Cross-Layer Consequence Propagation in Cyber–Physical Systems: A Multi-Order Effect Framework with Heterogeneous Graph Architecture

Parinay Bansal[1], Ayan Mondal[1], *Senior Member, IEEE*,
Krishan Berwal[2], *Senior Member, IEEE*
[1]*Indian Institute of Technology Indore, India*
[2]*Military College of Telecommunications Engineering, Mhow, India*
parinay.bansal@gmail.com, ayanm@iiti.ac.in, k2b@ieee.org

For Personal Use Only

***Abstract*—Existing cyber-physical systems (CPS) security models predominantly focus on first-order impacts, emphasizing the immediate technical consequences of an intrusion while overlooking cascading cross-domain effects. This paper introduces a formally structured Multi-Order Effect (MOrE) framework that models how cyber operations propagate across interconnected physical, institutional and strategic layers. The proposed framework defines three hierarchical effect orders linked through four propagation mechanisms within a unified five-layer CPS abstraction and incorporates quantitative metrics for severity assessment and controllability evaluation. To operationalize the framework, we develop a heterogeneous graph neural network (HGNN) architecture based on relational graph convolutions that encode typed cross-layer dependencies among CPS entities. This is integrated with a retrieval-augmented large language model (LLM) pipeline to extract institutional and strategic indicators from unstructured incident reports, enabling joint structured–unstructured reasoning. The framework is evaluated on six major cyber operations conducted between 2010 and 2025 (Stuxnet, the Ukraine power grid attack, NotPetya, SolarWinds, Colonial Pipeline and Operation Spiderweb), demonstrating its ability to capture cascading, dependency-mediated and bidirectional propagation patterns not represented in existing taxonomies. Results show improved cross-layer consequence modeling and enhanced prediction of uncontrolled cascading behaviors.**

***Index Terms*—Cyber-physical systems, multi-order effects, graph neural networks, critical infrastructure, cyber operations**

I. Introduction

CPS integrate computational processes with physical mechanisms to enable real-time monitoring, automation and control of critical infrastructure (CI) [1]. Energy grids, water distribution systems, transportation networks and defense manufacturing platforms rely on tightly coupled operational stacks in which supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), field devices and enterprise IT networks interact across layered architectures [2]. Existing CPS security research focuses on first-order effects, the immediate operational consequences of compromise. Prior work has addressed vulnerability classification and threat modeling [3], physics-based intrusion detection [4] and cascading failure analysis within interconnected CPS infrastructures [5], [6]. However, documented cyber operations demonstrate that CPS compromises routinely produce cross-domain cascading effects.

Stuxnet not only damaged centrifuges but delayed a nuclear program and influenced offensive cyber doctrine [7]. The SolarWinds intrusion extended beyond IT compromise to strategic trust erosion and geopolitical implications [8], [9]. Conceptually, Orye and Maennel [10] introduced the notion of first, second and third order cyber effects within a NATO analytical context. A recent systematic review of multidimensional cyber impact quantification [11] confirms this structural gap, concluding that no standardized taxonomy exists for coherently describing impacts across physical, economic, reputational and societal dimensions. Cascading-effect models [5], [6] remain confined to CPS boundaries. Kill chain models [12] describe attacker progression rather than consequence propagation. Strategic analyses [13], [14] examine geopolitical outcomes without formal CPS layer linkage. Cyber harm taxonomies [15] classify multidimensional impacts, however, no existing CPS security framework formally models the propagation mechanisms.

To address this gap, this paper introduces a MOrE framework that formalizes and extends the order-of-effects concept [10] into a structured multi-layer system model. The framework defines explicit propagation mechanisms, quantitative severity and controllability metrics and a computational architecture for learning cross-layer dependencies. By bridging CPS engineering, institutional impact analysis and strategic consequence modeling, the proposed approach provides both analytical structure and predictive capability. The contributions of this work are as follows:

- A multi-layer CPS abstraction extending cascading-effect models beyond physical-operational boundaries into institutional and strategic domains, defines three effect orders, four propagation mechanisms and quantitative metrics for severity scoring and controllability assessment.
- HGNN using relational graph convolutions to encode typed cross-layer CPS dependencies, integrated with a retrieval-augmented LLM pipeline for extracting institutional and strategic indicators from unstructured reports.

Accepted at 4th IEEE International Conference on Computer, Electronics, Electrical Engineering and their Applications (IC2E3-2026).

- Evaluation on six cyber operations spanning two decades, demonstrating the ability to model controlled, uncontrolled and bidirectional propagation patterns across heterogeneous attack vectors.
- Controllability spectrum ranging from precisely targeted to uncontrolled cascading propagation, along with spectral amplification conditions characterizing escalation from localized compromise to systemic strategic impact.

II. Related Work

Understanding cross-layer cyber consequences requires synthesizing insights from CPS security, cyber conflict analysis and computational graph modeling. Existing literature provides strong foundations within each domain. This section reviews prior work across three dimensions: (i) CPS security and cascading models (ii) cyber conflict and strategic consequence analysis and (iii) graph-based computational modeling. We highlight their contributions and identify structural limitations that motivate the proposed MOrE framework.

CPS Security and Cascading Effects: CPS security research has traditionally concentrated on threat taxonomies, vulnerability characterization and operational resilience. Humayed *et al.* [2] provided a comprehensive survey of CPS architectures and associated attack vectors, while Cárdenas *et al.* [3] identified critical gaps between classical IT security models and the timing and safety constraints of industrial control systems. Giraldo *et al.* [4] surveyed physics-based anomaly detection mechanisms that use process invariants and control-theoretic properties. Recent contributions have addressed automated security auditing [16], secure data fusion in defense IoT [17], data integrity protection [18] and IoT security across cryptographic paradigms [19]. Beyond intrusion detection, Palleti *et al.* [5] empirically analyzed cascading disruptions across interconnected CPS and Chockalingam and Maathuis [6] proposed a Bayesian Network (BN) framework for probabilistic cascading assessment. These approaches model dependency-driven degradation within and across CPS sectors but define "effect" exclusively at the physical-operational level. Complementing cascading models, Agrafiotis *et al.* [15] propose a multi-dimensional cyber-harm taxonomy spanning physical/digital, economic, psychological, reputational and societal categories. While this taxonomy broadens the impact lens, it does not embed harms within a layered system architecture nor define formal propagation mechanisms linking CPS compromise to institutional or strategic domains.

Cyber Conflict, Attack Models and Strategic Analysis: At the strategic level, cyber conflict scholarship examines geopolitical and doctrinal implications of cyber operations. Rid [14] characterized cyber operations as forms of sabotage, espionage, or subversion rather than conventional warfare. Schulze and Kerttunen [13] analyzed cyber activities in the Russia–Ukraine conflict, while Broeders and Kavanagh [9] examined cyber intelligence within international security frameworks. These works provide empirical and conceptual grounding for higher-order consequences but do not formalize the technical pathways connecting CPS compromise to strategic outcomes. Operational modeling frameworks focus primarily on attacker progression. Hutchins *et al.* [12] introduced the cyber kill chain model, decomposing intrusions into sequential phases. While MITRE ATT&CK extends this taxonomy to ICS environments, these models describe adversarial behavior and tactics but do not model consequence propagation beyond the compromised system. Orye and Maennel [10] introduced first, second and third-order cyber effects within a NATO CCD COE context, offering the closest conceptual antecedent to multi-order consequence analysis. However, their framework did not define a formal multi-layer system abstraction, explicit propagation mechanisms, quantitative severity metrics, or computational modeling. Governance-oriented standards such as NIST CSF [20] and IEC 62443 [21] provide compliance and risk management guidance but remain process-centric rather than consequence-propagation-centric.

Graph Neural Networks (GNNs) in Security: GNNs offer expressive relational learning capabilities for modeling structured dependencies. They have been applied to intrusion detection, malware classification, vulnerability analysis and dependency modeling in complex systems. In CPS contexts, Zhu *et al.* [22] demonstrates physics-informed GNNs for power-grid cascading failure prediction, representing the most advanced single-layer computational approach for modeling propagation within physical infrastructure. Heterogeneous GNNs extend homogeneous graph models by incorporating typed nodes and relation-specific transformations, enabling representation of multi-relational systems [23]. Despite these advances, no existing GNN models cross-layer consequence propagation spanning CPS infrastructure, nor integrate structured system modeling with unstructured evidence extraction. Table I summarizes coverage of existing approaches and shows the absence of a unified framework combining CPS cascading, strategic consequence modeling and computational propagation prediction.

TABLE I
Analytical Coverage of Existing Frameworks

Framework	CPS	Casc.	Inst.	Strat.	Comp.
CPS Taxonomies [2]	✓	–	–	–	–
Cascading Models [5]	✓	✓	–	–	–
BN Framework [6]	✓	✓	–	–	✓
PI-GNN [22]	✓	✓	–	–	✓
Cyber-Harms [15]	–	–	✓	✓	–
Kill Chain [12]	✓	–	–	–	–
CCD COE Orders [10]	–	✓	✓	✓	–
NIST/IEC 62443 [20], [21]	✓	–	✓	–	–
Strategic Analysis [13]	–	–	✓	✓	–
MOrE (proposed)	✓	✓	✓	✓	✓

Comp. = Computational architecture for propagation prediction.
Casc. = Cascading Effect.
Inst. = Institutional Modelling.
Strat. = Strategic Paradigm.

III. System and Threat Model

Layered System Model: We model a cyber–physical infrastructure as a layered system $\mathcal{S} = \{L_P, L_C, L_E, L_I, L_S\}$, where each layer represents a distinct functional and consequence domain: L_P (Physical Process) Mechanical, electrical,

For Personal Use Only

chemical, or kinetic processes subject to automated control; L_C (Control) PLCs, SCADA systems, field controllers and real-time supervisory software governing L_P; L_E (Enterprise IT): Corporate networks, data infrastructure, supply-chain management and business communications; L_I (Institutional) Organizational governance, regulatory compliance, policy formulation and executive decision-making; and L_S (Strategic) National security posture, alliance dynamics, deterrence equilibria and geopolitical positioning. Inter-layer dependencies are represented as a directed graph $\mathcal{G} = (\mathcal{S}, \mathcal{D})$, where $\mathcal{D} = \{d_{ij} : L_i \to L_j\}$ denotes structural dependence between layers. Importantly, dependency direction does not constrain effect propagation direction. For example, compromise at L_E may propagate downward to L_C via command injection or configuration tampering, or upward to L_I through intelligence exposure and decision disruption. Conventional CPS models restrict analysis to $\{L_P, L_C, L_E\}$. In contrast, we include L_I and L_S as formal system layers, reflecting empirical evidence that large-scale CPS operations routinely produce measurable institutional and strategic consequences.

Threat Model: We assume an advanced adversary with access vectors including supply-chain compromise, zero-day exploitation, credential theft or physical access. Resources for custom malware development, operational security and extended dwell time. Separation between access operations and payload activation. Multi-year operational planning horizons. This threat model is consistent with documented state-sponsored operations [8], [13], [24]. The Colonial Pipeline incident demonstrates that criminal actors may also generate multi-order consequences when systemic dependencies are present.

MOrE Framework: Effect Orders and Boundaries: We define an *effect order* O_k as a class of consequences characterized by (i) causal distance from the initial compromise and (ii) the system layer at which the effect manifests. An *effect boundary* β_k separates adjacent orders; crossing β_k requires a qualitative transformation in consequence domain. The framework defines three effect orders, O_1 *(Direct Effects)* consequences manifesting at L_P, L_C, or L_E, indicators include equipment degradation, service interruption and data exfiltration; O_2 *(Institutional Effects)* consequences at L_E or L_I arising from O_1, indicators include organizational restructuring, regulatory response, trust erosion, reputational damage or intelligence asymmetry; and O_3 *(Strategic Effects)* consequences at L_I or L_S emerging from O_1 and O_2, indicators include shifts in deterrence posture, escalation thresholds, alliance behavior, or long-term strategic doctrine. This structure formalizes cross-domain escalation from technical disruption to systemic strategic impact.

Severity Quantification: Each effect order is assigned a composite severity score $S(O_k) = \alpha_1 D_{phys} + \alpha_2 L_{econ} + \alpha_3 P_{policy}$, where $D_{phys} \in [0,1]$ denotes a normalized physical damage index, $L_{econ} \in [0,1]$ denotes a normalized economic loss index and $P_{policy} \in [0,1]$ denotes a policy or institutional transformation index. Weights satisfy $\alpha_1 + \alpha_2 + \alpha_3 = 1$ and may vary across layers. At O_1, D_{phys} typically dominates; at O_2, economic and institutional effects increase in weight and at O_3, P_{policy} becomes dominant. This weighting structure captures the qualitative shift across effect boundaries.

Propagation Mechanisms: Four mechanisms mediate transitions across effect orders, *Physical Cascade* (ϕ_{PC}) dependency-driven propagation among CPS components. Operates primarily within O_1 and is well studied in cascading-failure literature [5]; *Informational Propagation* (ϕ_{IP}) upward or lateral propagation through data exposure, intelligence extraction, or misperception, enabling transition from O_1 to O_2; *Trust Erosion* (ϕ_{TE}) amplification of institutional consequences via degraded confidence in vendors, partnerships, or governance structures and *Strategic Inference* (ϕ_{SI}) propagation driven by interpretation of observed consequences, influencing deterrence logic and strategic calculus, enabling $O_2 \to O_3$ transition. Table II summarizes their directional tendencies, latency characteristics and primary defensive countermeasures.

TABLE II
PROPAGATION MECHANISM PROPERTIES

Mech.	Direction	Latency	Prev.	Primary Defense
ϕ_{PC}	Lateral / Down	Hours–days	4/6	Segmentation; physics det.
ϕ_{IP}	Upward / Lat.	Days–months	6/6	Info compartment.; zero trust
ϕ_{TE}	Upward / Lat.	Weeks–months	3/6	Supply-chain verification
ϕ_{SI}	Upward	Months–years	6/6	Strategic intelligence

Controllability Metric We define controllability as the degree to which observed cumulative effects align with adversarial intent $C = 1 - \frac{|E_{obs} - E_{int}|}{E_{obs}}$, where E_{obs} denotes the aggregated observed severity across all orders and E_{int} denotes the intended effect magnitude. Values $C \approx 1$ indicate high precision and bounded propagation (e.g., tightly scoped sabotage), whereas $C \ll 1$ indicates uncontrolled cascading or unintended amplification (e.g., systemic spillover). This metric enables comparative classification of operations along a controllability spectrum.

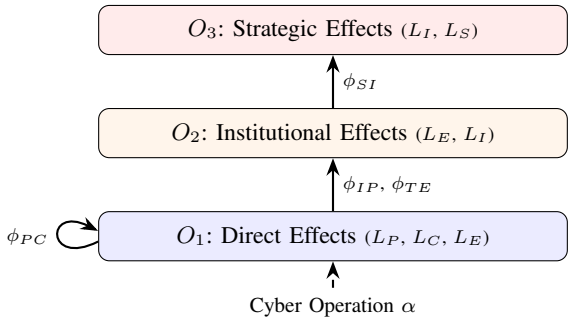


Fig. 1. Multi-Order Effect propagation model.

Formal Representation The MOrE framework forms a DAG: $\mathcal{M} = (\mathcal{O}, \Pi, \mathcal{I})$ where $\mathcal{O} = \{O_1, O_2, O_3\}$, Π is the set of propagation pathways and $\mathcal{I}$ is the set of observable indicators. The general effect structure for operation α is a subgraph $E(\alpha) \subseteq \mathcal{M}$, $\alpha \xrightarrow{\phi_{PC}} O_1(\alpha) \xrightarrow{\phi_{IP},\phi_{TE}} O_2(\alpha) \xrightarrow{\phi_{SI}} O_3(\alpha)$. The framework admits non-linear propagation: reverse paths ($O_2 \to O_1$ via ϕ_{PC}, as in cyber-enabled kinetic targeting), lateral propagation across organizational boundaries, or termination at any order. Fig. 1 illustrates the structure.

For Personal Use Only

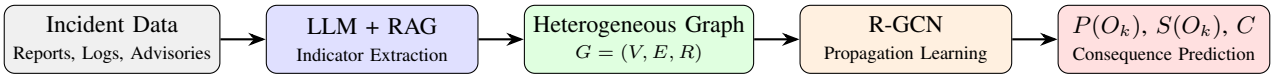


Fig. 2. MOrE computational pipeline incident data feeds LLM-augmented extraction of institutional/strategic indicators.

IV. Computational Architecture

Heterogeneous Graph Representation A CPS environment is encoded as a heterogeneous graph $G = (V, E, R)$. Nodes are partitioned by system layer: $V = V_P \cup V_C \cup V_E \cup V_I \cup V_S$, where each subset corresponds to assets, processes or functions at the respective layer. Each node v_i carries a feature vector $x_i \in \mathbb{R}^d$ encoding vulnerability exposure, dependency centrality, economic value and intelligence sensitivity. Edges are typed by relation: $R = \{r_{phys}, r_{info}, r_{econ}, r_{reg}, r_{geo}\}$, representing physical coupling, information flow, economic dependency, regulatory authority and geographic co-location respectively. The four propagation mechanisms map to edge subsets: ϕ_{PC} operates over r_{phys} edges; ϕ_{IP} over r_{info}; ϕ_{TE} over r_{econ}; ϕ_{SI} over r_{reg} and r_{geo}. Each organization constructs this graph by mapping data assets, network access points and third-party interdependencies across all five layers. Third-party mapping is essential: NotPetya and SolarWinds demonstrate that supply-chain interdependencies create ϕ_{TE} pathways invisible to single-organization assessment.

Relational Graph Neural Network To learn cross-layer propagation dynamics, we adopt a Relational Graph Convolutional Network (R-GCN) [23] architecture. The layer update rule is $h_i^{(l+1)} = \sigma\left(\sum_{r\in R}\sum_{j\in\mathcal{N}_i^r}\frac{1}{c_{i,r}}W_r^{(l)}h_j^{(l)} + W_0^{(l)}h_i^{(l)}\right)$ where $W_r^{(l)}$ is a relation-specific transformation matrix, $\mathcal{N}_i^r$ denotes neighbors of node i under relation r, $c_{i,r}$ is a normalization constant and σ is a nonlinear activation. This architecture preserves relation-type semantics during message passing, enabling the model to learn distinct propagation dynamics for each mechanism. The final layer produces cross-layer consequence predictions $P(O_k|v_i, G) = \text{softmax}(W_r h_i^{(L)})$, estimating the probability that compromise at node v_i produces effects at order O_k. Temporal dynamics are incorporated via exponential smoothing: $h_i^{t+1} = \gamma h_i^t + (1-\gamma) f_{\text{RGCN}}(h_i^t)$.

Spectral Amplification Condition Let $A_{cross} = \sum_{r\in R_{cross}} A_r$ denote the aggregate cross-layer adjacency matrix, where R_{cross} includes inter-layer relation types. Under linearized propagation, signal evolution follows $x^{t+1} = A_{cross}x^t$, yielding $x^t = A_{cross}^t x^0$. If the spectral radius $\rho(A_{cross}) > 1$, then $\|x^t\| \to \infty$: cross-layer signal amplification is unbounded, corresponding to uncontrolled propagation. If $\rho(A_{cross}) \leq 1$, propagation is bounded and controllability C remains above a positive minimum. It provides a computable criterion to identify supercritical dependency configurations in organizational graphs.

LLM-Augmented Indicator Extraction and Architecture Institutional (L_I) and strategic (L_S) indicators are embedded in unstructured documents, incident reports, policy advisories, regulatory filings and geopolitical assessments. Node features at these layers cannot be derived from network telemetry alone. RAG pipeline is (1) embed a corpus of incident-related documents; (2) retrieve the top-k passages relevant to each institutional or strategic node; (3) apply a structured prompt to classify extracted indicators into effect orders and assign severity component scores (D_{phys}, L_{econ}, P_{policy}). Extracted indicators populate institutional and strategic node features in the heterogeneous graph. Inter-annotator validation with $\kappa > 0.80$ ensures extraction reliability. This hybrid structured-semantic approach enables computational modeling of consequences that extend beyond the technical domain, addressing the fundamental challenge that L_I and L_S effects are not directly observable in network telemetry. Fig. 2 illustrates the end-to-end computational pipeline.

V. Case Study Validation

The MOrE framework is applied to six operations spanning 2010–2025. Each case is analyzed by mapping observed consequences to effect orders and identifying propagation mechanisms. Table III summarizes the mapping.

Stuxnet (2010) manipulated Siemens S7-315/S7-417 PLCs at Natanz to destroy ∼1,000 centrifuges while reporting nominal telemetry [7], [24]. O_1: centrifuge destruction via over-speed cycling ($L_C \to L_P$). O_2: 1–2 year program delay; operator trust collapse; doctrinal shock revealing a new class of offensive CPS capability. O_3: modification of nuclear negotiation dynamics; demonstration that cyber operations could replace kinetic action against hardened targets; doctrine proliferation. Propagation: $\phi_{PC} \to \phi_{IP} \to \phi_{SI}$. $C \approx 0.92$.

Ukraine Power Grid (2015) BlackEnergy 3 enabled pivot from enterprise networks to SCADA at three Ukrainian distribution companies; attackers opened breakers at 30 substations, causing outages to 225,000 customers [25]. O_1: power outage ($L_E \to L_C \to L_P$). O_2: months of manual grid operations; international CPS security cooperation. O_3: first confirmed cyber-caused power outage; coercive template below armed conflict threshold; NATO cyber domain recognition. Propagation: $\phi_{IP} \to \phi_{PC} \to \phi_{SI}$. $C \approx 0.88$.

NotPetya (2017) Destructive malware distributed via compromised MeDoc update, combining EternalBlue with Mimikatz [26]. O_1: global IT destruction; Maersk (76 port facilities) and Merck production halted via IT/OT dependency ($L_E \to L_C$). O_2: \$10B+ damages; Mondelez \$100M claim denial under war exclusion [27] reshaped cyber insurance. O_3: Five Eyes coordinated attribution precedent; demonstrated uncontrolled cascading through commercial interconnection. Propagation: $\phi_{TE} \to \phi_{PC} \to \phi_{SI}$. $C \approx 0.41$; effects exceeded intent, including self-inflicted Rosneft damage.

SolarWinds (2020) SUNBURST backdoor in Orion updates distributed to ∼18,000 organizations including U.S. federal agencies and critical infrastructure operators [8], [28]. O_1: supply-chain compromise; persistent network access (L_E). O_2: systemic trust erosion in signed software distribution; CISA ED 21-01; intelligence yield on policy deliberations [9]. O_3: *working hypothesis*: intelligence plausibly informed Russian

For Personal Use Only

TABLE III
MULTI-ORDER EFFECT ANALYSIS OF SIX CYBER OPERATIONS

Ops	**Stuxnet**	**Ukraine Grid**	**NotPetya**	**SolarWinds**	**Colonial Pipeline**	**UAC/Spiderweb**
O_1	Centrifuge destruction via PLC manipulation	Substation disconnection and outage	Global IT destruction via compromised update	Supply-chain backdoor; persistent enterprise access	IT ransomware; voluntary OT shutdown	Enterprise data exfiltration campaign
O_2	Nuclear program delay; doctrinal shock	Manual grid recovery; international cooperation	$10B+ global damage; insurance disruption	Trust erosion; intelligence advantage	Fuel shortage; mandatory federal regulation	Fleet intelligence exposure; precision targeting
O_3	Diplomatic shift; doctrine proliferation	NATO cyber domain recognition; coercive precedent	Attribution precedent; control debate	Strategic confidence shaping (hyp.)	Policy red lines; mandatory governance shift	Nuclear triad degradation; $7B impact
ϕ **chain**	$\phi_{PC}\rightarrow\phi_{IP}\rightarrow\phi_{SI}$	$\phi_{IP}\rightarrow\phi_{PC}\rightarrow\phi_{SI}$	$\phi_{TE}\rightarrow\phi_{PC}\rightarrow\phi_{SI}$	$\phi_{TE}\rightarrow\phi_{IP}\rightarrow\phi_{SI}$	$\phi_{IP}\rightarrow\phi_{TE}\rightarrow\phi_{SI}$	$\phi_{IP}\rightarrow\phi_{SI}\rightarrow\phi_{PC}$
C	0.92	0.88	0.41	0.79	0.36	0.94

assessment of Western response parameters prior to the February 2022 invasion. Propagation: $\phi_{TE}\rightarrow\phi_{IP}\rightarrow\phi_{SI}$. $C \approx 0.79$. Fig. 3 illustrates the multi-order propagation graph.

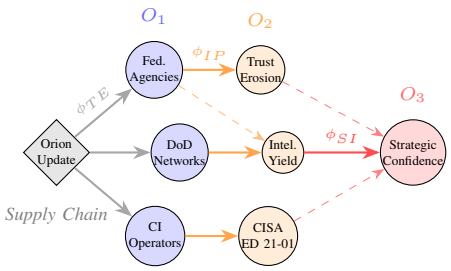


Fig. 3. SolarWinds multi-order propagation graph.

Colonial Pipeline (2021) DarkSide ransomware encrypted enterprise IT of the largest U.S. fuel pipeline (45% of East Coast supply). OT was *not* compromised; the company voluntarily shut down due to monitoring and billing dependency [29], [30]. O_1: IT encryption; voluntary OT shutdown (L_E, decision-mediated to L_C/L_P). O_2: regional fuel shortages; EO 14028; mandatory pipeline cybersecurity regulations. O_3: voluntary-to-mandatory CI governance shift; Biden-Putin Geneva Summit cyber red-line declaration [31]. Propagation: $\phi_{IP}\rightarrow\phi_{TE}\rightarrow\phi_{SI}$. $C \approx 0.36$.

UAC/Operation Spiderweb (2024–25) Russia's United Aircraft Corporation (UAC), consolidating all major military aircraft manufacturers under a single digital infrastructure, was subject to a reported cyber intrusion in 2024 [32]. On 1 June 2025, Ukraine's SBU executed Operation Spiderweb: 117 FPV drones struck five air bases across five time zones, destroying an estimated 12–13 strategic bombers (Tu-95MS, Tu-22M3) [33], [34]. O_1: enterprise data exfiltration (L_E). O_2: *working hypothesis*: UAC intelligence enabled precision targeting of irreplaceable Soviet-era assets; the 18-month planning [33] is temporally consistent intelligence yield. O_3: ∼34% strategic bomber fleet destroyed ($7B estimated) [35], [36]. Propagation is $\phi_{IP}\rightarrow\phi_{SI}\rightarrow\phi_{PC}$. $C \approx 0.94$.

VI. CROSS-CASE ANALYSIS

Observation 1: Universal strategic propagation. All six ops produced O_3 effects regardless of entry layer (L_C or L_E), actor type, or intent. This convergence is partially conditioned by case selection but suggests an inherent tendency toward strategic-layer propagation when CI is involved.

Observation 2: Multi-directional propagation. Stuxnet propagated downward ($L_C\rightarrow L_P$) then upward to L_S. UAC/Spiderweb propagated upward ($L_E\rightarrow L_I$) then back downward via kinetic targeting. Colonial Pipeline propagated laterally without downward cyber intrusion. This invalidates linear kill-chain models as consequence frameworks.

Observation 3: ϕ_{IP} as universal mechanism. Info propagation appears in all six cases, confirming ϕ_{IP} as the most general mechanism and the highest-priority defensive target.

Observation 4: Controllability spectrum. The controllability metric C quantifies divergence between intended and observed effect boundaries. Precise operations ($C > 0.85$: Stuxnet, Ukraine Grid, UAC/Spiderweb) exhibit bounded propagation. Uncontrolled operations ($C < 0.45$: NotPetya, Colonial Pipeline) exhibit effects exceeding adversary intent. The spectral amplification condition ($\rho(A_{cross}) > 1$) provides a structural explanation: supercritical cross-layer connectivity enables unbounded signal amplification.

Observation 5: CPS effects without CPS compromise. Colonial Pipeline demonstrates that physical op can cease without OT/SCADA compromise through IT/OT op dependency, extending the threat model to dependency-mediated effects.

Observation 6: Temporal-irreversibility gradient. O_1 effects may be recoverable within days; O_3 effects are structurally irreversible within any operationally relevant timeframe. System dependability under adversarial conditions therefore satisfies $D_{system} = D_{CPS}\cdot(1-P(O_3))$, where D_{CPS} is infrastructure-layer dependability. Even if D_{CPS} is fully restored post-incident, $D_{system} < 1$ whenever $P(O_3) > 0$. This formalizes the observation that strategic-layer degradation persists independently of infrastructure recovery as shown in Table IV.

TABLE IV
CONTROLLABILITY SPECTRUM CLASSIFICATION

Category	C **Range**	$\rho(A_{cross})$	**Cases**
Precise	> 0.85	≤ 1	Stuxnet, Ukr. Grid, UAC
Selective	0.70–0.85	≤ 1	SolarWinds
Uncontrolled	0.35–0.50	> 1	NotPetya
Incidental	< 0.40	> 1	Colonial Pipeline

Limitations: The UAC-to-Spiderweb linkage is a working hypothesis and alternative causal pathways cannot be ex-

For Personal Use Only

cluded. Controllability scores C are derived from publicly available information and involve analytical estimation. The proposed HGNN+LLM architecture has not yet been trained on a structured multi-order dataset, as no such corpus currently exists. The spectral amplification condition assumes linearized propagation, whereas real-world dynamics may exhibit nonlinear feedback. LLM-based indicator extraction is subject to reporting bias and hallucination risk, partially mitigated through retrieval augmentation and validation.

VII. Conclusion

This paper presented the MOrE framework formalizing three effect orders, four propagation mechanisms, quantitative severity and controllability metrics and spectral amplification conditions within a five-layer CPS model. A heterogeneous graph neural network with LLM-augmented indicator extraction was proposed as a computational architecture for cross-layer consequence prediction. Analysis of six operations demonstrates multi-directional propagation, a measurable controllability spectrum and strategic-layer effects persisting beyond infrastructure recovery. The results indicate that restoring physical infrastructure does not necessarily restore system-level dependability when higher-order effects remain active. Future work includes development of labeled multi-order datasets and empirical validation of the proposed HGNN architecture for predictive cross-layer threat modeling.

0pt plus 0.5ex

References

[1] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Design Automation Conference*. ACM/IEEE, 2010, pp. 731–736.

[2] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[3] A. A. Cárdenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Research challenges for the security of control systems," in *Proceedings of the 3rd USENIX Workshop on Hot Topics in Security, Article 6*, San Jose, CA, USA, 2008.

[4] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "A survey of physics-based attack detection in cyber-physical systems," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1–36, 2018.

[5] V. R. Palleti, S. Adepu, V. K. Mishra, and A. Mathur, "Cascading effects of cyber-attacks on interconnected critical infrastructure," *Cybersecurity*, vol. 4, no. 1, pp. 1–18, 2021.

[6] S. Chockalingam and C. Maathuis, "Assessing cascading effects of cyber-attacks in interconnected critical infrastructures," in *Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)*. Research Publishing, 2022, pp. 2852–2859.

[7] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[8] Mandiant, "Highly evasive attacker leverages SolarWinds supply chain to compromise multiple global victims via SUNBURST backdoor," *FireEye Threat Intelligence*, 2020.

[9] D. Broeders and C. Kavanagh, *Shades of Grey: Cyber Intelligence and (Inter)national Security*. Oxford University Press, 2023.

[10] E. Orye and O. M. Maennel, "Recommendations for enhancing the results of cyber effects," in *11th International Conference on Cyber Conflict (CyCon)*. Tallinn: NATO CCD COE Publications, 2019.

[11] O. A. Adekoya, H. F. Atlam, and H. S. Lallie, "Quantifying the multidimensional impact of cyber attacks in digital financial services: A systematic literature review," *Sensors*, vol. 25, no. 14, p. 4345, 2025.

[12] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," in *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, 2011, pp. 80–106.

[13] M. Schulze and M. Kerttunen, "Cyber operations in Russia's war against Ukraine: Uses, limitations, and lessons learned so far," *SWP Comment*, no. 23, 2023.

[14] T. Rid, *Cyber War Will Not Take Place*. Oxford University Press, 2013.

[15] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity*, vol. 4, no. 1, p. tyy006, 2018.

[16] S. K. Choudhary, N. Singh, N. Singh, and K. Berwal, "Dynamic automated red team tool (DARTT): A comprehensive framework for system, network and data security auditing," in *2025 IEEE International Conference on Computer, Electronics, Electrical Engineering and their Applications (IC2E3)*. IEEE, 2025.

[17] A. Prabagaran, S. Kalavathi, N. M. Balamurugan, J. Angelin Blessy, K. Berwal, and J. Ayeelyan, "Secured heterogeneous data fusion using adversarial autoencoders in Internet of Military Things," in *2025 International Conference on Data Science and Applications (ICDSA)*. IEEE, 2025.

[18] H. Singh, M. Deshmukh, L. K. Awasthi, and K. Berwal, "A robust watermarking approach for securing copyright in watershed images," in *Proceedings of the 6th International Conference on Deep Learning, Artificial Intelligence and Robotics (ICDLAIR 2024)*. Atlantis Press, 2025, pp. 291–302.

[19] P. Prakash, P. Rathee, L. K. Awasthi, and K. Kumar, "A review on security challenges: Cryptography and blockchain for Internet of Things," in *The Future of Artificial Intelligence and Robotics*. Springer, 2024, pp. 779–792.

[20] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity, version 1.1," NIST, 2018.

[21] International Electrotechnical Commission, "IEC 62443: Industrial communication networks – network and system security," IEC, 2018.

[22] Y. Zhu, Y. Zhou, W. Wei, and N. Wang, "Cascading failure analysis based on a physics-informed graph neural network," *IEEE Transactions on Power Systems*, vol. 38, no. 4, pp. 3632–3641, 2023.

[23] M. Schlichtkrull, T. N. Kipf, P. Bloem, R. van den Berg, I. Titov, and M. Welling, "Modeling relational data with graph convolutional networks," in *European Semantic Web Conference (ESWC)*. Hersonissos, Crete, Greece: Springer, 2018, pp. 593–607.

[24] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet dossier," *Symantec Security Response*, vol. 5, no. 6, p. 29, 2011.

[25] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," *SANS ICS*, 2016.

[26] A. Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday, 2019.

[27] J. Wolff, "Mondelez v. Zurich: Cyber insurance and the boundaries of the war exclusion," Lawfare, 2 November 2022, 2022.

[28] CISA, "Alert (AA21-008A): Detecting post-compromise threat activity in Microsoft cloud environments," https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-008a, 2021.

[29] Cybersecurity and Infrastructure Security Agency, "Alert (AA21-131A): DarkSide ransomware: Best practices for preventing business disruption from ransomware attacks," https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a, 2021.

[30] D. E. Sanger and N. Perlroth, "Cyberattack forces a shutdown of a top U.S. pipeline," *The New York Times*, 2021, 7 May 2021.

[31] The White House, "Remarks by President Biden in press conference," White House Briefing Room, 16 June 2021, 2021.

[32] D. Croft, "'Nothing secret left': Ukraine claims cyber attack on Russian warplane builder Tupolev," Cyber Daily, 5 June 2025, 2025.

[33] J. Marson, J. Lytvynenko, B. T. Smith, and S. Bosak, "Inside the Ukrainian drone operation that devastated Russia's bomber fleet," Wall Street Journal, 3 June 2025, 2025.

[34] S. Brown, "Ukraine trained AI for its 'Spiderweb' airfield drone attacks at aviation museum," Kyiv Post, 2 June 2025, 2025.

[35] O. Gibson, A. Harvey, D. Novikov, C. Harward, and K. Stepanenko, "Russian offensive campaign assessment, june 1, 2025," Institute for the Study of War, 2025.

[36] A. Stognei, F. Deprez, and C. Miller, "'An epic failure': Russia reels from surprise Ukrainian attack on bomber fleet," Financial Times, 3 June 2025, 2025.

For Personal Use Only