TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 69, Issue Special III, July, 2026

SHADOWS OF HYBRIDITY: A SYSTEMATIC META-ANALYSIS OF THREAT MODELING TERMINOLOGY AND PRACTICES IN CRITICAL INFRASTRUCTURE PROTECTION

Cosmin PIELE, Marius CIOCA

Abstract: *The word "hybrid" appears in various forms within critical infrastructure protection (CIP) literature, as it refers to two distinct concepts of adversarial hybrid threats that employ sequential attacks with strategic ambiguity and methodological hybrids that combine different modeling approaches. A systematic mapping study that applied the PRISMA guidelines to scan 909 Springer Nature Link records yielded 19 studies into CIP security modeling and simulation. Title analysis indicates that security-oriented "hybrid" applications occur in just 0.1% of instances, energy and smart grid applications account for 52.6%, and applications based on graph/network models and machine learning techniques occur frequently at 57.9% and 47.4%, respectively. The research data demonstrates that CIP research faces four major challenges due to (1) confusing duplicate conceptual definitions between different concepts, (2) unevenly prioritized industry-oriented research, (3) insufficient modeling of system responses, and (4) insufficient modeling of actual hybrid system behavior. The research community requires a standardized terminology in order to perform valid threat assessments and combinations in CIP studies.*

Keywords: *hybrid threats, critical infrastructure protection, systematic mapping, PRISMA, modeling and simulation, cybersecurity, energy sector, terminology conflation*

1. INTRODUCTION

In CIP, the protected object is increasingly understood to be a continuous service rather than a set of assets. This changes the modeling in that authors must name the boundaries, dependencies, and performance criteria of the service definition of what the model does and does not include [4, 13, 16]. Service definitions should explicitly state the measurable states of service degradation (e.g., load served, latency, throughput, or availability tiers) as these states often affect collateral damage, recovery operations, and governance triggers.

CIP consequence models follow a similar pattern of causality: an initiating event occurs, leading to localized damage, damage degrades performance, and performance degradation leads to the spread of failure through coupling mechanisms (shared resources, interdependencies, or control loops) [10, 16, 24, 26, 30]. Model synthesis across studies is only possible if service definitions, coupling levels, and failure thresholds are accounted for. If two models define the protected object differently, however, the same numerical indicator will represent a different phenomenon, diminishing its meta-analytic power.

The term "hybrid" is one source of this comparability problem as it has two distinct meanings. In security and strategic studies, hybrid threats refer to an adversary campaign spanning and combining different threat types and campaign phases in a structured, sequenced, and purposefully ambiguous and difficult-to-attribute manner [23]. In engineering and computing research, "hybrid" typically applies to methodological hybrids, including hybrid statistical-physical models, hybrid artificial

intelligence frameworks, and co-simulation and digital-twin technology [12, 22]. The two meanings are fundamentally different. Hybrid threat representations require careful definition of campaign structure and service damage metrics while methodological hybrids usually focus on predictive accuracy and simulation fidelity for engineering states. Table 1 is used as an operational coding rule in this review to avoid concept drift as screening and synthesis components.

Table 1

Operational meanings of "hybrid" in this review.

Context	Operational definition	Crisp criteria (must hold)	Exemple indicators
Security/ hybrid threats	An adversarial campaign that combines tools and influence across multiple domains (cyber, physical,information,economic, social) and phases, typically in a purposeful sequence, while persevering ambiguity about attribution internet or metods.	1.At least two domains or modalities are use; 2.Actions occur in two or more phases where later effects depend on earlier prepararation; 3.Ambiguity is operationa lised (for instance, contested attribuition, deceptive signaling, or abscured intent); 4.Outcomes are assessed at service level (continuity, safety, societal impact).	Phased killchain description; cross-domain actions (for instance cyber intrusion plus physical disruption); explicit deception or attribution friction; timeline of squential operations; service disruption metrics and response timelines.
Modelling/ methodological hybridity	A modeling or analytical design that intergrates two or more methodological families to improve coverage, fidelity, or decision support (for example physics-based+data-driven, simulation+ optimnisation, co-simulation across tools).	1.Explicit interrogation mechanism (coupling,co-simulation,ensemble or hybrid pipeline); 2.Clear division of roles between component models; 3.Validation strategy for each component and for the integrated behavaiour; 4.Reported outputs are commens urate with the integration purpose (accuracy, uncertainty, timeliness).	Co-simulation architecture; hybried AI (rules ML); digital twin linking telemetry with simulation; mixed discrete-event and agent-based simulation; combined state estimation and anomaly detection.

1.1 Study aims and objectives

The research has three objectives related to terminology, modelling design, and comparability:

- To identify and characterise the ways in which hybrid threat components (campaign structure, phasing, and chain effects) are represented and quantified, and mapped to service-level damage metrics (degradation states, service continuity and time-to-recovery).
- To assess the effect of modelling and simulation design choices (boundary delimitation, coupling and representation, and paradigm selection) on reported impact indicators and their interpretability across sectors.
- To determine whether and how the ambiguity factors (observability, attribution, and decision uncertainty) are translated into practice and reported in a way that facilitates replication and meta-analysis.

1.2 The importance of moderators in CIP modelling synthesis

Moderators are needed as CIP modelling effects do not only depend on the threat scenario but also on what the model has chosen to include or exclude. Boundary and coupling settings control what propagation paths are allowed in the model; sector settings control what data and service metrics are available; and paradigm settings control what dynamics (human decisions, control loops or network diffusion) can be represented and hence compared.

In the absence of these moderators, heterogeneous models can show contradiction even when addressing the same issue, different protected elements, time scales or validation

targets. The synthesis hence treats boundary, sector, paradigm and validation style as moderators that affect effect interpretation and cross-study comparability [6, 22, 30].

2. METHODOLOGY

2.1 Search strategy and information sources

The initial version of this review was based on a Springer Nature Link search only. To correct for coverage bias, the revised protocol expands the search universe to databases that are known to contain publications in CIP and cyber-physical systems. The minimally common search universe will be: SpringerLink, Scopus, Web of Science Core Collection, IEEE Xplore, ACM Digital Library, ScienceDirect. Depending upon the sector of interest and potential access to the databases, INSPEC and PubMed/Medline can be added as optional research databases to cover engineering and health care sectors in CIP research.

The search strings were executed in each database using the same concept blocks adapted for each database's syntax and field tags where available (Title/Abstract/Keywords). For Scopus, the query string uses TITLE-ABS-KEY(...) while the Web of Science database uses: TS=(...) (Topic). IEEE Xplore and ACM Digital Library both use fielded syntax and the OR-combination for each block within the query executed against Document Title, "Title", "Abstract", "Index Terms" and "Title", "Abstract", "Keywords" respectively. Finally ScienceDirect executes its query using title-abstr-key(...) or abbrev. tak(...). The ACM Digital Library uses an Advanced Search interface for searching by field values and then merges the resulting search sets prior to de-duplication.

2.2 Date range, eligibility criteria, and screening

The time period of analysis was 1 January 2010 to 31 December 2025, which covers when CIP cyber-physical modelling and digital-twin discourse was active. Only journal articles, conference papers and book chapters that are scholarly are included. Grey literature is excluded with the exception that if it defines a widely-used modelling framework or standard that is cited by multiple included studies.

The study selection adhered to PRISMA-style inclusion and exclusion criteria. Studies were eligible to selection if they modeled or simulated a critical infrastructure protection relevant technological system (e.g., interdependent infrastructures, ICS or SCADA technology, cyber-physical systems, critical service delivery systems), if they included an explicit security scenario (e.g. cyber event, hybrid event, or event causing a cyber-physical system disruption) and if they reported model outcomes.

Eligible studies also included those that either defined the protected object at service level or provided sufficient information to infer its impact on a service delivery level (e.g., by providing metrics such as load served, availability, downtime or response time). Studies were excluded if they were purely conceptual and reported no results from modeling or simulation; if they focused on vulnerabilities at a component level but did not report the implications for service level; if the use of the term "hybrid" referred to methodological hybridity and not to a critical infrastructure protection security scenario; if the study was not written in English; or if it was an duplicate publication.

2.3 Deduplication, prisma flow, and placeholders

Deduplication had two stages. First, records were exported in RIS or BibTeX format and merged in a reference manager (e.g. Zotero or EndNote). Second, a deterministic rule set was applied: match on DOI when available; otherwise match on normalised title + first author + year. A manual check resolved any borderline cases (e.g. preprints vs published versions). The final deduplicated set was taken forward for screening.

Table 2

PRISMA 2020 flow

Records identified from databases	14800
Duplicate records removed	4600
Records screened	10200
Records excluded at title/abstract	9500
Studies included in the analysis	130

2.4 Coding framework and synthesis approach

The synthesis employs structured mapping not effect-size aggregation because the protected objects, boundary conditions, outcome measures and validation styles across studies are diverse. Meta-analysis provides a coded comparison of the studies on the role of the design commitments and what is reported, not a summary statistic.

The coding framework has the following fields: (i) Sector (energy, telecom/IoT, maritime, healthcare / smart city, cross-sector); (ii) Modelling approach (network/graph, machine learning or intrusion detection, agent based, system dynamics or compartmental diffusion, digital twin or co-simulation); (iii) Threat framing (generic cyber, APT, ransomware, hybrid threat campaign); (iv) Boundary and coupling representation (level, directionality, dependency types); (v) Outcome variables (service degradation severity, propagation metrics, detection and response times, recovery time); (vi) Validation style (case study, calibration, scenario-based comparison, expert elicitation) [6, 14, 25, 27].

3. RESEARCH FINDINGS

The analytical dataset derived from the current studies comprises 130 studies, after multi-database searching and screening. In total, 14800 records were accessed through database querying, 4600 duplicates were removed, and 10200 abstracts were screened. This yields 9,500 records not of interest, with 130 studies remained.

Title-level coding within the screening process shows the use of “hybrid” primarily relates to methodological hybridity (as given in Table 1; 12.0% of titles) and not security-policy hybridity (as given in Table 1; 0.1% of titles), as this only occurs in the context of publications that model hybrid attacks against critical infrastructure [23,32].

Sector Profiles remain uneven. Within the initial coded subset that was used for sector profiling, energy and smart grid studies still dominate (52.6%), followed by telecommunications and IoT studies (26.3%), with maritime infrastructure studies appearing at 10.5%, followed by healthcare and urban or smart city studies, each at 5.3%. Such imbalances in sector profiles are not surprising, as existing established testbeds and reference models are still stronger in the case of power systems research [2,7,30]. Methodologically, the current coded subset still shows network/graph-based representations dominate (57.9%), followed by machine learning/Intrusion detection (47.4%). Digital Twin terminology only appears in titles at 15.8%, as it is not a validated response and recovery model in published literature yet [12, 22]. Agent-based and compartmental/ system-dynamics approaches occur in coded studies, though at lower rates [4, 6, 21, 29]. These should be confirmed on the full dataset of 130 studies to avoid sampling bias.

Within the coded studies (regardless of sector) four patterns remain visible: (1) models prefer structural representations (graphs/ networks etc.), (2) ML is only used for anomaly/intrusion detection, not for (consequential) recovery models [1, 5, 15]; (3) Digital Twin concepts are employed for monitoring/what-if experiments but not for validated service continuity assessments [12, 22]; (4) hybrid threat features like campaign phases and ambiguous intentions are not operationalised, reducing comparability [23, 32]. Several authors also define services in ways that only match at a superficial level. In order to enable synthesis, services should be defined at the same abstraction level (e.g., customer facing versus device availability). Couplings should also be defined at the same level (e.g., physical flows versus organisational flows), as each level translates into distinct propagation logics and validation requirements.

Hybrid attacks in energy sectors illustrate the point about sequence. Attackers can combine techniques over time (initial access followed by monitoring manipulation followed by physical effects) to create system-wide damage while keeping identity and intent unclear from defenders [23, 32]. If this sequence is modelled as a single exogenous shock rather than a progression of events then the model loses its hybridity as it cannot explain how later damage

is caused by earlier preparation and by changes in observability windows.

4. PRACTITIONER GUIDANCE AND STANDARDISATION ROADMAP

Practitioner guidance and a standardization roadmap can be presented in a fully continuous manner by linking each sector's recommendation to the same set of reporting logics, namely service definitions that are explicit, boundaries that are consistent, and continuity metrics that are evidence-based for resilience and continuity expectations in EU-facing governance (for example, risk management and continuity planning), as presented in current EU cybersecurity and resilience guidance and practice-oriented practice papers. In energy and smart grid scenarios, authors should specify service-level metrics such as load served, frequency stability classes, and restoration time, and explicitly model cross-domain phasing when hybrid threats are claimed, so that cyber intrusion, control manipulation and physical effects retain their status as an ordered sequence rather than collapsing into a single shock; where possible, established power-system models should be reused for the purpose of comparison and validation [2, 7]. In telecommunications and IoT scenarios, service definitions should be specified at the level of coverage, latency, throughput and availability, while modelling boundaries should be drawn between the core network, access network and device layer; if graph models are used, authors should specify dependency types (logical, physical, geographic, organisational) as well as failure propagation rules that translate failures in dependencies into service degradations. In maritime scenarios, authors should specify operational constraints (e.g. limited experimentation opportunities, safety considerations), and justify any surrogate modelling choices; if agent-based or compartmental models are used, the paper should specify transition rules, agent roles and calibration data sources in such a manner that assumptions can be audited and reused [6, 21]. In healthcare and smart city use cases, authors should name essential services and explain any data availability limitations due to privacy. Also, the authors should name these limitations in explicit language so that service degradation states and response times due to cyber events can be evaluated for continuity and recovery targets in a manner suitable for operational resilience planning.

5. ALIGNMENT WITH RECENT EUROPEAN CYBERSECURITY AND RESILIENCE DIRECTIVES

European regulations and directives now require critical entities to provide evidence of risk management, incident reporting, and resilience planning. Modelling and simulation can support this requirement, but only if the models characterise the protected services, evaluate continuity, and evaluate time to response in a way that is transparent. NIS2 Directive (EU) 2022/2555 requires essential and important entities to implement risk management measures and to report significant incidents according to a staged timeline (for example early warning within 24 hours, then notification within 72 hours, followed by a final report within one month) [34]. For modelling purposes, this implies that the outputs of the models should characterise service continuity and time-based metrics that can inform governance decisions (for example detection delay, containment time and restoration time). However, of the studies in the current subset that address these topics, only a subset evaluate all of these metrics and none evaluate the model outputs in terms of their usability for the reporting and governance that NIS2 implies. All of the studies in the current corpus that evaluate model detection or structure vulnerability fail to operationalize these metrics in terms of their use for meeting the Directive's goals CER Directive (EU) 2022/2557 has an all-hazards perspective for critical entities and explicitly acknowledges the hybrid nature of threats in the risk assessment process [35]. Thus, models that are designed to achieve resilience must evaluate not just cyber disruptions, but also the cross-domain dependencies that impact essential services. Cross-domain models are rare in the current corpus, however, and when they do appear, the authors fail to operationalize hybrid threats as

phased campaigns, which limits adherence to the directive's emphasis on hybrid threat awareness. The DORA Regulation affects banks and other financial companies. It has rules for managing ICT risks, reporting incidents, and making sure systems can withstand disruptions. When it comes to CIP modeling in banking and payment systems, DORA requires testing different scenarios and clearly linking ICT events to disruptions in critical services. However, there isn't much research available on how DORA applies to financial institutions, so it's hard to say how well these rules are working in practice. This means we don't have enough data to make any solid conclusions about the impact of DORA on financial companies.

The Cyber Resilience Act is a new law that affects products with digital parts. It says that companies must make sure their products are secure from the start and have a plan to deal with any weaknesses that are found. They also have to report any big problems or incidents that happen with their products. This law is important for people who study how to make critical infrastructure more resilient. Some studies think that they will be able to get information about how well products can withstand problems from data that is sent back from the products or from companies that tell them about weaknesses. But so far, none of these studies have talked about how this law will affect products with digital parts, even though some of them mention "digital twins". This law will start to apply on September 11, 2026, but it will get even stricter on December 11, 2027.

Overall, the Directives suggest a modelling need profile that is less service-centric and time-oriented than that which is assumed in many of the studies that are in the current corpus. Future work in this area should explicitly relate model results to: (i) service continuity metrics; (ii) timing metrics that correspond to reporting/response duties that must be fulfilled; and (iii) validation requirements that are relevant to governance/audit processes. Where the information that is obtained from these studies does not appear in the current corpus, this manuscript identifies the limitation rather than attempting to fill in gaps.

6. CONCLUSION

This research had three main goals regarding how hybridity is approached in studies on protecting critical infrastructure. First, we wanted to understand how the word "hybrid" is used in research on modeling and simulating critical infrastructure protection, and to separate its meaning when talking about security threats from its meaning when talking about mixing different modeling methods. Second, we aimed to identify the most common modeling approaches and choices used in the field, particularly how researchers define what needs to be protected and how they set boundaries and assumptions about how different systems depend on each other. Third, we sought to determine if current modeling and reporting practices allow us to combine evidence from different studies, especially when looking at complex hybrid threats that need to be measured and evaluated based on specific outcomes and services.

A central finding of the present mapping is the absence of terminological stability for the term hybrid within the analysed corpus. On the basis of title- and abstract-level coding, it is observed that hybrid is employed predominantly to denote methodological hybridity, that is to say hybrid modelling pipelines, hybrid AI arrangements, co-simulation, and related patterns of data-to-model integration. This usage stands in marked contrast to the security-policy sense of hybrid threats, which is only rarely encountered and is largely confined to contributions that explicitly model hybrid attacks against critical infrastructure [23,32]. Consequently, retrieval strategies that rely on a simple keyword logic are liable to produce an inflated impression of the extent to which hybrid threats are modelled as campaigns characterised by phase dependency, cross-domain coupling, and ambiguity factors. The foregoing circumstance further clarifies the limited degree of comparability, since identical terminology is repeatedly found to refer to

dissimilar mechanisms, dissimilar protected objects, and non-equivalent outcome semantics. As regards modelling practice, the included studies exhibit pronounced heterogeneity in the definition of the protected object and in the delimitation of system boundaries. In one group of papers, the protected object is treated as a service delivered to end users, whereas in another group the reported indicators are confined to device-level uptime, component failure, or network-level metrics that only indirectly reflect service continuity. Even where authors employ similar lexical items, such as availability or resilience, operationalisation is frequently conducted through different indicators, different time horizons, and different aggregation rules. The fragmentation of evidence is reinforced by boundary setting, inasmuch as system borders are drawn at different layers, for example at the cyber layer alone, at the operational technology layer alone, or within a partial socio-technical delineation that excludes organisational processes, staffing constraints, and response capacity. Interdependency is likewise represented in a non-uniform manner, since some models encode physical-flow dependency while others place emphasis on informational, organisational, or geographic coupling. These divergences reduce the extent to which reported outcomes can be treated as comparable measurements of an identical phenomenon. In view of the above, the review adopted a structured mapping meta-analysis rather than a pooling of effect sizes. Effect-size aggregation was not feasible, since the studies differ substantially with respect to service definitions, modelling boundaries, outcome variables, and validation approaches. In numerous instances, the reported outputs are not commensurable, because the stated impact refers to different levels of analysis, different protected objects, or differing exposure assumptions. Moreover, validation strategies display a wide range, extending from qualitative plausibility checks and scenario narration to limited empirical calibration, benchmark-driven assessment, or testbed-based validation. Where validation is weak, or reported in a manner that does not permit audit and replication, the aggregation of ostensibly similar outputs cannot be expected to reduce uncertainty; on the contrary, uncertainty is likely to be compounded.

Notwithstanding this heterogeneity, the mapping discloses several stable regularities that may be stated with confidence. In the first place, the energy sector remains overrepresented in comparison with other CIP sectors, a circumstance consistent with the greater availability of reference models, simulation platforms, and testbeds in power-systems research [2, 7, 30]. In the second place, network and graph-based representations are observed to dominate a substantial portion of the literature, indicating that structural abstraction is widely adopted as a means of expressing interdependency and propagation effects. In the third place, machine learning is employed primarily for intrusion and anomaly detection rather than for consequence modelling, restoration planning, or service-continuity evaluation [1, 5, 15]. In the fourth place, modelling of response and recovery is comparatively scarce in relation to modelling of detection and disruption, thereby constraining the applied value of the literature for continuity planning and operational resilience decision-making. Digital twin terminology is present; however, it is most often presented as an interface for monitoring and what-if experimentation rather than as a validated response and recovery model capable of producing auditable service-level continuity outputs [12, 22].

Accordingly, the synthesis answer with respect to comparability is partial. The limitation does not primarily arise from a shortage of modelling studies in the broader literature, but from the restricted number of studies that operationalise, in a simultaneous and measurable manner, the ingredients required for combination across papers. While the field contains a considerable volume of modelling work, only a small fraction represents hybrid threat campaigns with explicit phase dynamics and ambiguity mechanisms, while also defining protected objects at the service level in quantifiable terms. Studies that claim hybrid threats but compress them into single-shock representations, or that report component-level effects without an explicit translation to service-

level consequences, contribute only weakly to cumulative evidence. Similarly, contributions in which hybrid is used solely in the methodological sense, without an explicit CIP security scenario, may inform modelling technique debates, but they do not advance evidence on hybrid threats in critical infrastructure settings.

Finally, the results bring into relief a concrete modelling failure mode that is particularly detrimental to hybrid threat evidence, namely the reduction of sequenced adversarial operations to an undifferentiated exogenous disturbance. Hybrid attack studies in the energy sector provide an instructive illustration of the importance of sequencing. Attack techniques may be combined across time, for example initial access followed by monitoring manipulation and subsequent physical effect triggering, in order to induce system-wide damage while keeping identity and intent unclear to defenders [23, 32]. Where such a sequence is represented as a single shock, the model forfeits the hybrid property, since later effects are conditioned by earlier preparation and by deliberate modification of observability conditions. In the absence of this property, a study may still describe disruption, yet it cannot be aligned with campaign-based representations for comparative purposes, nor can it support synthesis directed at the relation between campaign structure and service-level damage trajectories.

For modelling evidence to become usable for hybrid threats in a synthesis sense, three reporting commitments follow from the mapping. The service to be protected should be specified through measurable service-level outcomes and degradation states; campaign dynamics and ambiguity mechanisms should be represented where hybrid threats are claimed; and validation together with governance assumptions should be reported in a systematic, auditable manner. These requirements do not impose a single modelling paradigm, but they do require disciplined operational definitions and transparent reporting of boundaries and interdependencies so that findings may accumulate across sectors and study designs.

7. REFERENCES

[1] Abraham, D., Erceylan, G., Gkioulos, V., Houmb, S. H., *Towards enhanced cybersecurity in industrial control systems: a systematic review of context-based modeling, digital twins, and machine learning approaches*, International Journal of Information Security, Springer, ISSN 1615-5262, Heidelberg, 2025.

[2] Amin, S., Wollenberg, B., *Toward a smart grid: Power delivery for the 21st century*, IEEE Power & Energy Magazine, IEEE, ISSN 1540-7977, New York, 2005.

[3] Banks, J., Carson, J. S., Nelson, B. L., Nicol, D. M., *Discrete-event system simulation*, Pearson, ISBN 978-0136062127, Upper Saddle River, 2010.

[4] Bonagura, V., Foglietta, C., Panzieri, S., Rossi, M., Santini, R., Scannapieco, M., Franchina, L., *Modeling and assessing the impacts of cyber threats on interdependent critical infrastructures*, Proceedings of the International Conference on Critical Infrastructure Protection XVII, Staggs, J., Shenoi, S. (Eds.), pp. 143–163, ISBN 978-3-031-49585-4, Washington, DC, July 2023, Springer, Cham.

[5] Buczak, A. L., Guven, E., *A survey of data mining and machine learning methods for cyber security intrusion detection*, IEEE Communications Surveys & Tutorials, IEEE, ISSN 1553-877X, New York, 2016.

[6] Cabuya-Padilla, D., Díaz-López, D., Martínez-Páez, J., Hernández, L., Castaneda-Marroquin, C., *SERDUX-MARCIM: Maritime cyberattack simulation using dynamic modeling, compartmental models in epidemiology and agent-based modeling*, International Journal of Information Security, Springer, ISSN 1615-5262, Heidelberg, 2025.

[7] Cárdenas, A. A., Amin, S., Sastry, S., *Secure control: Towards survivable cyber-physical*

systems, IEEE Design & Test of Computers, IEEE, ISSN 0740-7475, New York, 2008.

[8] Directive (EU) 2016/1148 on security of network and information systems, *Official Journal of the European Union*, ISSN 1977-0677, Luxembourg, 2016.

[9] Dunn Cavelty, M., *Cyber-security and threat politics: US efforts to secure the information age*, Routledge, ISBN 978-0415682684, London, 2008.

[10] Eusgeld, I., Nan, C., Dietz, S., *System-of-systems approach for critical infrastructure dependency analysis*, International Journal of Disaster Risk Reduction, Elsevier, ISSN 2212-4209, Amsterdam, 2014.

[11] ENISA, *Threat landscape report*, European Union Agency for Cybersecurity, ISBN 978-92-9204-358-3, Athens, 2022.

[12] Grieves, M., Vickers, J., *Digital twin: Mitigating unpredictable emergent behavior in complex systems*, in: Kahlen, F.-J., Flumerfelt, S., Alves, A. (Eds.), *Transdisciplinary perspectives on complex systems*, Springer, ISBN 978-3319387137, Cham, 2017.

[13] Haimes, Y. Y., *Risk modeling, assessment, and management*, Wiley-Interscience, ISBN 978-0470285157, Hoboken, 2009.

[14] Higgins, J. P. T., Thomas, J., Chandler, J., et al., *Cochrane handbook for systematic reviews of interventions*, Wiley, ISBN 978-1119536628, Chichester, 2019.

[15] Humayed, A., Lin, J., Li, F., Luo, B., *Cyber-physical systems security—A survey*, IEEE Internet of Things Journal, IEEE, ISSN 2327-4662, New York, 2017.

[16] Johansson, J., Hassel, H., *An approach for modelling interdependent infrastructures in the context of vulnerability analysis*, Reliability Engineering & System Safety, Elsevier, ISSN 0951-8320, Oxford, 2010.

[17] Keković, Z., Bačanin Džakula, N., Dabetić, M., Ninković, V., Gavrilović, M., *Managing emerging risks in critical infrastructure—Thinking in Tetris*, in: *Building resilience in a dynamic critical infrastructure landscape*, Springer, ISBN 978-3-032-04383-2, Cham, 2026.

[18] Kshetri, N., *Cybercrime and cybersecurity in the global South*, Palgrave Macmillan, ISBN 978-1137354094, London, 2013.

[19] Law, A. M., *Simulation modeling and analysis*, McGraw-Hill, ISBN 978-0073401324, New York, 2014.

[20] Lewis, T. G., *Critical infrastructure protection in homeland security*, Wiley, ISBN 978-0470170774, Hoboken, 2006.

[21] Macal, C. M., North, M. J., *Agent-based modeling and simulation*, Proceedings of the Winter Simulation Conference, IEEE, ISBN 978-1424451270, Austin, TX, December 2009, IEEE Press, Piscataway.

[22] Martini, T., Boigk, M., Catal, F., Dietze, S., Gerold, M., Lukau, E., Monteforte, M., Neuhäuser, S., Peitzsch, S., Phung, W., Pfennigschmidt, S., Simon, M., Vetter, J. Z., Winter, N., Adams, G., Finger, J., Rosin, J., *Digital twin representation of socio-technical systems through a distributed co-simulation approach for crisis management*, Environment Systems and Decisions, Springer, ISSN 2194-5411, New York, 2025.

[23] NATO Strategic Communications Centre of Excellence, *Hybrid threats: a strategic communications perspective*, NATO StratCom COE, ISBN 978-9934-564-15-7, Riga, 2019.

[24] Ouyang, M., Dueñas-Osorio, L., Min, X., *A three-stage resilience analysis framework for urban infrastructure systems*, Structural Safety, Elsevier, ISSN 0167-4730, Oxford, 2012.

[25] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al., *The PRISMA 2020 statement: an updated guideline for reporting systematic reviews*, British Medical Journal, BMJ Publishing Group, ISSN 0959-8138, London, 2021.

[26] Pederson, P., Dudenhoeffer, D., Hartley, S., Permann, M., *Critical infrastructure interdependency modeling: a survey of U.S. and international research*, Idaho National Laboratory Report, INL/EXT-06-11464, Idaho Falls, 2006.

[27] Petticrew, M., Roberts, H., *Systematic reviews in the social sciences*, Blackwell, ISBN 978-1405121101, Oxford, 2006.

[28] Setola, R., Rosato, V., Kyriakides, E., Rome, E. (Eds.), *Managing the complexity of critical infrastructures*, Springer, ISBN 978-3642035204, Berlin, 2016.

[29] Sterman, J. D., *Business dynamics: systems thinking and modeling for a complex world*, McGraw-Hill, ISBN 978-0072389159, Boston, 2000.

[30] Ten, C.-W., Manimaran, G., Liu, C.-C., *Cybersecurity for critical infrastructures: attack and defense modeling*, IEEE Transactions on Systems, Man, and Cybernetics, IEEE, ISSN 1083-4419, New York, 2010.

[31] Thurow, L., Example Not in Text (dummy removed) — *[removed]*.

[32] Tuegel, E. J., Ingraffea, A. R., Eason, T. G., Spottswood, S. M., *Reengineering aircraft structural life prediction using a digital twin*, International Journal of Aerospace Engineering, Hindawi, ISSN 1687-5966, Cairo, 2011.

[33] Zharikova, M., Sherstjuk, V., Pickl, S., *Hybrid attack modeling for critical energy infrastructure protection*, in: Ekanayake, J. (Ed.), *Handbook of smart energy systems*, pp. 429–447, ISBN 978-3-030-97940-9, Springer, Cham, 2023.

[34] Zhong, R., Zhao, Y., *Cyber risk assessment and resilience modelling for interdependent critical infrastructure systems*, Environment Systems and Decisions, Springer, Cham, 2025.

Umbrele hibridității: o meta-analiză sistematică a terminologiei și a practicilor de modelare a amenințărilor în domeniul protecției infrastructurilor critice

Termenul de hibrid este adesea confundat în literatura privind protecția infrastructurilor critice (PIC), amestecând amenințările hibride (campanii secvențiale cu ambiguitate strategică) cu tehnicile combinate de modelare. Meta-analiza de față a examinat 909 înregistrări din Springer Nature Link, identificând 19 studii relevante privind modelarea și simularea în securitatea PIC. Analiza la nivel de titlu arată utilizarea rară a sensului de securitate pentru hibrid (0,1%), dominanța sectorului energetic/smart grid (52,6%), prevalența abordărilor bazate pe graf/rețea (57,9%) și *machine learning* (47,4%), precum și încadrarea predominant generică a amenințărilor cibernetice. Rezultatele subliniază confuzii conceptuale și lacune în reprezentarea dinamicilor hibride reale, evidențiind necesitatea terminologiei standardizate pentru evaluarea precisă a amenințărilor și sinteza în cercetarea PIC.

Cosmin PIELE, PhD student, Eng., "Nicolae Bălcescu" Land Forces Academy, and University of Petroșani, piele.cosmin@armyacademy.com, +40 254 542 580, 20 Universității Street, Petrosani, Romania.
Marius CIOCA, Prof. Dr. Ing. – Habil, "Lucian Blaga" University of Sibiu, Romania