciberguerra en los Asuntos Militares. *Air and Space Power Journal*.

Smart, W. (2018). *Lessons learned review of the WannaCry Ransomware Cyber Attack*.

TC, O. C. T. I. (2025a). STIX Version 2.1. Committee Specification 02. In: OASIS.

TC, O. C. T. I. (2025b). TAXII Version 2.1. Committee Specification 01. In: OASIS.

Wu, Q., Zhang, S., Zheng, B., You, C., & Zhang, R. (2021). Intelligent Reflecting Surface-Aided Wireless Communications: A Tutorial. IEEE *Transactions on Communications,* 69(5), 3313-3351. https://doi.org/10.1109/tcomm.2021.3051897