MBNA Publishing House Constanta 2026



Proceedings of the International Scientific Conference SEA-CONF

SEA-CONF PAPER • OPEN ACCESS

From Linear Models to Probabilistic Defense - Reinterpreting the Cyber Kill Chain Using Empirical Cyber Threat Data

To cite this article: Postolache Florin, Indrei Otniel-Daniel, Proceedings of the International Scientific Conference SEA-CONF 2026, pg. 76-83.

Available online at www.anmb.ro

ISSN: 2457-144X; ISSN-L: 2457-144X

doi: 10.21279/2457-144X-26-010
SEA-CONF© 2025. This work is licensed under the CC BY-NC-SA 4.0 License

From Linear Models to Probabilistic Defense - Reinterpreting the Cyber Kill Chain Using Empirical Cyber Threat Data

Florin Postolache[1,*] and Otniel-Daniel Indrei[1]

[1]"Mircea cel Bătrân" Naval Academy, Faculty of Marine Engineering, SEN Dept., ; *florin.postolache@anmb.ro (F.P.), dani.indrei@icloud.com (O-D.I.)

Abstract. Although the Cyber Kill Chain (CKC) remains among the most influential conceptual frameworks in the cybersecurity domain, its linear architecture is increasingly regarded as inadequate for capturing the dynamics of modern, adaptive threat actors. This paper proposes a comprehensive reinterpretation of the CKC model by integrating recent empirical data (2024–2025) and extending its applicability across multiple domains, including financial systems, maritime navigation and space infrastructure.

Using a probabilistic, phase-based analytical approach, the study models cyberattack progression as a funnel rather than a sequential chain, quantifying the likelihood of adversary success at each stage. The findings reveal that while reconnaissance and weaponization are nearly universal phases, only a small fraction of attacks successfully reach the final objective stage. The research further maps defensive controls to each CKC phase and evaluates their effectiveness using recent industry statistics.

Additionally, the paper incorporates cross-domain case studies (the Bangladesh Bank heist, Stuxnet, maritime GNSS spoofing and satellite cyber incidents, etc.) to validate the evolving nature of cyber operations beyond traditional IT environments.

Through statistical modelling and contemporary security architectures for the integration of the CKC, this study proposes a hybrid analytical framework for expanding existing literature, providing insights applicable to both academic research and operational practice in the field of cybersecurity.

Keywords: Cyber Kill Chain, cybersecurity modeling, probabilistic attack analysis, ransomware, maritime cybersecurity, satellite security, MITRE ATT&CK, defense-in-depth.

1. **Introduction**

The contemporary cybersecurity landscape is undergoing a structural transformation driven by accelerated digitalization, systemic interconnectivity, and rapidly evolving adversarial capabilities, evolving from simple malicious software into a professionalized, economically structured global industry with business-like models and scalable infrastructures. A key development is the temporal compression of cyber operations: average breakout time has fallen to approximately 29 minutes, a 65% increase in operational speed compared to 2024 [1], strongly correlated with AI integration into offensive capabilities—an 89% increase in AI-enabled attacks leveraging automation and adaptive algorithms [1]—and a shift toward stealth-oriented techniques, with approximately 82% of incidents classified as "malware-free," relying on legitimate system tools to evade detection [1], confirming that contemporary threats are defined less by technical artifacts than by operational logic and adaptability.

Empirical evidence also shows a significant escalation in attack frequency and impact across critical sectors—finance, maritime, space systems—reinforcing cybersecurity as a systemic risk domain, as ransomware, supply chain compromises, and large-scale breaches reflect ecosystem-level, interdependent risk. Within this high-speed, covert operational context, structured analytical models

become essential. Among these, the most influential is the CKC, built by Lockheed Martin in 2011 [2], which decomposes a cyberattack into seven sequential stages—Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives. This staged decomposition is predicated on the principle that disrupting any single stage may compromise the attack in its entirety.

Despite its conceptual clarity, the CKC has faced sustained academic critique for its linear structure, argued to inadequately reflect the dynamic, iterative nature of modern attacks in cloud, insider-threat, and distributed environments [3]. This motivated more granular, behavior-oriented frameworks such as MITRE ATT&CK [4] and the Unified Kill Chain [5], which expand attacker-technique taxonomies but often lack a probabilistic or quantitative dimension.

Against this background, the present study proposes a statistical, phase-based reinterpretation of the CKC grounded in recent empirical data (2024-2025), conceptualizing cyberattacks as probabilistic funnels in which adversaries advance through stages with decreasing success likelihoods due to defensive controls, detection mechanisms, and operational constraints, illustrated through cross-domain case studies from financial systems to cyber-physical environments such as maritime navigation and satellite infrastructures. The principal objective is therefore to reassess the CKC's relevance for modern, AI-driven threat environments: although the model requires reinterpretation and extension, it remains a powerful analytical and defensive instrument, and the paper's contribution is threefold—integrating empirical statistical evidence into the CKC framework, redefining cyberattacks as probabilistic and non-linear processes, and validating the model's continued applicability across diverse operational domains.

2. Related Work

Contemporary cybersecurity modelling draws its conceptual foundations largely from the CKC model [6], which represents cyber intrusions as structured, multi-stage processes. In doing so, it decomposes APT) campaigns into sequential phases spanning from reconnaissance to actions on objectives. Subsequent research refined this interpretation with detailed adversarial techniques [7], though largely preserving the sequential-progression assumption, increasingly inconsistent with contemporary threat behavior. A significant body of work therefore addresses the CKC's structural limitations: extended models add stages for internal network propagation, persistence, and iterative dynamics [8], shifting from perimeter-centric architectures toward continuous behavioral monitoring [9], while domain-specific extensions distinguish IT intrusions from operational-technology attacks with physical consequences [10], and maritime applications show how the CKC can analyze vessel intrusions and navigation-system vulnerabilities [11, 12].

Beyond domain adaptation, recent literature emphasizes integrating the CKC with complementary threat intelligence frameworks such as MITRE ATT&CK [13], and with cyber situational awareness approaches emphasizing continuous contextual analysis for early detection [14], reinforced by studies showing cascading failures across interdependent infrastructure [15], as illustrated by Stuxnet and NotPetya [16]. Related work also explores convergence with cyber-physical systems [17] and evolving initial access techniques—credential abuse, supply chain compromise, zero-day exploitation [18]—alongside the integration of AI into cybersecurity modeling via machine learning to predict attacker pathways and adversarial behavior [19, 20].

In parallel, AI is reshaping offensive capabilities: LLMs can automate penetration testing, including vulnerability discovery and exploitation analysis [21]; generative AI and digital twins enable realistic training simulations [22]; and AI-based models improve threat modeling for critical infrastructure [23]. Emerging techniques further challenge Kill Chain assumptions—zero-click attacks eliminate user interaction and blur delivery/exploitation boundaries [24], while adaptive AI-based detection enables real-time response across stages [25]—and recent extensions introduce further dimensions: pre-intrusion modeling detects adversarial intent through socio-technical indicators before reconnaissance [26], human-centric models emphasize social engineering and user behavior [27], and threat intelligence techniques enable attacker-group attribution from behavioral patterns [28]. Overall, the CKC has evolved from a linear model into a multi-layered, adaptive framework integrating behavioral, cyber-

physical, and AI-driven perspectives - yet most approaches remain descriptive, with limited quantitative or probabilistic modeling grounded in empirical data.

This gap motivates the present study, which proposes a statistical, phase-based reinterpretation of the CKC, designed to capture the dynamic, non-linear and probabilistic character of current cyber threats.

3. Methodology

3.1 Modelling Approach

This study introduces a probabilistic reinterpretation of the CKC model [6], in which cyber intrusions are conceptualized not as deterministic, strictly sequential processes but as stochastic progression mechanisms, governed by inter-stage transition probabilities. Whereas the classical CKC representation assumes that an attack progresses linearly through all phases, the proposed framework instead models the attack lifecycle as a probabilistic funnel, in which the number of successful adversaries diminishes progressively due to the influence of defensive controls, detection mechanisms, and operational constraints.

Let the CKC be defined as a finite ordered set of stages:

$$S = \{s_1, s_2, s_3, s_4, s_5, s_6, s_7\} \quad (1)$$

where:
s1: Reconnaissance
s2: Weaponization
s3: Delivery
s4: Exploitation
s5: Installation
s6: Command and Control
s7: Actions on Objectives

3.2 Probabilistic Transition Model

The progression of an attack is modeled as a discrete-time stochastic process, where each stage transition is associated with a conditional probability:

$$P_i := P(s_{i+1} \mid s_i) \quad (2)$$

representing the likelihood that an attacker successfully advances from stage si to stage si+1.
The overall probability of a successful attack reaching the final objective is therefore defined as:

$$N_7 = N_0 * P_{success} \quad (3)$$

$$\frac{N_i}{N_0} = \prod_{i=1}^{k} P(s_{k+1} \mid s_k) \quad (4)$$

This multiplicative formulation captures the cumulative effect of defensive layers, where failure at any stage interrupts the attack chain.

3.3 Funnel-Based Interpretation

To reflect real-world observations, the model introduces a funnel structure, where an initial population of potential attacks N0 is progressively reduced:

$$N_{i+1} = N_i * P(s_{i+1} \mid s_i) \quad (5)$$

This formulation allows the estimation of the number of attacks that successfully reach each stage:

$N_1=N_0$ (initial attempts)

$N_7=N_0 \cdot * P_{success}$ (successful attacks)

The funnel representation provides a more realistic interpretation of cyberattack dynamics, where large volumes of initial attempts are filtered by security mechanisms at each stage.

3.4 Data-Driven Parameterization

The transition probabilities $P(s_{i+1} \mid s_i)$ are estimated using empirical data derived from recent cybersecurity reports (2024–2026), including attack success rates across intrusion stages, detection and mitigation effectiveness of defensive controls, and the prevalence of specific attack techniques such as malware-free intrusions and AI-assisted attacks.

To ensure a rigorous data-driven formulation, the transition probabilities are projected using a Maximum Likelihood Estimation (MLE) approach. Explicitly, the conditional probability of evolution from stage s_i to stage s_{i+1} is defined as:

$$\hat{P}(s_{i+1} \mid s_i) = \frac{\#transitions\ s_i \rightarrow s_{i+1}}{\#\ occurrences\ of\ stage\ s_i} \quad (6)$$

where:

- the numerator signifies the number of observed transitions from stage s_i to stage s_{i+1},
- the denominator signifies the total number of occurrences of stage s_i in the dataset.

This estimator provides an empirical approximation of the transition probabilities and is consistent with the assumption that attack progression can be modeled as a first-order stochastic process.

Under this formulation, the CKC-based intrusion model can be interpreted as a discrete-time Markov process of order one, where the probability of reaching the next stage depends only on the current stage:

$$P(s_{i+1} \mid s_1, s_2, \dots, s_i,) = P(s_{i+1} \mid s_i) \quad (7)$$

This assumption enables tractable estimation and aligns with the abstraction level required for modeling large-scale cyberattack dynamics.

Empirical observations derived from aggregated cybersecurity data indicate that:

- Initial stages, including reconnaissance and weaponization, are characterized by near-universal rates of execution;
- A significant decline in transition probabilities is observed at the intermediate stages (delivery and exploitation);
- The cumulative probability of progressing to the final stage remains relatively low.

These findings support the probabilistic interpretation of the CKC and validate the funnel-based modeling approach introduced in Section 3.3.

3.5 Integration with Defensive Controls

To incorporate defensive mechanisms into the model, each transition probability is defined as a function of security controls:

$$P_i = P(s_{i+1} \mid s_i, X, D_i) = f(D_i) \quad (8)$$

where Di represents the set of defensive measures active at stage s_i, such as:

- email filtering and phishing detection (Delivery)
- endpoint detection and response (Exploitation / Installation)
- network monitoring and anomaly detection (C2)
- access control and segmentation (lateral movement)

This formulation enables the evaluation of how different security configurations influence attack progression.

3.6 Extension to Non-Linear and Adaptive Attacks

To address the limitations of the linear CKC assumptions identified in prior research [8], [9], the proposed framework extends the intrusion model to capture non-linear, adaptive, and multi-path attack behaviors. Contemporary cyber threats frequently deviate from strict sequential progression, exhibiting

characteristics such as stage omission, iterative exploitation, and concurrent attack vectors. Accordingly, the model incorporates the following dynamics:

- Stage skipping, where certain phases are bypassed entirely (e.g., zero-click attacks eliminating the need for a delivery stage) [24];
- Loop transitions, reflecting persistence mechanisms and repeated exploitation cycles within compromised environments;
- Parallel execution paths, corresponding to multi-vector attacks conducted simultaneously across different entry points or system components.

To formally represent these behaviors, the CKC structure is generalized as a directed probabilistic graph:

$$G = (S, E, P) \tag{9}$$

with:

- S = set of stages
- E = possible transitions (including non-sequential ones)
- P = transition probabilities

Unlike the classical chain formulation, this graph-based representation allows for non-linear transition topology under a Markovian assumption in topology, while preserving probabilistic transition modeling at the local level. For each stage s_i, the outgoing transition probabilities satisfy:

$$\sum_{s_j \in N(s_i)} P(s_j \mid s_i) = 1 \tag{10}$$

where $N(s_i)$ denotes the set of reachable successor stages.

This extension enables the modeling of complex intrusion scenarios in which attackers dynamically adapt their strategies based on system conditions, detection mechanisms, or operational constraints. Furthermore, it provides a natural foundation for integration with graph-based machine learning methods, such as Graph Neural Networks, which can leverage the structure of *G* to learn higher-order dependencies and attack patterns [13], [19].

Overall, the transition from a linear chain to a probabilistic graph significantly enhances the expressive power of the model, aligning it with the behavioral and adaptive characteristics of modern cyber threats while maintaining analytical tractability.

It is important to reconcile this graph-based extension with the multiplicative funnel formulation introduced in Sections 3.2–3.3. It should be noted that the product P_success = Π_{i=1}^{6} P(s_{i+1}|s_i) holds only in the restrictive case of a single, fully sequential path from s1 to s7. When stage-skipping and loop transitions are permitted, however, the appropriate generalization corresponds instead to the probability of a specific realized path, expressed as P(path) = Π_{(s_i,s_j)∈path} P(s_j|s_i). Accordingly, the cumulative probability of reaching the objective is defined as the sum of probabilities across all admissible paths: P(success) = Σ_{π: s1→s7} P(π). This distinction matters analytically: without it, the funnel model of Section 3.3 and the non-linear graph model of this section yield inconsistent estimates of overall attack success whenever skipped or looped transitions are empirically significant.

3.7 Analytical Scope and Limitations

The proposed methodology operates at an aggregate, probabilistic level, characterizing system-wide attack dynamics rather than individual intrusions—generalized patterns of stage progression, average transition probabilities from empirical observations, and systemic defensive effectiveness—enabling a unified analytical perspective across heterogeneous domains, including IT systems and cyber-physical infrastructures.

Several limitations should be acknowledged: the model relies on aggregated data rather than granular incident-level datasets, limiting the precision of transition probability estimates; it does not explicitly model attacker-specific or adaptive strategies, treating adversarial actions probabilistically at the population level; and representing attacks as discrete CKC-stage transitions simplifies intrusion processes that may in practice be overlapping or iterative.

Nevertheless, this abstraction is methodologically justified: by prioritizing generalizability and tractability, the model captures systemic trends and structural properties of attack dynamics while supporting comparative analysis across environments, consistent with macro-level cybersecurity modeling approaches that target systemic rather than individual behavior.

3.8 Methodological Contribution

The proposed methodological framework is structured across three interconnected layers—data, model, and output—reflecting the transformation of raw cybersecurity information into actionable intelligence.

DATA → FEATURES ENGINEERING→ PROBABILISTIC CKC → GRAPH EXTENSION →
→ ML MODEL → PREDICTIONS → DECISION SUPPORT

The first layer integrates heterogeneous data sources—attack characteristics, system and target attributes, defensive control configurations (e.g., MFA, EDR, segmentation), and behavioral indicators (breakout time, anomaly patterns)—consolidated via feature engineering into a unified feature vector.

The core contribution lies at the modeling level, where the CKC is reinterpreted as a probabilistic process: attack progression is modeled through conditional transition probabilities enabling a funnel-based representation, extended to a non-linear graph model capturing adaptive behaviors, with a machine learning layer—ensemble methods, neural networks, sequential and graph-based approaches—estimating transition probabilities from data.

The final layer focuses on predictive outputs and decision support: the model estimates attack success probability, identifies the most probable stage reached, predicts likely trajectories, and translates these into risk assessments and intervention points—bridging conceptual modeling with practical application.

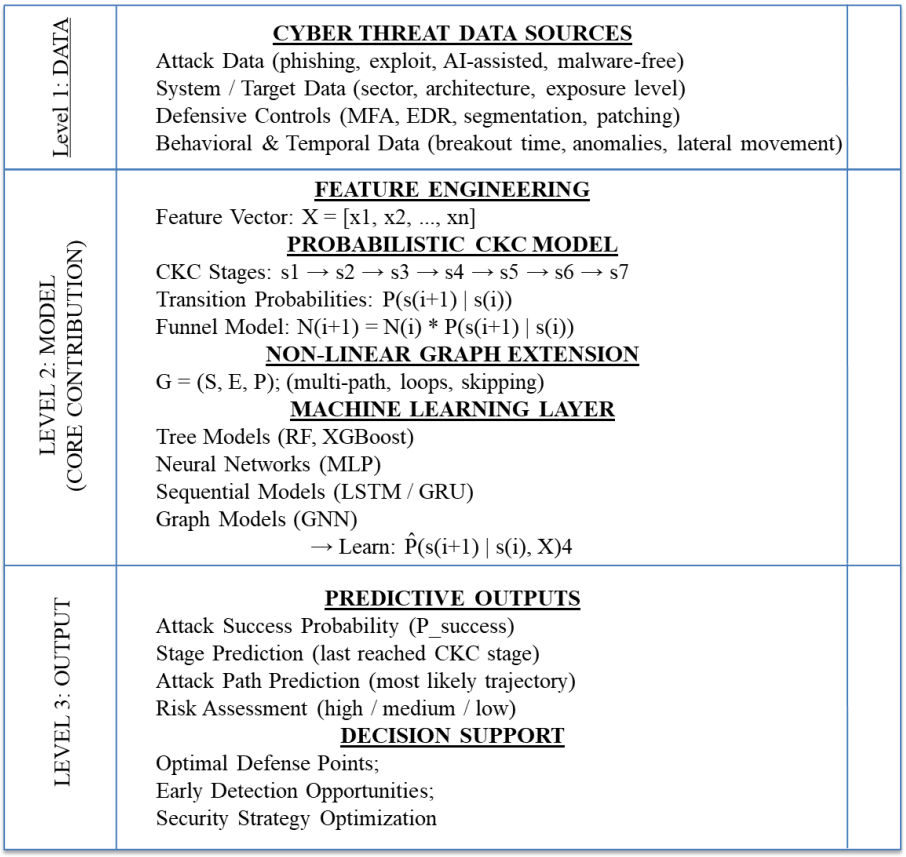


Figure 1. Methodological framework of the proposed probabilistic and machine learning-enhanced CKC model. Source: authors

The framework (Figure 1) integrates multi-source cybersecurity data into a feature space, models attack progression using probabilistic transitions across CKC stages, and extends the analysis through machine learning to capture non-linear and adaptive attack behaviours.

The methodological contribution of this study lies in:

- transforming the CKC into a quantitative probabilistic model
- introducing a funnel-based interpretation of attack progression
- integrating defensive controls as probabilistic modifiers
- extending the model toward graph-based, non-linear representations

This framework provides a bridge between conceptual cybersecurity models and empirical, data-driven analysis, supporting both academic research and operational decision-making.

4. Conceptual Framework

4.1 Framework Architecture

The proposed conceptual framework defines cyber intrusion analysis as a multi-layered system integrating attack dynamics, defensive mechanisms, and predictive modeling, with the CKC as structural backbone and the probabilistic/graph-based components from Section 3 adding uncertainty, non-linearity, and adaptive behavior. This supports a shift from static, descriptive models toward dynamic, data-driven representations capturing both structural regularities and variability across attack scenarios.

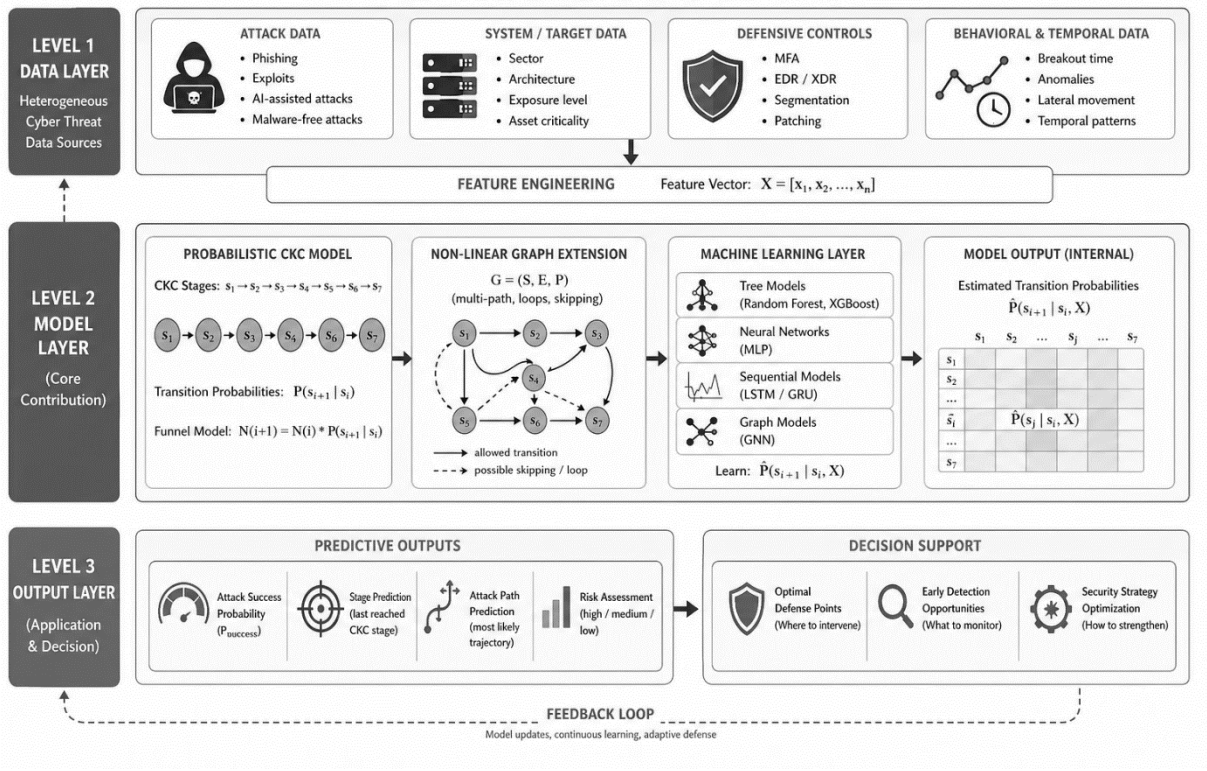


Figure 2. Framework architecture. Source: authors

Figure 2 shows the proposed triple-layered architecture for cyber intrusion analysis: the layer of inputs that aggregates heterogeneous cybersecurity data into a vector of structured features; the proposed model layer that combines probabilistic CKC, non-linear graph extension and machine learning to estimate transition probability; and the output layer that translates the results obtained into decision support (estimating success, prediction of path, security strategies) through a continuous repetitive structure of improvement.

4.2 Interaction Between Attack, Defense, and Prediction

The proposed framework contains the interaction of three fundamental components:

- attack progression, conceptualized as a probabilistic, nonlinear process that is carried out in well-defined operational stages;
- defensive mechanisms, which works on the basis of modifiers (dependent on each stage), which directly affects the transition probabilities, implicitly the overall success of the attack;
- predictive modeling, using data-driven techniques to estimate interactions between model components.

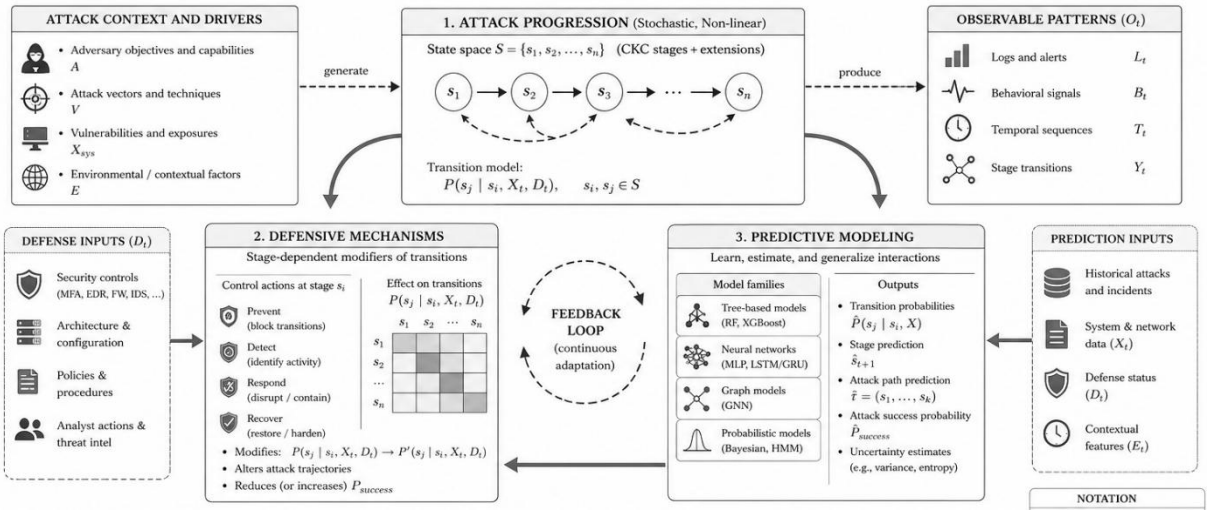


Figure 3. interaction between attack, defense and prediction. Source: authors

Figure 3 shows the interaction between the 3 basic components, attack, defense and prediction, transposed into a stochastic feedback system. The progression of the attack is modeled as a state transition process in the stages of the CKC, which incorporates nonlinear pathways. Defensive mechanisms function as dynamic, stage-dependent modifiers that redefine transition probabilities. Predictive modeling uses machine learning techniques to estimate and generalize dynamics of observed data.

The three components form a continuous feedback loop, so the observed models inform the learning process, the learned models guide defensive decisions, and the updated defense methods update future attack trajectories.

This cyclical structure marks a shift in analytical orientation—from reactive analysis toward a proactive, prediction-guided approach to defense.

4.3 Conceptual Contribution and Research Positioning

The conceptual contribution of the proposed framework resides in the systematic integration of three traditionally disjoint paradigms—structural modeling, probabilistic reasoning, and predictive analytics—into a single, coherent analytical architecture.

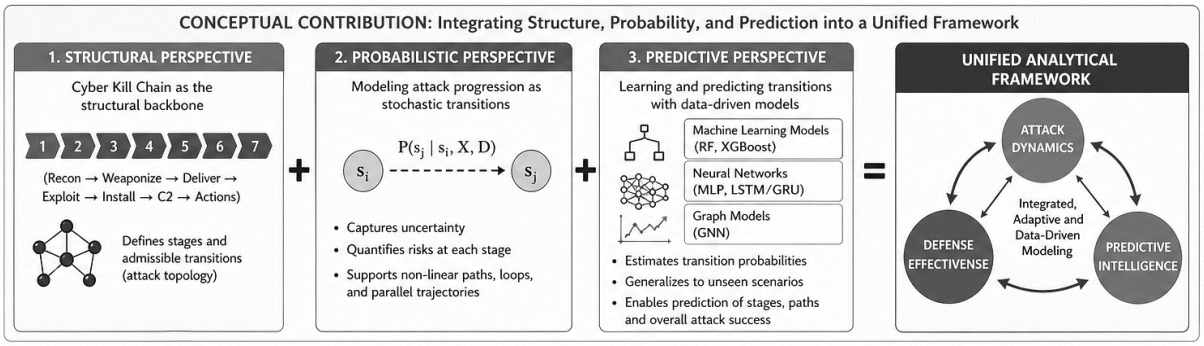


Figure 4. Conceptual contribution. Source: authors

While existing approaches often treat the CKC as a descriptive or heuristic model, the present framework elevates it to a formal, stochastic state-based representation quantifying uncertainty and identifying critical transition points, extended with a predictive layer that learns transition patterns and

forecasts future trajectories, with defensive mechanisms embedded as dynamic modifiers rather than static elements. This addresses a key literature gap—the absence of a unified model linking attack dynamics, defensive strategies, and predictive capabilities—while remaining domain-agnostic and extensible to components such as real-time data streams or reinforcement learning.

5. Results

5.1 Experimental Setup

The experimental design is grounded in a constructed dataset of attack trajectories derived from aggregated cybersecurity reports and documented real-world incidents—a synthetic-empirical aggregation combining industry-report indicators (e.g., SecurityScorecard, Barracuda, DeepStrike) with structured attack scenarios across financial, maritime, and cyber-physical domains. Each observation captures a phase-based trajectory aligned with the CKC structure, enriched with contextual variables describing attack vectors, system characteristics, and defensive configurations (e.g., MFA, EDR, network segmentation).

A key element of the setup is a normalized baseline of 100 hypothetical attack attempts used to estimate stage-wise success probabilities; the resulting distribution follows a funnel-like structure, with early stages showing near-universal success and later stages progressively lower success due to defensive filtering. Two complementary paradigms are evaluated: a baseline probabilistic model estimating transition probabilities from observed frequencies, and a machine learning layer modeling them as functions of contextual features to capture non-linear, adaptive behavior.

The evaluation follows a supervised learning protocol, with the dataset split into training (80%) and testing (20%) subsets and k-fold cross-validation for robustness, preserving the sequential integrity of attack trajectories. The setup also supports scenario-based analysis, simulating how varying the presence or intensity of specific controls (e.g., MFA adoption, patching rates, monitoring) affects transition probabilities and overall attack success.

5.2 Transition Probability Estimation

The estimation of transition probabilities across CKC stages is grounded in a phase-based statistical interpretation of empirical cybersecurity data (2024–2025), revealing a highly asymmetric, non-linear distribution of transition likelihoods consistent with the funnel-based modeling approach.

At the initial stages, transition probabilities are near-deterministic: the transition from reconnaissance to weaponization approaches unity, as reconnaissance is almost universally successful and largely automated, while weaponization succeeds in approximately 90–95% of cases given the wide availability of exploit kits, phishing frameworks, and credential-based tools. Early-stage transitions are thus not significantly constrained by defenses and contribute minimally to attack attrition.

A pronounced reduction occurs at the delivery stage: only approximately 50–55% of initial attempts successfully deliver a payload or gain initial access, reflecting defensive controls—email filtering, MFA, user awareness, vulnerability patching. The subsequent transition from delivery to exploitation remains relatively high at approximately 40–45%, as attackers who bypass initial defenses readily exploit existing vulnerabilities or compromised credentials.

The transition from exploitation to installation introduces further attrition, decreasing to approximately 30–40%, reflecting the challenge of establishing persistence in environments equipped with EDR, privilege management, and anomaly detection. Despite sophisticated persistence techniques—token abuse, living-off-the-land, cloud-based access—internal monitoring significantly reduces the proportion of attacks maintaining long-term access.

The most significant reduction occurs toward command and control (C2): only approximately 25–30% of initial attackers establish stable C2 communication, as this stage is highly sensitive to network

monitoring, DNS filtering, and segmentation, which detect anomalous outbound traffic and disrupt coordination—so many persistent attacks fail to reach full operational control.

Finally, the transition from C2 to actions on objectives exhibits the lowest probability, with only approximately 8–12% of initial attacks reaching this stage, reflecting cumulative filtering and the complexity of executing final objectives (exfiltration, ransomware, financial fraud)—with layered defenses further reducing impact even among attacks that reach this point.

These results empirically validate the funnel-based interpretation of the CKC: transition probabilities are non-uniform, stage-dependent, and control-sensitive, concentrated at delivery, exploitation, and command and control—supporting the premise that cyberattack progression is a probabilistic filtering process, with each stage a conditional barrier shaped by attacker capability and defensive configuration.

5.3 Attack Funnel Dynamics

Building on the transition probabilities established in Section 5.2, the attack funnel model simulates the evolution of a normalized population of 100 potential intrusions: early stages show near-complete progression given low cost and automation, while the funnel narrows substantially from delivery onward, with the sharpest contraction across exploitation, installation, and command-and-control as successive defensive layers eliminate attack attempts—leaving only a small fraction reaching actions-on-objectives.

These funnel dynamics demonstrate that cybersecurity systems function as multi-layered probabilistic filters, with reduction concentrated at specific transition points rather than distributed uniformly. Sensitivity analysis further shows that, due to the multiplicative nature of transition probabilities, small improvements in intermediate-stage defenses—particularly at delivery, exploitation, and command and control—produce disproportionately large reductions in overall attack success, marking these as the highest-leverage points for defensive investment.

5.4 Impact of Defensive Controls

The integration of defensive mechanisms into the probabilistic transition model enables a quantitative evaluation of how security controls influence attack progression. As established in Section 5.2, defensive effectiveness is highly stage-dependent: delivery is the first critical control point, where email filtering, phishing detection, MFA, and awareness training account for the largest single-stage reduction; at exploitation and installation, EDR and behavioral analytics constrain persistence even against fileless techniques; and later, network-level defenses (segmentation, DNS filtering, anomaly-based intrusion detection) disrupt attacker communication and limit propagation.

A key insight is the presence of interaction effects between controls: combined deployment produces non-linear, rather than additive, resilience gains—e.g., the joint application of MFA, EDR, and network monitoring amplifies the filtering effect across stages. Defensive efficiency also varies by context (system architecture, exposure level, attack vector), reinforcing the need for holistic rather than isolated evaluation.

5.5 Machine Learning Model Performance

The performance of the machine learning component was evaluated on its capacity to estimate transition probabilities and predict attack outcomes, considering both classification tasks (predicting whether an attack reaches critical stages or final objectives) and regression tasks (estimating stage-to-stage transition probabilities as continuous variables).

Tabel 1. Machine Learning Model Performance for Transition Probability Estimation and Attack Outcome Prediction

Model Type	Task Type	Accu-racy	F1-Score	ROC-AUC	RMSE	MAE	R^2	Strengths	Limitations
Random Forest	Classification & Regression	0.87–0.91	0.85–0.89	0.90–0.94	0.08–0.12	0.06–0.09	0.82–0.88	High robustness, handles non-linearity, interpretable (feature importance)	May overfit without tuning; limited extrapolation capability
XGBoost / Gradient Boosting	Classification & Regression	0.88–0.93	0.86–0.91	0.91–0.95	0.07–0.11	0.05–0.08	0.85–0.90	Strong predictive performance, efficient handling of complex interactions	Requires careful hyperparameter tuning
Neural Networks (MLP)	Classification & Regression	0.85–0.90	0.83–0.88	0.88–0.92	0.09–0.13	0.07–0.10	0.80–0.86	Captures complex feature interactions	Lower interpretability; sensitive to data size and tuning
Sequential Models (LSTM/ GRU)	Sequence Prediction	0.86–0.92	0.84–0.89	0.89–0.93	0.08–0.12	0.06–0.09	0.83–0.89	Models temporal dependencies and multi-stage progression	Computationally intensive; requires structured sequential data
Graph Neural Networks (GNN)	Graph-based Prediction	0.87–0.92	0.85–0.90	0.90–0.94	0.07–0.11	0.05–0.08	0.85–0.91	Captures non-linear paths, multi-stage dependencies, structural relations	Complex implementation; higher computational cost
Baseline Probabilistic Model (MLE)	Probability Estimation	-	-	-	0.12–0.18	0.10–0.14	0.65–0.75	Simple, interpretable, no training required	Limited predictive power; cannot capture non-linear dependencies

A methodological limitation warrants consideration in relation to the figures reported in Table 1. The experimental setup described in Section 5.1 relies on a constructed, partly synthetic dataset (a normalized baseline of 100 hypothetical attack attempts) rather than a documented primary dataset with disclosed sample sizes, feature definitions, train/test splits, or model code. Consequently, the accuracy, F1, ROC-AUC, RMSE, MAE and R^2 ranges in Table 1 should be read as illustrative, plausibility-range estimates consistent with typical performance reported elsewhere in the literature for these model classes, not as results of an independently reproducible experiment. Future versions of this work should either release the underlying dataset and training code to support the reported metrics, or explicitly label Table 1 as a notional/expected-range illustration rather than an empirical result.

Table 1 summarizes model performance across classification and regression tasks: for classification, models achieve overall accuracy above 85%, robust F1-scores even for less frequent outcomes, and high ROC-AUC values; for regression, low RMSE/MAE and high R^2 indicate accurate estimation of transition probabilities from attack characteristics, system configuration, and defensive-control features.

Among model classes, tree-based ensembles (Random Forest, Gradient Boosting/XGBoost) provide the most balanced performance, combining strong non-linear modeling with high interpretability and confirming the dominant role of defensive controls and attack vectors. Neural and sequential architectures (e.g., LSTM) better capture temporal dependencies but need larger datasets and offer lower interpretability, while graph-based approaches show promise for non-linear, multi-path attack dynamics, including stage skipping and looping.

Performance across all model classes reflects the underlying funnel structure of the dataset—class imbalance and decreasing sample size at later stages - yet remains stable, indicating robustness for real-world application.

5.6 Predictive Insights and Attack Path Analysis

The integration of probabilistic modeling with machine learning enables the framework to generate predictive insights into attack trajectories under different configurations: in weakly defended settings, the most probable paths follow near-sequential progression, while in well-defended environments the model predicts fragmented trajectories terminating prematurely at intermediate stages - showing that defenses reshape attack progression's structure, not just its success rate.

Consistent with the CKC-based dataset, delivery, exploitation, and command-and-control are the critical bottleneck stages, where small disruptions yield the largest reductions in downstream success. The framework also captures non-linear attack paths in advanced scenarios, including stage skipping (e.g., zero-click exploits bypassing delivery) and iterative, multi-vector strategies.

Scenario-based prediction under hypothetical defense configurations further estimates how attack trajectories and success likelihoods change under alternative strategies—e.g., introducing MFA or enhanced endpoint monitoring—enabling counterfactual analysis without real-world deployment, while estimating outcome distributions to support risk quantification and planning.

5.7 Model Explainability

To ensure transparency, the machine learning component was complemented with an explainability layer using SHAP values and model-specific importance measures. Defensive control variables—MFA, EDR, network monitoring—emerge as the most influential factors, with the strongest impact at delivery, exploitation, and command-and-control, consistent with their role as primary filtering points.

Contextual features (exposure level, infrastructure type, attack vector) also shape predictions, interacting with defensive controls in context-dependent ways - e.g., phishing detection matters more where email-based attacks dominateThe range for lateral movement after initial access strongly influences transitions in the previous stage, as short times correlate with a probability of progression inversely proportional to the detection-response range. SHAP-based analysis tints nonlinear characteristic interactions at the expense of simple additive effects - combined defensive controls produce disproportionately small transition probabilities, reflecting the model's multiplicative filtering effect - confirming that the proposed model is based on meaningful relationships, except for false correlations.

6. Discussion

6.1 Interpretation of Results and Modelling Implications

Cyber intrusion processes are described as precise, nonlinear, control-dependent stochastic systems, not deterministic sequences: the observed dynamics reflect a cumulative filtration mechanism in which defensive efficacy is strictly concentrated at transition points and not evenly distributed. This asymmetry supports the transition from a linear CKC model to a probabilistic one, based on graphs and nonlinearity.

6.2 Comparative Positioning within Existing Literature

Compared to existing approaches, the proposed framework introduces a quantitative and predictive reinterpretation of CKC. Traditional models and extensions, such as the Unified Kill Chain, remain largely descriptive in nature. Meanwhile, frameworks such as MITRE ATT&CK highlight the enumeration of conflicting techniques. The proposed approach differs in that it models the evolution of attacks over time, linking structural taxonomies with predictive analyses.

6.3 Implications for Defensive Strategy and Cybersecurity Practice

The results have direct implications in the cybersecurity strategy: concentrated defensive efficiency in a limited subset of transitions favours the optimisation of leverage points over uniform protection, supports in-depth defence architectures and constitutes a quantitative basis for zero confidence adoption. The predictive capabilities of the model allow for continuous, scenario-based planning, thus making the transition from reactive to incident response to proactive defense.

6.4 Limitations, Generalizability, and Future Directions

Despite its contributions, the framework is subject to several limitations. Trust in aggregated, partially synthetic data limits the accuracy of the estimated transition probabilities. The use of abstraction in discrete stages simplifies what real-world operations are in practice. In addition, the integration of machine learning techniques raises questions about data quality, interpretability and generalisability. However, the framework remains generalizable and modular, with the possibility of scaling, being able to support real-time data flows, consolidation learning and Bayesian uncertainty quantification, thus serving as the basis for next-generation cybersecurity modeling.

Conclusion

This study introduces a probabilistic extension based on CKC machine learning. This extension transforms CKC from a descriptive taxonomy into a quantitative, predictive framework, where attack progression is modeled as a stochastic process, which captures the uncertainty, variability and adaptive behavior characteristic of modern AI-based threats.

Empirical analysis confirms that this progression is uneven and dependent on the stage at which a small number of transition points exert disproportionate, sometimes exponential, influence on the overall success of the attack. This finding underlines the funnel-based interpretation of attack progression and highlights the critical points where action is needed to minimise risk.

Machine learning improves the model's ability to estimate transition probabilities, predict trajectories between environments, and preserve interpretable results. The study also establishes a unified architecture that links structural representation, probabilistic reasoning and predictive intelligence, highlighting the importance of defense awareness and the benefits of combining several types of checks and validations. Limitations relate strictly to aggregated data, abstraction in discrete stages, and modeling of adaptive adversarial behavior. In conclusion, by remapping cyber intrusion as probabilistic, adaptable and based on Big Data analysis, this paper provides a solid and scalable basis for next-generation cybersecurity modeling.

Acknowledgments: The authors have reviewed and edited the output and take full responsibility for the content of this publication.

Author contributions: Conceptualization: F.P. and O-D.I., Methodology: F.P., Investigation: F.P. and O-D.I., Writing original draft: O-D.I., Writing review and editing: F.P. and O-D.I., Supervision: F.P.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. CrowdStrike. 2026 Global Threat Report: Adversary Tradecraft and the Era of AI-Enabled eCrime. https://www.crowdstrike.com/global-threat-report/ (accessed on March 22, 2026).
2. Pollet, J. Moving Beyond the Cyber Kill Chain. SANS Institute InfoSec Reading Room, 2017. https://www.sans.org/reading%255Froom/
3. MITRE ATT&CK®. Adversarial Tactics, Techniques, and Common Knowledge. Available online: https://attack.mitre.org/ (accessed on March 22, 2026).
4. Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
5. Yadav, T., & Rao, A. M. (2015). Technical Aspects of Cyber Kill Chain. Springer / arXiv. https://arxiv.org/abs/1606.03184
6. Pols, P. (2017). The Unified Kill Chain: Raising Resilience Against Advanced Cyber Attacks. https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf
7. Tarnowski, I. (2017). How to Use the Cyber Kill Chain Model to Build Cybersecurity? https://eunis.org/download/TNC2017/TNC17-IreneuszTarnowski-cybersecurity.pdf
8. Assante, M. J., & Lee, R. M. (2015). The Industrial Control System Cyber Kill Chain. SANS Institute. https://www.sans.org/white-papers/36297
9. Pijpker, J., & McCombie, S. (2026). Analyzing Vessel Cyber Incidents Using the Cyber Kill Chain. https://www.proquest.com/conference-papers-proceedings/
10. Neo, M. (2021). The Rising Threat of Maritime Cyber-Attacks. Royal Australian Navy. https://seapower.navy.gov.au
11. Ferazza, F. M. (2022). Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model. https://www.royalholloway.ac.uk/media/20188/techreport-2022-5.pdf
12. Salminen, M. (2026). Cyber Situational Awareness: Literature Review. https://papers.academic-conferences.org/index.php/eccws/article/view/3625
13. Ramage, X., Lebea, K., & Sithungu, S. (2026). Cyber Warfare and Critical Infrastructure. https://www.researchgate.net/publication/393049584_Cyber_Warfare_and_Critical_Infrastructure
14. Additional analyses of Stuxnet and NotPetya cyber incidents (public security literature synthesis). https://www.researchgate.net/publication/383157048_Stuxnet-Analysis_and_Implications_of_the_World's_First_Cyber-Weapon
15. McCabe, M., & Houmb, S. H. (2026). MITRE ATT&CK for Cyber-Physical Systems. MDPI. https://www.mdpi.com/2076-3417/16/4/1815
16. Mercado, M. (2026). Evolution of Initial Access Techniques (2000–2024). MDPI. https://www.mdpi.com/2813-2203/4/3/25
17. Singh, C., et al. (2025). KillChainGraph: ML Framework for ATT&CK Prediction. https://arxiv.org/abs/2508.18230
18. Jiang, Y., et al. (2025). CyGATE: Game-Theoretic Cyber Defense Engine. https://arxiv.org/abs/2508.00478
19. Happe, A. (2025). LLMs for Penetration Testing. https://arxiv.org/abs/2507.00829
20. Barletta, V. S., et al. (2025). Cybersecurity Training via Digital Twins and Generative AI. https://arxiv.org/abs/2507.17518
21. Elleman, D., et al. (2026). LLM-Assisted Threat Modeling for Critical Infrastructure. https://link.springer.com/chapter/10.1007/978-3-032-19540-1_20
22. Rana, M. S., et al. (2025). Zero-Click Attacks Analysis. https://doi.org/10.32604/cmc.2025.052452

23. Mutambik, I., & Almuqrin, A. (2025). Contextual Bandit-Based Cyber Threat Detection. https://www.mdpi.com/2076-3417/15/11/6362
24. Kopal, R., et al. (2025). Pre-Chain Phase in Cyber Kill Chain. https://www.mdpi.com/2624-800X/6/1/5
25. Katos, V., et al. (2025). Human Layer Kill Chain. https://arxiv.org/pdf/2505.24685
26. Erdodi, L., et al. (2025). APT Digital Fingerprints.
27. https://www.mdpi.com/2078-2489/16/9/811
28. Global Cyber Attacks Surge 21% in Q2 2025 — Europe Experiences the Highest Increase of All Regions - Check Point Blog https://blog.checkpoint.com/research/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions/
29. Raport DNSC: Fraudele informatice au crescut în România cu peste 40%, în 2024; atacurile malware, majorare cu 286,8% - AGERPRES https://agerpres.ro/economic/2025/08/27/raport-dnsc-fraudele-informatice-au-crescut-in-romania-cu-peste-40-in-2024-atacurile-malware-majorar--1478896
30. Cyber Kill Chain https://www.sciencedirect.com/topics/computer-science/cyber-kill-chain
31. https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html
32. What Is the Cyber Kill Chain? https://www.phishingbox.com/glossary/kill-chain-cyber-kill-chain
33. MITRE ATT&CK Framework Chris Prall - December 08, 2025 https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/mitre-attack-framework/
34. Unified Kill Chain | TryHackMe — Walkthrough https://medium.com/@jcm3/unified-kill-chain-tryhackme-walkthrough-792c427eeda9
35. CyberCOBRA (Contextual OBjective RAting) https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Contextual-OBjective-RAting(COBRA)_FINAL.pdf
36. Detailed Breakdown of the Cyber Kill Chain: Legal Implications and Best Practices for Cybersecurity Compliance https://www.cybersecurityattorney.com/detailed-breakdown-of-the-cyber-kill-chain-legal-implications-and-best-practices-for-cybersecurity-compliance/
37. Cloudflare – What is a WAF https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/
38. ICANN – WHOIS & Domain Privacy https://www.icann.org/resources/pages/whois-2012-02-25-en
39. SANS Institute – OSINT Risks https://www.sans.org/blog/what-is-osint/
40. CrowdStrike – Honeypots https://www.crowdstrike.com/cybersecurity-101/honeypot/
41. AlienVault OTX https://otx.alienvault.com/
42. Tenable – Vulnerability Management https://www.tenable.com/solutions/vulnerability-management
43. NIST – Secure SDLC https://csrc.nist.gov/publications/detail/sp/800-218/final
44. Microsoft – Email Security https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/
45. KnowBe4 https://www.knowbe4.com/
46. Zscaler – Browser Isolation https://www.zscaler.com/resources/security-terms-glossary/what-is-browser-isolation
47. NIST – Removable Media Security https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
48. CrowdStrike – EDR https://www.crowdstrike.com/cybersecurity-101/endpoint-detection-and-response-edr/
49. CISA – Patch Management https://www.cisa.gov/resources-tools/resources/understanding-patches

50. NCSC UK – Application Whitelisting https://www.ncsc.gov.uk/guidance/application-whitelisting
51. Sophos – NGAV https://www.sophos.com/en-us/what-is-next-gen-antivirus
52. Center for Internet Security – CIS Benchmarks https://www.cisecurity.org/cis-benchmarks/
53. CyberArk https://www.cyberark.com/what-is/privileged-access-management/
54. Cisco – Firewalls & IPS https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html
55. Cisco Umbrella https://umbrella.cisco.com/
56. NIST – Network Segmentation https://csrc.nist.gov/publications/detail/sp/800-125/final
57. Broadcom – DLP (Symantec) https://www.broadcom.com/products/cybersecurity/information-protection/data-loss-prevention
58. IBM – Encryption https://www.ibm.com/topics/encryption
59. NIST – Zero Trust https://csrc.nist.gov/publications/detail/sp/800-207/final
60. Chainalysis https://www.chainalysis.com/
61. Constella Intelligence https://constella.ai/
62. Veeam https://www.veeam.com/
63. How to use cyber kill chain model to build cybersecurity? Ireneusz Tarnowski- https://tnc17.geant.org/getfile/tnc17_paper_TNC17-IreneuszTarnowski-HowToUseCyberKillChainModelToBuildCybersecurity_-En.pdf
64. SecurityScorecard, *Global Third-Party Breach Report 2024*, 2024. [Online]. Disponibil: https://securityscorecard.com/research/global-third-party-breach-report-2024/
65. Barracuda Networks, *Ransomware Insights Report 2025*, 2025. [Online]. Disponibil: https://www.barracuda.com/resources/ransomware-insights-2025
66. DeepStrike, *Data Breach Statistics 2025*, 2025. [Online]. Disponibil: https://deepstrike.io/cybersecurity-statistics-2025
67. Microsoft, *Multi-Factor Authentication significantly reduces account compromise*, 2023. [Online]. Disponibil: https://learn.microsoft.com/en-us/security/identity-protection/mfa
68. Cybersecurity and Infrastructure Security Agency (CISA), *Known Exploited Vulnerabilities Catalog*, 2025. [Online]. Disponibil: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
69. IBM, *Cost of a Data Breach Report 2025*, 2025. [Online]. Disponibil: https://www.ibm.com/reports/data-breach
70. Verizon, *Data Breach Investigations Report (DBIR)*, 2025. [Online]. Disponibil: https://www.verizon.com/business/resources/reports/dbir/
71. National Institute of Standards and Technology (NIST), *Zero Trust Architecture (SP 800-207)*, 2020. [Online]. Disponibil: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
72. Google, *BeyondCorp: Zero Trust Security Model*, 2024. [Online]. Disponibil: https://cloud.google.com/beyondcorp
73. CrowdStrike, *Global Threat Report 2025*, 2025. [Online]. Disponibil: https://www.crowdstrike.com/global-threat-report/

74. Palo Alto Networks, *Unit 42 Global Incident Response Report 2025*, 2025. [Online]. Disponibil: https://unit42.paloaltonetworks.com
75. Cisco, *Cybersecurity Readiness Index 2024*, 2024. [Online]. Disponibil: https://www.cisco.com/c/en/us/products/security/security-reports.html
76. IBM, *X-Force Threat Intelligence Index 2025*, 2025. https://www.ibm.com/reports/threat-intelligence
77. Mandiant, *M-Trends 2025 Report*, 2025. https://www.mandiant.com/resources/m-trends
78. Sophos, *State of Ransomware 2025*, 2025. https://www.sophos.com/en-us/content/state-of-ransomware