

A multilevel attributed cyberspace model for cyber threat intelligence in ICT systems

Alla Pinchuk^{1,†}, Roman Odarchenko^{1,*,†}, Oleh Polihenko^{1,†}, Azamat Imanbayev^{2,†} and Rat Berdibayev^{3,†}

¹National University "Kyiv Aviation Institute", Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine

²Kazakh-British Technical University, Tole bi Str., 59, Almaty, 050000, Kazakhstan

³Almaty University of Power Engineering and Telecommunications, Baitursynuly Str., 126/1, Almaty, 050013, Kazakhstan

Abstract

The rapid expansion of 5G, cloud-native, and software-defined networking technologies has rendered information and telecommunications (ICT) systems increasingly complex socio-technical environments whose security analysis requires a formal, multidimensional representation of cyberspace. Existing modelling approaches – multilayer, network-of-networks (NoN), topographic, and ontological – each address specific aspects of this representation, yet do not simultaneously provide multilevel coverage, formal computability, dynamic state modelling, and explicit integration points for cyber threat intelligence (CTI) data. This paper proposes a Multilevel Attributed Cyberspace Model for ICT systems, formalized as the tuple $M_{cs} = (L, V, E^{intra}, E^{inter}, A, \lambda, \tau, \alpha, \Sigma, \sigma, T)$, comprising six levels: geospatial, physical, logical-network, service-functional, information-data, and organizational-personnel. The model represents intra-level and inter-level dependencies through directed attributed edges classified by topology and functional semantics, and supports temporal state tracking and CTI-oriented attribute binding. A criterion-based design assessment against seven requirements (R1–R7) and six evaluation criteria (C1–C6) shows how the proposed model addresses the identified gaps by construction. An illustrative synthetic case study based on a 5G infrastructure attack scenario shows by example how the model can support multilevel threat-propagation analysis, CTI enrichment, state-change auditing, and SOC/NOC incident-response workflows.

Keywords

cyberspace model, cyber threat intelligence, multilevel attributed graph, ICT security, security operations centre, network-of-networks, 5G network security, attack graph

1. Introduction

Contemporary information and telecommunications (ICT) systems have evolved into large-scale socio-technical environments in which physical infrastructure, logical networks, software services, data assets, and the organizations and personnel that operate them are tightly coupled. The accelerated deployment of cloud-native architectures, software-defined networking (SDN), the Internet of Things (IoT), and fifth-generation (5G) and beyond-5G mobile networks has dramatically expanded the attack surface and the interdependence between previously separable domains [1, 2]. Consequently, security operations centres (SOCs) and cyber threat intelligence (CTI) teams must reason not about isolated assets, but about a heterogeneous, continuously evolving environment in which a single adversarial action may propagate across several technological and organizational layers.

CTI has become a central pillar of modern defence, providing structured knowledge about indicators of compromise (IoC), adversary tactics, techniques, and procedures (TTPs), vulnerabilities, and observed campaigns through standardized representations such as STIX 2.1, TAXII, and the MITRE ATT&CK knowledge base [3, 4, 5]. However, the operational value of CTI depends not only on the quality of the intelligence itself, but on a coherent formal model of the environment to which it is applied. Without an

WCH'26: Fifth International Workshop on Cyber Hygiene, June 25–26, 2026, Krakow, Poland

*Corresponding author.

†These authors contributed equally.

✉ alla.pinchuk@npp.kai.edu.ua (A. Pinchuk); roman.odarchenko@npp.kai.edu.ua (R. Odarchenko); o.poligenko@ukr.net (O. Polihenko); imanbaevazamat@gmail.com (A. Imanbayev); r.berdybaev@aes.kz (R. Berdibayev)

0000-0003-3567-0445 (A. Pinchuk); 0000-0002-7130-1375 (R. Odarchenko); 0000-0002-2427-4976 (O. Polihenko); 0000-0003-3719-4091 (A. Imanbayev); 0000-0002-8341-9645 (R. Berdibayev)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

explicit, machine-interpretable representation of cyberspace, analysts must mentally reconstruct how a given indicator or technique relates to the underlying infrastructure, services, data, and personnel—an approach that does not scale to large, distributed ICT systems.

Existing formal cyberspace models each optimize for a single dimension: multilayer models offer intuitive stratification without formalization or CTI integration; graph-based and NoN models provide tractability but underrepresent event semantics and dynamics; topographic models support situational awareness but are not machine-oriented; and ontological models deliver formal expressiveness yet remain fragmented and hard to operationalize [6, 7, 8, 9]. No single computable model simultaneously captures the multidimensional structure of an ICT system, the dependencies linking its levels, the temporal evolution of its state, and the integration points required for CTI.

To address this gap, we propose the Multilevel Attributed Cyberspace Model $M_{cs} = (L, V, E^{\text{intra}}, E^{\text{inter}}, A, \lambda, \tau, \alpha, \Sigma, \sigma, T)$: a multilevel, attribute-oriented directed graph over six levels (geospatial, physical, logical-network, service-functional, information-data, and organizational-personnel) with explicitly typed intra- and inter-level edges. The contributions are threefold: (i) a set of requirements (R1–R7) and a criterion-based assessment (C1–C6) of existing modelling families extended to include M_{cs} ; (ii) a unified formalization combining the six-level decomposition, typed inter-level dependencies, CTI-oriented attribute binding, and temporal state tracking; and (iii) a synthetic 5G case study illustrating multilevel threat-propagation analysis for SOC/CTI environments. The remainder of the paper covers related work (Section 2), the proposed model (Section 3), discussion (Section 4), and conclusions (Section 5).

2. Related work

Research relevant to this work spans five largely independent communities: CTI operationalization, attack modelling and propagation, semantic technologies, infrastructure interdependency representation, and digital-twin-based security modelling.

CTI operationalization. Standardized representations (STIX 2.1), transport mechanisms (TAXII), the MITRE ATT&CK taxonomy, and intrusion-analysis frameworks such as the Cyber Kill Chain and the Diamond Model have established a common vocabulary for indicators, techniques, and campaigns [3, 4, 10]. Their focus, however, is adversarial activity rather than the structure of the defended environment. Cybersecurity knowledge graphs integrate heterogeneous CTI artefacts [11], yet the underlying environment model remains implicit.

Attack modelling and propagation. Attack graphs, attack trees, and Bayesian extensions enable systematic reasoning about how an adversary chains vulnerabilities and privileges to reach a target [6, 7, 8]. Their expressiveness is typically confined to technical and logical layers: geospatial, service-functional, and organizational dimensions are rarely represented, non-attack telemetry is absent, and state-space explosion limits scalability [6].

Security ontologies and knowledge graphs. Ontological approaches—e.g. the Unified Cyber Ontology, the Common Core Cyber Ontology, and domain-specific event ontologies—offer formal rigour and support for data fusion and reasoning [9, 12, 13]. In practice, adoption in SOC/CTI environments is hindered by ontology fragmentation, population/maintenance effort, and the absence of a single ontology jointly covering technical, organizational, geographical, and legal dimensions.

Infrastructure interdependency. Network and NoN formulations describe cyberspace as graphs of infrastructure elements, services, or users, with edges encoding physical, logical, or functional connections [14, 15]; interdependency models capture cross-domain coupling between communication, energy, control, and organizational subsystems [16]. These privilege topology over semantics: CTI context, semantic typing, and dynamic updating are underdeveloped, and the explicit ICT level structure is often absent [17]. Topographic and cartographic models treat cyberspace by analogy with geographic space for visualization and situational awareness [17, 18, 19]; they are intuitive but oriented toward representation rather than machine-oriented formal description and are weakly coupled to CTI data structures.

Table 1

Criterion-Based Comparison of Cyberspace-Modelling Families (1 = low, 5 = high)

Model	C1	C2	C3	C4	C5	C6
Multilayered models	4	2	2	1	3	5
Network and NoN models	3	4	3	3	3	3
Topographic/cartographic models	3	2	2	2	3	5
Ontological/semantic models	4	5	4	3	2	3
Proposed model M_{cs} (this work)	5	5	5	5	4	4

Digital twins. Security-oriented digital twins offer a dynamic, attribute-rich environment model for what-if assessment, intrusion detection, and slice management [20, 2], sharing our emphasis on dynamic state. However, they provide neither a unified multilevel formalization, nor explicit inter-level dependency typing, nor native integration with standardized CTI data. The scores assigned to M_{cs} reflect requirements coverage by design rather than experimentally measured performance.

Taken together, each direction supports only a subset of the properties required for CTI-oriented cyberspace modelling: CTI standards describe adversarial behaviour but not the defended environment; attack graphs capture technical propagation but lack geospatial, service-functional, and organizational coverage; ontological models offer expressiveness but are hard to operationalize; NoN models support structural analysis but are weak on CTI semantics and dynamics; and digital twins provide dynamic state without a general multilevel dependency formalism. The next section operationalizes these gaps as requirements and design criteria and introduces M_{cs} to address them by construction.

3. Proposed model

3.1. Comparative analysis of existing cyberspace models

The four families reviewed in Section 2—multilayered models [21, 22], network and “network-of-networks” models [15, 16], topographic/cartographic models [17, 18, 19], and ontological/semantic models [12, 13]—each cover only a subset of the dimensions (technical, organizational, geospatial, legal) and properties required for CTI-oriented modelling. To compare them systematically, six criteria are used: C1—coverage of cyberspace dimensions; C2—formal rigour and computability; C3—suitability for integration with ICT and CTI data; C4—support for dynamism; C5—scalability and practical feasibility; C6—interpretability for analysts and decision support. Each is scored on a five-point scale (Table 1).

Scores for existing families derive from the works cited in Section 2 (1 – absent; 2 – marginal; 3 – partial; 4 – substantial with limitations; 5 – explicit and formally defined); scores for M_{cs} are design-target assessments, not empirical measurements, with validation left to future work (Section 4.3). The comparison confirms that existing families suffer from incomplete dimensional coverage, weak formalization of cross-level dependencies, limited dynamic updating, and poor CTI integration—motivating a model that combines multilevel representation, graph formalization, dynamic updating, and CTI-oriented attribute binding.

3.2. Requirements for an improved model

Table 2 states the seven requirements (R1–R7) the improved model must satisfy. Legal and regulatory attributes (compliance frameworks, jurisdictional constraints, authorization policies) are embedded within L_o through α rather than as a separate level, avoiding over-segmentation while preserving governance coverage.

Table 2

Requirements for the Improved Cyberspace Model

ID	Requirement	Description
R1	Multilevel structure	Reflects the geospatial, physical, logical-network, service-functional, information-data, and organizational-personnel components of the ICT system.
R2	Formal determinacy	A formal mathematical framework suitable for algorithmic analysis and automated reasoning.
R3	Dependency mapping	Describes intra-level and inter-level connections, classified by topology (adjacent, cross-level) and functional nature.
R4	Dynamism	Supports changes in states, attributes, relations, and elements over time via temporal state functions and, where necessary, time-dependent attribute mappings.
R5	CTI integration	Accommodates IoC, TTPs, CVE identifiers, CVSS scores, ATTACK mappings, event logs, and telemetry as typed attributes attached to vertices and edges.
R6	Scalability	Applicable to individual ICT segments and large-scale distributed infrastructures, with graph-theoretic representation supporting efficient querying.
R7	Interpretability	Results understandable to SOC/CTI analysts and suitable for decision support, via named levels, typed links, and human-readable state labels.

3.3. Multilevel structure

Cyberspace is a multidimensional socio-technical environment in which infrastructural, logical, informational, and socio-organizational components interact simultaneously. We therefore propose the six-level structure of Fig. 1: the geospatial (L_g), physical-infrastructure (L_p), logical-network (L_n), service-functional (L_s), information-data (L_d), and organizational-personnel (L_o) levels. This extends classical physical/logical/information/human decompositions by elevating the geospatial and service-functional levels as first-class concerns: L_g represents jurisdiction, location-based access constraints, and geographic threat attribution, while L_s models the microservices, APIs, and orchestration layers characteristic of 5G core and cloud-native architectures. Legal and regulatory attributes are embedded in L_o via α rather than forming a separate level. The levels interact through adjacent and cross-level connections—classified formally in Section 3.4—and dynamic processes (events, state changes, configuration updates, telemetry) overlay all levels as a temporal characteristic.

3.4. Formal representation

The proposed model is a multilevel, attribute-oriented directed graph whose vertices correspond to entities at different cyberspace levels and whose edges represent directed operational, dependency, access, or propagation relations between them. Formally,

$$M_{cs} = (L, V, E^{\text{intra}}, E^{\text{inter}}, A, \lambda, \tau, \alpha, \Sigma, \sigma, T), \quad (1)$$

where L is the set of cyberspace levels, V the set of vertices, E^{intra} the intra-level edges, E^{inter} the inter-level edges, A the attribute domain, λ the vertex-level membership function, τ the inter-level edge typification function, α the attribute-mapping function, Σ the state domain, σ the state function, and T the set of observation time points or intervals.

The set of levels is

$$L = \{L_g, L_p, L_n, L_s, L_d, L_o\}, \quad (2)$$

where L_g is the geospatial level, L_p the physical-infrastructure level, L_n the logical-network level, L_s the service-functional level, L_d the information-data level, and L_o the organizational-personnel level.

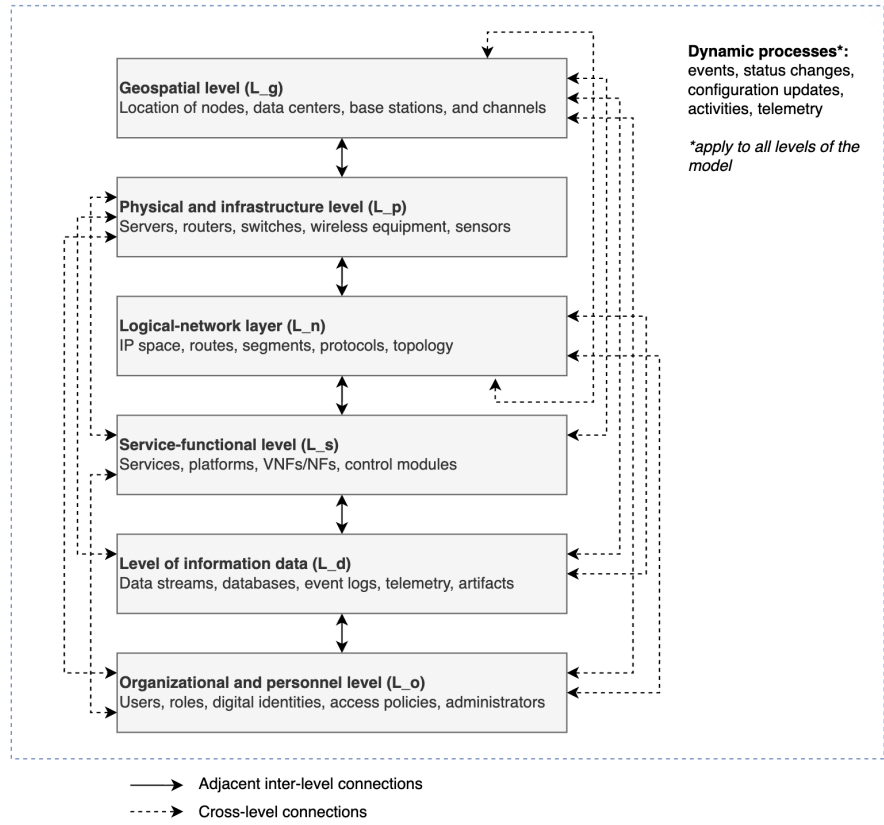


Figure 1: Six-level cyberspace model for ICT systems. Solid arrows denote adjacent inter-level dependencies; dashed arrows denote cross-level dependencies. Dynamic processes and telemetry may affect all levels.

To describe adjacency, an order function is introduced:

$$\text{ord} : L \rightarrow \{1, 2, 3, 4, 5, 6\}, \quad (3)$$

with $\text{ord}(L_g) = 1$, $\text{ord}(L_p) = 2$, $\text{ord}(L_n) = 3$, $\text{ord}(L_s) = 4$, $\text{ord}(L_d) = 5$, and $\text{ord}(L_o) = 6$. Two levels L_i and L_j are *adjacent* if $|\text{ord}(L_i) - \text{ord}(L_j)| = 1$, and *non-adjacent* if $|\text{ord}(L_i) - \text{ord}(L_j)| > 1$.

The vertex set is the disjoint union of level-specific vertex sets:

$$V = V_g \cup V_p \cup V_n \cup V_s \cup V_d \cup V_o, \quad V_i \cap V_j = \emptyset \text{ for } i \neq j, \quad (4)$$

so that each vertex belongs to exactly one base level. The level membership function is

$$\lambda : V \rightarrow L, \quad \lambda(v) = L_i \Leftrightarrow v \in V_i. \quad (5)$$

Intra-level edges connect vertices belonging to the same level:

$$E^{\text{intra}} = \bigcup_{L_i \in L} E_i, \quad E_i \subseteq \{(u, v) \in V_i \times V_i \mid u \neq v\}. \quad (6)$$

Self-loops are thus excluded from the base model; if required by a specific implementation they may be added as an extension, but they are not part of the default formalism. The interpretation of intra-level edges is level-dependent: at L_g they represent territorial adjacency or spatial inclusion; at L_p physical connections between hardware components; at L_n routing paths, logical segmentation, or protocol-level channels; at L_s service-to-service dependencies, API calls, or orchestration links; at L_d relationships between data flows, storage artefacts, processing pipelines, and log streams; and at L_o role-based, hierarchical, or policy-oriented dependencies.

Table 3Formal Symbols and Semantics of Inter-Level Link Functional Types (τ_{fun})

Symbol	Type	Semantics
<i>loc</i>	Localization	Geospatial containment, physical positioning, or jurisdictional localization of an ICT entity.
<i>inf</i>	Infrastructure-implementation	Physical hosting, power, hardware, or deployment dependency between an entity and the infrastructure that realizes it.
<i>net</i>	Network-functional	Logical, protocol, signalling, or interface dependency between a logical-network entity and a service-functional entity.
<i>data</i>	Information-process	Data flow, read/write access, storage, query, logging, or processing dependency between a service and a data asset.
<i>org</i>	Organizational-management	Role-based authority, ownership, policy, compliance, escalation, or governance dependency involving organizational entities.

Inter-level edges connect vertices belonging to different levels:

$$E^{\text{inter}} = \bigcup_{L_i \neq L_j} E_{ij}, \quad E_{ij} \subseteq V_i \times V_j. \quad (7)$$

The direction of an edge $e = (u, v)$ follows the analytical propagation direction used by the model: from the source or enabling element u to the dependent, accessed, affected, or operationally influenced element v . This convention lets the same graph support dependency analysis, attack-path traversal, impact propagation, and SOC workflow reconstruction. A bidirectional real-world relation is represented by two directed edges with potentially different attributes. Inter-level edges are partitioned by topology into adjacent and cross-level edges:

$$E_{\text{adj}} = \{(u, v) \in E^{\text{inter}} \mid |\text{ord}(\lambda(u)) - \text{ord}(\lambda(v))| = 1\}, \quad (8)$$

$$E_{\text{cross}} = \{(u, v) \in E^{\text{inter}} \mid |\text{ord}(\lambda(u)) - \text{ord}(\lambda(v))| > 1\}, \quad (9)$$

$$E^{\text{inter}} = E_{\text{adj}} \cup E_{\text{cross}}, \quad E_{\text{adj}} \cap E_{\text{cross}} = \emptyset. \quad (10)$$

The typification function classifies inter-level edges:

$$\tau : E^{\text{inter}} \rightarrow T_\tau, \quad T_\tau = T_{\text{top}} \times T_{\text{fun}}, \quad (11)$$

where $T_{\text{top}} = \{\text{adj}, \text{cross}\}$ and $T_{\text{fun}} = \{\text{loc}, \text{inf}, \text{net}, \text{data}, \text{org}\}$; the temporal set T and the type set T_τ are distinct. For each inter-level edge e , $\tau(e) = (\tau_{\text{top}}(e), \tau_{\text{fun}}(e))$, where $\tau_{\text{top}}(e)$ specifies whether the edge is adjacent or cross-level and $\tau_{\text{fun}}(e)$ its functional semantics (Table 3). For example, an edge between an N2 logical interface at L_n and an AMF service instance at L_s has $\tau = (\text{adj}, \text{net})$, because L_n and L_s are adjacent levels; a cross-level edge between a data-centre jurisdiction at L_g and a NOC/compliance role at L_o has $\tau = (\text{cross}, \text{org})$, connecting non-adjacent levels through a regulatory or governance dependency.

The attribute domain is a set of typed key-value records:

$$A = \{(key, value, type, source, timestamp)\}, \quad (12)$$

and the attribute-mapping function is time-dependent:

$$\alpha : (V \cup E^{\text{intra}} \cup E^{\text{inter}}) \times T \rightarrow 2^A. \quad (13)$$

Thus $\alpha(x, t)$ returns the attributes associated with a vertex or edge x at time t . Vertex attributes may include identifier, type, level, criticality, location, configuration, owner, software version, CVE/CVSS, ATT&CK technique, IoC, and jurisdiction; edge attributes may include relation semantics, direction, admissibility, criticality, protocol, evidence source, and exploitability indicator.

For algorithmic analysis, two derived functions are introduced. The weight function

$$w : E^{\text{intra}} \cup E^{\text{inter}} \rightarrow \mathbb{R}_{\geq 0} \quad (14)$$

assigns a traversal or risk score to each edge, which may be derived from edge criticality, CVSS-related attributes, exploitability, telemetry confidence, or analyst-defined priorities in $\alpha(e, t)$. The propagation predicate

$$\text{propagatable} : E^{\text{intra}} \cup E^{\text{inter}} \rightarrow \{\text{true}, \text{false}\} \quad (15)$$

indicates whether an edge can be used for attack or impact propagation, since not every dependency is automatically exploitable.

The state domain distinguishes vertex and edge states:

$$\Sigma = \Sigma_V \cup \Sigma_E, \quad (16)$$

where vertex states decompose into operational, security, and workflow components:

$$\Sigma_V = \Sigma_V^{\text{op}} \times \Sigma_V^{\text{sec}} \times \Sigma_V^{\text{wf}}. \quad (17)$$

For example, $\Sigma_V^{\text{op}} = \{\text{active}, \text{inactive}, \text{degraded}, \text{unavailable}\}$, $\Sigma_V^{\text{sec}} = \{\text{normal}, \text{vulnerable}, \text{compromised}, \text{exposed}\}$, and $\Sigma_V^{\text{wf}} = \{\text{none}, \text{alert}, \text{incident_opened}, \text{escalated}\}$; edge states may include active, inactive, degraded, overloaded, and broken. The state function is therefore a pair of typed functions:

$$\sigma_V : V \times T \rightarrow \Sigma_V, \quad (18)$$

$$\sigma_E : (E^{\text{intra}} \cup E^{\text{inter}}) \times T \rightarrow \Sigma_E, \quad (19)$$

and for compactness σ denotes the pair (σ_V, σ_E) . This typing prevents vertex-only states such as compromised or exposed from being assigned to edges, while still allowing both vertices and edges to evolve over time. The temporal set is

$$T = \{t_0, t_1, \dots, t_n\}, \quad (20)$$

representing either discrete observation points or observation intervals. Together, α and σ allow the model to capture changes in attributes, states, relations, and CTI evidence over time.

3.5. Illustrative case study: multi-step attack on 5G infrastructure

To illustrate the applicability of the proposed model, this section presents a synthetic case study based on a multi-step attack scenario targeting a 5G mobile operator's infrastructure. The case study is not intended as empirical validation; rather, it shows by example how the formal components of M_{cs} can represent multilevel propagation, CTI enrichment, typed dependencies, temporal state changes, and SOC/NOC escalation.

The modelled ICT segment comprises seven vertices across six levels. At the geospatial level L_g , v_{g1} represents the data-centre site and jurisdictional context of the operator in the Republic of Kazakhstan. At the physical level L_p , v_{p1} represents a 5G gNB hardware/control module. At the logical-network level L_n , v_{n1} represents the N2/NGAP signalling channel between the gNB and the AMF. At the service-functional level L_s , v_{s1} represents the AMF service instance and v_{s2} the UDM service instance. At the information-data level L_d , v_{d1} represents the UDR subscriber-data repository. At the organizational-personnel level L_o , v_{o1} represents the NOC/SOC administrator or incident-response role.

The attack unfolds in six analytical steps, summarized in Table 4. In Step 1 the adversary exploits a synthetic remote-code-execution vulnerability in the gNB management/control component (CVE-20XX-XXXX, CVSS 8.8); ATT&CK T1190 (Exploit Public-Facing Application) applies only if the vulnerable interface is externally reachable, otherwise it is recorded as a domain-specific CTI tag, and $\sigma_V(v_{p1}).\text{sec}$ moves from normal to compromised. In Step 2 the adversary pivots to the N2 signalling channel via the

Table 4
Corrected Attack Path in the Proposed Cyberspace Model

Step	Propagation / relation	Edge type	State change	CTI / evidence
1	Initial compromise of v_{p1} (L_p)	—	normal $\rightarrow$ compromised	Synthetic CVE-20XX-XXXX, CVSS 8.8; T1190 only if externally reachable
2	$v_{p1}(L_p) \rightarrow v_{n1}(L_n)$	(adj, inf)	normal $\rightarrow$ degraded/controlled	Pivot evidence; interface-control telemetry
3	$v_{n1}(L_n) \rightarrow v_{s1}(L_s)$	(adj, net)	normal $\rightarrow$ compromised/degraded	Malformed NGAP/NAS signalling; domain-specific CTI tag
4	$v_{s1}(L_s) \rightarrow v_{s2}(L_s)$	intra-level E^{intra}	normal $\rightarrow$ suspicious/compromised	Unauthorized service-to-service request
5	$v_{s2}(L_s) \rightarrow v_{d1}(L_d)$	(adj, data)	protected $\rightarrow$ exposed	Anomalous-query IoC; affected subscriber-data category
6	$v_{d1}(L_d) \rightarrow v_{o1}(L_o)$; $v_{g1}(L_g) \rightarrow v_{o1}(L_o)$	(adj, org); (cross, org)	none $\rightarrow$ incident_opened/escalated	SOC/NOC incident; jurisdictional/regulatory context

adjacent infrastructure-implementation edge (v_{p1}, v_{n1}) , $\tau = (\text{adj}, \text{inf})$, marked *propagatable* = *true*, and v_{n1} becomes degraded/controlled. In Step 3 malformed NGAP/NAS signalling is sent toward the AMF over $(v_{n1}, v_{s1}) \in E_{\text{adj}}$, $\tau = (\text{adj}, \text{net})$ —an adjacent, *not* cross-level, transition, since L_n and L_s are adjacent; it is tagged as signalling abuse rather than mapped to ATT&CK T1071 unless application-layer command-and-control is actually observed.

In Step 4 the compromised AMF interacts with the UDM through the intra-level service edge $(v_{s1}, v_{s2}) \in E^{\text{intra}}$, to which no τ value is assigned because τ is defined only for inter-level edges. In Step 5 the UDM accesses the UDR repository via $(v_{s2}, v_{d1}) \in E_{\text{adj}}$, $\tau = (\text{adj}, \text{data})$; v_{d1} moves from protected to exposed and $\alpha(v_{d1}, t_5)$ is enriched with an anomalous-query IoC, affected data category, times-tamp, and confidence score. In Step 6 the incident propagates to L_o via $(v_{d1}, v_{o1}) \in E_{\text{adj}}$, $\tau = (\text{adj}, \text{org})$, opening the incident-response workflow, while the cross-level governance edge $(v_{g1}, v_{o1}) \in E_{\text{cross}}$, $\tau = (\text{cross}, \text{org})$, supplies the jurisdictional and regulatory context—so the geospatial level informs SOC/NOC decisions without being modelled as a technical propagation step.

The corrected attack path distinguishes multilevel propagation from cross-level governance. The technical propagation path follows adjacent edges from L_p to L_n , L_s , L_d , and L_o , while the cross-level edge (v_{g1}, v_{o1}) represents a governance dependency between geospatial jurisdiction and the responsible organizational role. This avoids treating the $L_n \rightarrow L_s$ transition as cross-level, since these two levels are adjacent by definition.

4. Discussion

4.1. Algorithmic capabilities

Representing cyberspace as a directed, attributed, multilevel graph enables algorithmic analysis unavailable in purely conceptual models. The central operation is not the discovery of a “highest-probability” path— M_{cs} does not by itself define a probabilistic model—but of highest-scoring or highest-risk paths under a user-defined weight function w and a propagation predicate *propagatable*. Let $s \in V$ be a compromised source vertex, C_{target} a target class (e.g. “subscriber-data repository”), and $F \subseteq T_{\text{fun}}$ the allowed functional edge types; the traversal considers only edges e with *propagatable*(e) = *true* and, for inter-level edges, $\tau_{\text{fun}}(e) \in F$ (Algorithm 1).

Algorithm 1. Filtered multilevel attack-path discovery.

Input: graph $G = (V, E^{\text{intra}} \cup E^{\text{inter}})$, source s , target class C_{target} , allowed functional types F , weight function w , integer k .

Output: top- k highest-scoring paths.

1. Initialize priority queue Q with path $[s]$ and score 0; initialize result set $P = \emptyset$.
2. **while** $Q \neq \emptyset$ and $|P| < k$ **do**:
3. pop the highest-scoring path p ending at vertex u ;
4. **if** $\text{class}(u) = C_{\text{target}}$ **then** add p to P ;
5. **for** each outgoing edge $e = (u, v)$ **do**:
6. **if** $\text{propagatable}(e) = \text{false}$, **continue**;
7. **if** $e \in E^{\text{inter}}$ and $\tau_{\text{fun}}(e) \notin F$, **continue**;
8. **if** v already appears in p , **continue**;
9. push $p + [v]$ to Q with score $\text{score}(p) + w(e)$.
10. **return** P .

For sparse operational graphs, a priority-queue traversal over the filtered edge set E_F has complexity $O(|E_F| \log |V|)$ for a single-source traversal, excluding the cost of enumerating alternative paths. The same procedure can be implemented in a graph database by filtering edges on τ_{fun} , propagatable , state, and CTI attributes.

The state functions σ_V and σ_E support temporal reconstruction of incidents: by recording when vertices and edges move from normal to degraded, compromised, exposed, or *incident_opened* states, the model yields a timestamped audit trail aligned with SIEM, NDR, EDR, vulnerability-scanner, and CTI-feed evidence. The time-dependent attribute function $\alpha(x, t)$ is the binding point for CTI enrichment: CVE identifiers, CVSS scores, ATT&CK technique IDs, IoCs, confidence scores, telemetry references, and source timestamps can be attached to vertices and edges without changing the graph structure.

4.2. Practical implications for SOC and CTI workflows

Named levels and functionally typed edges translate the abstract formalism into operationally meaningful categories: an edge with $\tau = (\text{adj}, \text{net})$, such as an N2-to-AMF signalling dependency, directs attention to network monitoring and protocol-level signatures, while an edge with $\tau = (\text{cross}, \text{org})$, such as a jurisdiction-to-incident-response dependency, directs attention to governance, escalation, and compliance workflows—a semantic specificity absent from generic graph models and advantageous for triage and escalation. The model applies to both individual segments and large distributed architectures. In the 5G context the six levels map naturally onto the system architecture of 3GPP TS 23.501 [23]: L_p to RAN hardware, L_n to the N2/N3/N4/N6 reference interfaces, L_s to core network functions (AMF, SMF, UPF, UDM), L_d to subscriber/session databases, L_o to operator roles and regulatory obligations, and L_g to jurisdictional context for cross-border attribution.

4.3. Limitations and future directions

Several limitations must be acknowledged. First, the model is a formal framework; operational deployment requires populating the graph from real ICT and CTI sources via standardized attribute schemas and machine-readable bindings to STIX 2.1 and ATT&CK identifiers. Second, cross-level connections can cause combinatorial edge growth (bounded by $O(k^2 n^2)$ for n vertices per level and k levels); in practice this is expected to be sparse, but hierarchical aggregation, attribute-based pruning, and compressed adjacency structures will be needed at very large scale. Third, σ currently uses discrete categorical states over discrete time points, and probabilistic or continuous-time extensions would increase fidelity for quantitative risk assessment. Fourth, the contribution is conceptual: the case study is synthetic, and empirical validation on real ICT and 5G datasets is required to assess completeness, precision, and analytical utility at scale.

Finally, M_{cs} distinguishes dependency representation from attack propagation. The existence of an edge does not by itself imply exploitability: attack or impact propagation is allowed only when the

propagation predicate is true, when the relevant edge attributes support such an interpretation, and when the current states of the elements involved permit traversal. This distinction prevents the model from over-approximating every operational dependency as an attack path.

5. Conclusions

This paper addressed the absence of a unified, computable cyberspace model tailored to CTI-oriented analysis of ICT systems. A review of multilayer, network-of-networks, topographic/cartographic, ontological, attack-graph, and digital-twin approaches showed that existing model families cover important aspects of cyberspace representation but do not jointly provide multilevel ICT coverage, formal graph computability, typed inter-level dependencies, temporal state tracking, and CTI-oriented attribute binding.

The principal contribution is the Multilevel Attributed Cyberspace Model $M_{cs} = (L, V, E^{intra}, E^{inter}, A, \lambda, \tau, \alpha, \Sigma, \sigma, T)$. Its novelty lies in unifying, within a single graph-theoretic formalism, six ICT-oriented cyberspace levels, directed intra-level and inter-level relations, topology- and function-based edge typing, time-dependent CTI attributes, and typed temporal state functions. The model is designed to support algorithmic tasks such as filtered multilevel traversal, state-change auditing, CTI enrichment, and SOC/NOC workflow reconstruction.

The synthetic 5G case study illustrated these capabilities by example, representing a gNB compromise as a multilevel path through the N2 signalling channel, the AMF and UDM service functions, the UDR subscriber-data repository, and an organizational incident-response role, while a separate cross-level governance edge captured the jurisdictional context—clarifying that adjacent technical propagation and cross-level governance dependencies must be represented separately.

Future research will pursue four directions: empirical validation on real ICT and 5G datasets; prototype implementation using a graph-database backend and formal queries; machine-readable mappings to STIX 2.1, ATT&CK, CVE, CVSS, and SIEM telemetry schemas; and probabilistic or continuous-time extensions of the state model for quantitative risk assessment and propagation-likelihood estimation.

Information on funding

This research was funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP26199941).

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne, M. Ylianttila, 5g privacy: Scenarios and solutions, in: Proceedings of the IEEE 5G World Forum (5GWF), Santa Clara, CA, USA, 2018, pp. 197–203.
- [2] 3GPP, Security Architecture and Procedures for 5G System, Technical Specification TS 33.501, 3rd Generation Partnership Project, Sophia Antipolis, France, 2022.
- [3] OASIS, Stix version 2.1, OASIS Committee Specification 01, 2021. URL: <https://docs.oasis-open.org/cti/stix/v2.1/cs01/>.
- [4] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, C. B. Thomas, MITRE ATT&CK: Design and Philosophy, Technical Report MTR190003, MITRE Corporation, Bedford, MA, USA, 2020.

- [5] O. Holubnychyi, et al., Self-organization technique with a norm transformation based filtering for sustainable infocommunications within CNS/ATM systems, in: I. Ostroumov, M. Zalisky (Eds.), *Proceedings of the 2nd International Workshop on Advances in Civil Aviation Systems Development*, volume 992 of *Lecture Notes in Networks and Systems*, Springer Nature Switzerland, Cham, 2024, pp. 262–278. doi:10.1007/978-3-031-60196-5_20.
- [6] O. Sheyner, J. Haines, S. Jha, R. Lippmann, J. M. Wing, Automated generation and analysis of attack graphs, in: *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, Oakland, CA, USA, 2002, pp. 273–284.
- [7] X. Ou, S. Govindavajhala, A. W. Appel, Mulval: A logic-based network security analyzer, in: *Proceedings of the 14th USENIX Security Symposium*, Baltimore, MD, USA, 2005, pp. 113–128.
- [8] N. Poolsappasit, R. Dewri, I. Ray, Dynamic security risk management using bayesian attack graphs, *IEEE Transactions on Dependable and Secure Computing* 9 (2012) 61–74. doi:10.1109/TDSC.2011.34.
- [9] V. Mavroeidis, S. Bromander, Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence, in: *Proceedings of the European Intelligence and Security Informatics Conference (EISIC)*, Athens, Greece, 2017, pp. 91–98.
- [10] E. M. Hutchins, M. J. Cloppert, R. Amin, Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, in: *Proceedings of the 6th International Conference on Information Warfare and Security (ICIW)*, Washington, DC, USA, 2011, pp. 113–125.
- [11] A. Piplai, S. Mittal, A. Joshi, T. Finin, J. Holt, R. Breadner, Creating cybersecurity knowledge graphs from malware after action reports, *IEEE Access* 8 (2020) 211691–211703. doi:10.1109/ACCESS.2020.3039234.
- [12] D. Colle, Representing cyberspace with the basic formal ontology, in: *Proceedings of the 13th International Conference on Formal Ontology in Information Systems (FOIS)*, volume 3828 of *CEUR Workshop Proceedings*, Enschede, Netherlands, 2024.
- [13] B. Donohue, M. Jensen, A. P. Cox, R. Rudnicki, A common core-based cyber ontology in support of cross-domain situational awareness, in: *Proceedings of SPIE 10635, Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR IX*, 2018, p. 106350F. doi:10.1117/12.2307719.
- [14] M. Halappanavar, S. Choudhury, E. Hogan, P. Hui, J. R. Johnson, I. Ray, L. Holder, Towards a networks-of-networks framework for cyber security, *arXiv preprint arXiv:1304.6761* (2013). URL: <https://arxiv.org/abs/1304.6761>.
- [15] M. Halappanavar, E. Cotilla-Sanchez, E. Hogan, D. Duncan, Z. Huang, P. D. H. Hines, A network-of-networks model for electrical infrastructure networks, *arXiv preprint arXiv:1512.01436* (2015). URL: <https://arxiv.org/abs/1512.01436>.
- [16] S. J. Kim, B. B. Lim, Cyberspace modelling for critical infrastructure systems, *International Journal of Computer Science and Network Security* 20 (2020) 22–30.
- [17] J. Applegate, *Topography of cyberspace and its consequences for operations*, 2013.
- [18] Z. Li, M. Chen, Cybermaps: A novel mapping approach for cyber situational awareness, *ISPRS International Journal of Geo-Information* 12 (2023) 353. doi:10.3390/ijgi12090353.
- [19] B. Jiang, X. You, K. Li, T. Li, X. Wang, D. Si, Virtual geo-cyber environments: Metaphorical visualization of virtual cyberspace with geographical knowledge, *International Journal of Digital Earth* 17 (2024). doi:10.1080/17538947.2024.2324959.
- [20] M. Eckhart, A. Ekelhart, A specification-based state replication approach for digital twins, in: *Proceedings of the ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC)*, Toronto, Canada, 2018, pp. 36–47.
- [21] D. D. Clark, *Characterizing Cyberspace: Past, Present and Future*, Working Paper, MIT Computer Science and Artificial Intelligence Laboratory, Cambridge, USA, 2010.
- [22] A. Klimburg, P. Mirtl, *Cyberspace and Governance: A Primer*, Technical Report Working Paper 65, Austrian Institute for International Affairs (oiip), 2012.
- [23] 3GPP, *System Architecture for the 5G System (5GS)*, Technical Specification TS 23.501, 3rd Generation Partnership Project, 2022.