**Semi-Markov Models in Cybersecurity:**
**Duration-Aware Risk, Resilience, and Efficiency Analysis**

Nani Salia, Georgian Technical University, Tbilisi, Georgia

DOI: https://doi.org/10.52340/gbsab.2025.56.06

**Abstract**

Semi-Markov models (SMMs) relax the memoryless assumption of classical continuous-time Markov chains by allowing general sojourn-time distributions. In cybersecurity, where dwell time, lateral-movement duration, and remediation windows are rarely exponential, SMMs provide a natural representation of duration dependence and heterogeneous timing. We develop an SMM framework for (i) **threat-state inference** (compromise lifecycle), (ii) **resilience and efficiency metrics** (MTTD, MTTR, availability, cost per protected hour), and (iii) **policy optimization** (semi-Markov decision processes for patching, scanning, and containment). Methodologically, we leverage a modified supplementary-variables technique (SVT) that avoids Kolmogorov partial differential equations, improving tractability for transient analysis. We specify estimation pipelines (parametric, semi-parametric, and non-parametric), incorporate covariates (assets, controls, attacker class) via duration-dependent hazards and frailty, and derive renewal-reward expressions for long-run risk and cost. The result is a reproducible approach that strengthens cyber risk forecasting, reduces uncertainty in investment decisions, and quantifies efficiency frontiers for security operations — particularly relevant for small and mid-size enterprises and for emerging digital economies such as Georgia.

**Keywords:** semi-Markov process, cybersecurity analytics, dwell time, resilience, efficiency, hazard modeling, semi-Markov decision process, renewal reward, transient analysis

**რეზიუმე**

ნახევრად მარკოვის მოდელები (Semi-Markov Models, SMMs) ამცირებს კლასიკური უწყვეტი დროის მარკოვის ჯაჭვების „მეხსიერების არქონის“ დაშვებას და ზოგადი ყოფნის დროის (sojourn-time) განაწილებების გამოყენების საშუალებას იძლევა. კიბერუსაფრთხოების სფეროში, სადაც დარჩენის ხანგრძლივობა, გვერდითი გადაადგილების დრო და აღდგენის ფანჯრები იშვიათად ექვემდებარება

ექსპონენციურ განაწილებას, SMM ბუნებრივად აღწერს დროით დამოკიდებულებებსა და ჰეტეროგენულ ტემპებს. ნაშრომში შემუშავებულია SMM-ის ჩარჩო შემდეგი ამოცანებისთვის: (i) საფრთხის მდგომარეობის ამოცნობა (კომპრომისის სასიცოცხლო ციკლი), (ii) მდგრადობისა და ეფექტიანობის მეტრიკები (MTTD, MTTR, ხელმისაწვდომობა, დაცული საათის ღირებულება) და (iii) პოლიტიკის ოპტიმიზაცია (ნახევრად მარკოვის გადაწყვეტილების პროცესები განახლებისთვის, სკანირებისა და იზოლაციისთვის). მეთოდოლოგიურად გამოყენებულია მოდიფიცირებული დამატებითი ცვლადების ტექნიკა (SVT), რომელიც გამორიცხავს კოლმოგოროვის ნაწილობრივ დიფერენციალურ განტოლებებს და ზრდის გამოთვლით მოქნილობას გარდამავალი ანალიზისთვის. წარმოდგენილია შეფასების არხები (პარამეტრული, ნახევრად პარამეტრული და არაპარამეტრული), ვაერთიანებთ შემთხვევით სიდიდეებს (აქტივები, კონტროლები, თავდამსხმელის ტიპი) ხანგრძლივობაზე დამოკიდებული საფრთხეებისა და სისუსტის მეშვეობით, და ვღებულობთ განახლება-ანაზღაურების ფორმულებს გრძელვადიანი რისკისა და ხარჯის განსასაზღვრად. შედეგად მიღებულია გამეორებადი, პრაქტიკული მიდგომა, რომელიც აძლიერებს კიბერუსაფრთხოების რისკების პროგნოზირებას, ამცირებს გაურკვევლობას საინვესტიციო გადაწყვეტილებებში და უზრუნველყოფს ოპერაციული ეფექტიანობის საზღვრების რაოდენობრივ შეფასებას — განსაკუთრებით მნიშვნელოვანია მცირე და საშუალო საწარმოებისათვის და ისეთი განვითარებადი ციფრული ეკონომიკებისთვის, როგორიცაა საქართველო.

**საკვანძო სიტყვები:** ნახევრად მარკოვის პროცესი, კიბერუსაფრთხოების ანალიტიკა, ხანგრძლივობა, მდგრადობა, ეფექტიანობა, საფრთხის მოდელირება, ნახევრად მარკოვის გადაწყვეტილების პროცესი, განახლება-ანაზღაურება, გარდამავალი ანალიზი

## 1. Introduction

Cyber incidents evolve through stages—reconnaissance, intrusion, persistence, escalation, lateral movement, exfiltration, and recovery—whose **durations** vary across organizations,

attacker toolkits, and control postures. Classical Markov models assume exponential holding times and therefore constant hazards; empirical telemetry (e.g., dwell-time distributions, patching delays, containment windows) is typically **heavy-tailed** or multi-modal, violating memorylessness.

Semi-Markov models (SMMs) resolve this by specifying **transition probabilities** and **sojourn-time distributions** per edge of the state graph. This captures (i) persistence (long compromises), (ii) path-dependence (controls activated sooner reduce subsequent durations), and (iii) heterogeneity (assets, sectors, and attacker sophistication). We adapt SMMs to (a) model the **attack–defense dynamics** end-to-end, (b) quantify **resilience and efficiency** under realistic timing, and (c) optimize **policy timing** (inspection, patching, isolation) when action costs and benefits are duration-dependent.

## 2. Methodological Foundations

### 2.1 Semi-Markov kernel and embedded chain

Let $\{X(t), t \geq 0\}$be an SMM on state space $S = \{1, \dots, m\}$. When entering state $i$, the next state $j$is selected with probability $p_{ij}$(embedded Markov chain $P = [p_{ij}]$), and the sojourn time $T_{ij}$before transition $i \to j$has distribution $F_{ij}(t)$with density $f_{ij}(t)$and survivor $\bar{F}_{ij}(t)$. The semi-Markov kernel is

$$Q_{ij}(t) = p_{ij}F_{ij}(t), i \neq j.$$

Allow $F_{ij}$to be Weibull, log-normal, Pareto, phase-type, or non-parametric.

### 2.2 Transient probabilities via modified SVT

Let $p_k(t) = \Pr\{X(t) = k\}$. In standard treatments, transient analysis requires solving integral or partial differential equations. We adopt a **modified supplementary-variables technique (SVT)**—a partially probabilistic construction that augments the state with **elapsed time since entry** and exploits renewal decomposition to avoid Kolmogorov PDEs. Denote $\tau$the elapsed time in the current state. Conditional on $(X(t) = i, \tau)$, the residual life for transition $i \to j$has hazard

$$h_{ij}(\tau) = \frac{f_{ij}(\tau)}{\bar{F}_{ij}(\tau)}.$$

The total hazard out of $i$at age $\tau$is $h_i(\tau) = \sum_{j \neq i} p_{ij}\, h_{ij}(\tau)$. The modified SVT yields numerically stable recursions for $p_k(t)$based on **age-stratified** survival and jump probabilities, discretizing $\tau$or using quadrature, without PDEs. This is crucial for real-time SOC dashboards that must recompute risks quickly as age $\tau$increases.

### 2.3 Rewards, costs, and availability

Associate a cost (or reward) rate $c_i$to state $i$(e.g., loss per hour under "Active Compromise", operating cost under "Hunt Mode"). The renewal-reward theorem gives the long-run average cost

$$\bar{C} = \frac{\mathbb{E}\left[\sum_k c_{X_k}\, T_k\right]}{\mathbb{E}[\sum_k T_k]} = \frac{\sum_i \pi_i\ \mathbb{E}[T_i]\, c_i}{\sum_i \pi_i\ \mathbb{E}[T_i]},$$

where $\pi_i$is the stationary distribution of the embedded chain and $T_i$the generic sojourn in $i$(mixture over $j$). **Availability** of "Secure Operation" is

$$A = \frac{\mathbb{E}[\text{time in Secure}]}{\mathbb{E}[\text{cycle length}]} = \frac{\pi_{\text{Sec}}\ \mathbb{E}[T_{\text{Sec}}]}{\sum_i \pi_i\ \mathbb{E}[T_i]}.$$

## 3. Cybersecurity State Space and Timing

### 3.1 Threat–defense states

A compact yet expressive state space for enterprise environments:

1. **S** (Secure/Normal)
2. **L** (Latent Compromise / Persistence) – beaconing, dormant implants
3. **A** (Active Attack / Lateral Movement)
4. **D** (Detected / Containment Initiated)
5. **R** (Recovery / Eradication)
6. **H** (Hunt / Heightened Monitoring)

Directed edges encode feasible transitions (e.g., $S \to L$, $L \to A$, $A \to D$, $D \to R$, $R \to S$; recidivism $R \to L$possible). Each edge $i \to j$has $p_{ij}$and $F_{ij}$. Key cyber durations are **dwell time** (sojourn in $L$), **exploitation time** (in $A$), **MTTD** (sojourn until $D$), and **MTTR** (sojourn in $D$and $R$).

### 3.2 Duration dependence and heterogeneity

**Hazard increasing with age** ($h'(\tau) > 0$): longer lateral movement raises detection likelihood (more artifacts).

**Hazard decreasing with age** ($h'(\tau) < 0$): stealth implants become harder to detect as operators reduce activity.

**Covariate effects**: segment $F_{ij}(t \mid Z)$by asset criticality, EDR presence, patch latency, attacker class (commodity vs. targeted), and SOC staffing; model via accelerated failure time (AFT) or proportional hazards with frailty terms.

## 4. Estimation and Inference

### 4.1 Data sources

SIEM/SOAR timelines; EDR alerts; NDR beacons (times of first seen, detection, isolation).

Patch and vulnerability timelines (TTx: time-to-scan/patch/remediate).

Incident tickets (containment start/stop, recovery closure).

For unseen transitions (censoring), use interval-censoring constructs.

### 4.2 Fitting $P$and $F_{ij}$

**Embedded chain** $P$: multinomial MLE from observed next-states.

**Sojourn distributions** $F_{ij}$:

Parametric (Weibull/log-normal/Pareto): MLE with right/interval censoring.

Semi-parametric: Cox with time-varying covariates; baseline estimated non-parametrically.

Non-parametric: Kaplan-Meier / Turnbull estimators per transition class.

**Hidden states**: if latent $L$not directly observed, use EM with forward–backward recursions adapted to SMMs (using dwell-time likelihoods).

**Goodness-of-fit**: probability integral transform of dwell times; QQ plots; information criteria for distribution choice.

### 4.3 Transient risk and forecasting

Using the modified SVT, compute at time $t$with elapsed age $\tau$in state $i$:

$$\Pr\{X(t+\Delta) \in B \mid X(t) = i, \tau\} \approx \int_0^{\Delta} \sum_{j \in B} h_{ij}\,(\tau + s)\, S_i(\tau, \tau + s)\, ds,$$

with $S_i(\tau, \tau + s) = \exp(-\int_{\tau}^{\tau+s} h_i\,(u)\, du)$.

This yields **short-horizon breach risk** for SOC triage and **time-to-containment** distributions for staffing decisions.

## 5. Efficiency and Resilience Metrics

Let costs per hour: $c_S$(prevention/monitoring), $c_L$(exposure), $c_A$(active loss), $c_D$(containment operations), $c_R$(rebuild), $c_H$(hunt).

**Key metrics (renewal reward):**

**Average loss rate** $\bar{C}$ (see 2.3).

**Availability** $A$ of "Secure" or "At-least-Contained" states.

**MTTD** $= \mathbb{E}[T_{S \to D}]$under the SMM (time from clean to detection; passes through $L$and $A$with general durations).

**MTTR** $= \mathbb{E}[T_D + T_R]$.

**Cost per protected hour** $= \bar{C}/(A)$.

**Duration-elasticity of loss**: $\partial \bar{C} / \partial \mathbb{E}[T_{LA}]$quantifies the benefit of reducing lateral-movement time by one hour.

These metrics create an **efficiency frontier** comparing control portfolios (e.g., EDR+NDR+patch SLAs vs. EDR-only), with uncertainty bands from parametric bootstrap on $F_{ij}$.

## 6. Policy Optimization: Semi-Markov Decision Processes (SMDP)

### 6.1 Actions and timing

At state $i$and elapsed age $\tau$, choose action $a \in \mathcal{A}_i$ ={ intensify hunt, isolate host, patch now/defer, reimage, escalate IR }. An action can **modify hazards** $h_{ij}^{(a)}(\tau)$ and incur costs $k_i^{(a)}$(e.g., downtime, analyst time).

### 6.2 Objective

Minimize long-run average loss

$$g^* = \inf_{\pi} \limsup_{t\to\infty} \frac{1}{t}\, \mathbb{E}_{\pi}\left[\int_0^t c_{X(s)}^{(\pi)}\, ds + \sum \text{action costs}\right].$$

Age-dependent SMDP dynamic programming uses the **semi-Markov optimality equation**:

$$g^* + V(i,\tau) = \min_{a\in\mathcal{A}_i}\left\{c_i^{(a)}\, d\tau + \int_0^{\infty} \sum_j [\, V(j,0) + K_{ij}^{(a)}]\, dQ_{ij}^{(a)}(\tau + s)\right\},$$

with $Q_{ij}^{(a)}(\cdot)$the action-modified kernel and $K_{ij}^{(a)}$lumped action costs. Numerically, discretize $\tau$and solve by **relative value iteration** or **policy iteration**.

**Interpretation:** Optimal policies resemble **age-threshold rules** (e.g., "If elapsed time in L exceeds $\tau^{\star}$, force isolation") that trade disruption cost against expected loss from continued exposure.

## 7. Case Blueprint and Simulation

### 7.1 Data blueprint (SOC of a mid-size enterprise)

12 months of alert timelines (SIEM/EDR/NDR), incident tickets, patch SLAs.

Asset covariates: criticality tier, internet exposure, EDR coverage.

Outcomes: transitions observed/censored; durations for $S \to L$, $L \to A$, $A \to D$, $D \to R$.

### 7.2 Estimation and validation

1. Fit $P$and $F_{ij}$with covariates (AFT log-normal for $L \to A$; Weibull for $A \to D$).
2. Validate dwell-time fit (Cramér–von Mises; PIT histograms).
3. Compute $\bar{C}, A$,MTTD, MTTR (renewal reward).
4. Counterfactuals: reduce $E[T_{L\to A}]$by 20% (micro-segmentation), reduce $E[T_{A\to D}]$by 30% (NDR), compare $\Delta\bar{C}$.

5. SMDP: evaluate policies—continuous hunt vs. age-threshold isolation—report average loss and action burden.

### 7.3 Simulation

Use the fitted SMM to **generate synthetic incident streams**; stress-test under:

- Heavier-tailed dwell times (targeted actors).
- Surge scenarios (wormable CVE).
- Reduced SOC staffing (longer $A \to D$).

Measure degradation in $A$and growth in $\bar{C}$; identify **most cost-effective levers** (often reducing $A \to D$beats reducing $S \to L$in commodity threat environments).

## 8. Managerial and Policy Implications

**Duration-aware KPIs:** Replace single-number MTTD/MTTR with **age-conditioned hazards** and availability; align SLAs to **duration elasticities of loss**.

**Investment prioritization:** Fund controls with largest $\partial \bar{C} / \partial \mathbb{E}[T_{ij}]$(often detection and containment rather than prevention-only).

**Regulatory reporting:** SMM-based resilience metrics (availability, loss-rate) enable comparable, auditable disclosures.

**Emerging economies (e.g., Georgia):** SMMs accommodate irregular attack cycles and resource constraints; the modified SVT allows **computationally light** transient risk dashboards suitable for SMEs and public agencies.

## 9. Advantages, Limitations, and Extensions

**Advantages:** temporal realism; explicit duration dependence; actionable efficiency metrics; policy optimization with age thresholds; tractable transient analysis via modified SVT. **Limitations:** greater data needs; hidden states and censoring complicate inference; model risk if $F_{ij}$mis-specified.

**Extensions:**

**Hierarchical SMMs** for multi-site enterprises.

**Non-parametric Bayesian** dwell-time priors.

**Game-theoretic SMDPs** (attacker–defender).

**Coupled SMMs** for supply-chain propagation of cyber risk.

## 10. Conclusion

Semi-Markov models align naturally with cybersecurity's duration-driven dynamics. By replacing memoryless assumptions with empirically grounded sojourns, organizations can (i) forecast breach evolution more accurately, (ii) quantify resilience and efficiency through renewal-reward metrics, and (iii) optimize timing of actions via semi-Markov decision policies. The modified SVT enables practical transient analysis without PDEs, making SMMs usable in live SOC settings. For enterprises and national programs seeking **cost-effective cyber resilience**, SMMs provide a rigorous, decision-oriented toolkit.

## Appendix A: Minimal Implementation Steps (Practitioner Checklist)

1. **Define states** $S, L, A, D, R, H$; map telemetry to transitions.
2. **Estimate** embedded $P$and dwell-time $F_{ij}$(AFT/Weibull/log-normal; capture censoring).
3. **Validate** fits; compute hazards $h_{ij}(\tau)$.
4. **Compute** $\bar{C}, A$,MTTD, MTTR via renewal-reward; show uncertainty bands.
5. **Run counterfactuals** (reduce specific durations by control improvements).
6. **Optimize policy** with age-threshold SMDP; compare cost–loss trade-offs.
7. **Operationalize**: weekly re-estimation; dashboard transient risks with modified SVT.

## Appendix B: Notation

- $P = [p_{ij}]$: embedded transition matrix.
- $F_{ij}(t)$, $f_{ij}(t)$, $\bar{F}_{ij}(t)$: CDF, PDF, survivor for $i \to j$.
- $h_{ij}(\tau)$: transition-specific hazard; $h_i(\tau) = \sum_j p_{ij}\, h_{ij}(\tau)$.
- $c_i$: cost rate in state $i$; $\bar{C}$: long-run average cost; $A$: availability.

- $T_{ij}$: sojourn time for $i \to j$; $T_i$: mixture sojourn in $i$.

## References


1. Abate, Joseph, Gagan L. Choudhury, and Ward Whitt. 1994. "Waiting-Time Tail Probabilities in Queues with Long-Tail Service-Time Distributions." *Queueing Systems* 16 (3–4): 311–338. https://doi.org/10.1007/BF01158947.
2. Artalejo, Jesus R., and Antonio Gómez-Corral. 2008. *Retrial Queueing Systems: A Computational Approach.* New York: Springer.
3. Barbu, Vlad Stefan, and Nikolaos Limnios. 2008. *Semi-Markov Chains and Hidden Semi-Markov Models Toward Applications: Their Use in Reliability and DNA Analysis.* New York: Springer. https://doi.org/10.1007/978-0-387-73173-5.
4. Barbu, Vlad Stefan, Jan Bulla, and Nikolaos Limnios. 2012. "Discrete-Time Semi-Markov Models for Reliability and Survival Analysis." *Journal of Statistical Planning and Inference* 142 (5): 1230–1241. https://doi.org/10.1016/j.jspi.2011.11.012.
5. Béres, Ferenc, Imre Péntek, and Gábor Horváth. 2020. "Semi-Markov Decision Processes for Cybersecurity Incident Management." *Computers & Security* 94: 101819. https://doi.org/10.1016/j.cose.2020.101819.
6. Bulla, Jan, and Ines Bulla. 2006. "Stylized Facts of Financial Time Series and Hidden Semi-Markov Models." *Computational Statistics & Data Analysis* 51 (4): 2192–2209. https://doi.org/10.1016/j.csda.2006.07.020.
7. Cárdenas, Alvaro A., Saurabh Amin, and Shankar Sastry. 2008. "Research Challenges for the Security of Control Systems." In *Proceedings of the 3rd Conference on Hot Topics in Security (HotSec '08).* Berkeley, CA: USENIX Association.
8. Colbourn, Charles J., and Jeffrey H. Dinitz, eds. 2006. *Handbook of Combinatorial Designs.* 2nd ed. Boca Raton, FL: Chapman & Hall/CRC.
9. Dandekar, Anil, and Jay Patel. 2021. "Modeling Dwell Time Distributions in Cybersecurity Incident Detection Using Semi-Markov Processes." *IEEE Transactions on Information Forensics and Security* 16: 2150–2163. https://doi.org/10.1109/TIFS.2021.3054509.
10. Filar, Jerzy A., and Koos Vrieze. 1997. *Competitive Markov Decision Processes.* New York: Springer.
11. Ghosh, Souvik, Wei Liu, and Chen Zhang. 2022. "Cyber Resilience Assessment Using Stochastic Models: A Semi-Markov Decision Framework." *Reliability Engineering & System Safety* 221: 108322. https://doi.org/10.1016/j.ress.2022.108322.

12. Howard, Ronald A. 1971. *Dynamic Probabilistic Systems: Volume II—Markov Models.* New York: Wiley.
13. Iyer, Ravishankar K., and Kishor S. Trivedi. 1989. “Stochastic Models for Computer System Reliability and Performance.” In *Real-Time Systems and Applications,* edited by S. A. Smolka, 107–138. Berlin: Springer.
14. Kemeny, John G., and J. Laurie Snell. 1976. *Finite Markov Chains.* 2nd ed. New York: Springer-Verlag.
15. Kikalishvili, Levan, and Maia Kharadze. 2024. “A Modified Supplementary Variable Technique for Transient Analysis of Semi-Markov Models.” *Proceedings of the Georgian Academy of Sciences, Series A: Mathematical and Physical Sciences* 52 (2): 45–61. *(in press).*
16. Limnios, Nikolaos, and Gheorghe Oprisan. 2001. *Semi-Markov Processes and Reliability.* Boston: Birkhäuser. https://doi.org/10.1007/978-1-4612-0163-1.
17. Lye, Kian-Wah, and Jeannette M. Wing. 2005. “Game Strategies in Network Security.” *International Journal of Information Security* 4 (1–2): 71–86. https://doi.org/10.1007/s10207-004-0043-y.
18. Medina, Rodrigo, Antonio Jiménez, and Julio Pastor. 2020. “Modeling Cyber-Attack Propagation with Semi-Markov Processes.” *Computers & Security* 96: 101901. https://doi.org/10.1016/j.cose.2020.101901.
19. Miller, Rupert G. 2011. *Survival Analysis.* 2nd ed. Hoboken, NJ: Wiley.
20. Rausand, Marvin, and Arnljot Høyland. 2004. *System Reliability Theory: Models, Statistical Methods, and Applications.* 2nd ed. Hoboken, NJ: Wiley-Interscience.
21. Ross, Sheldon M. 2014. *Introduction to Probability Models.* 11th ed. San Diego: Academic Press.
22. Rubino, Gérard, and Bruno Tuffin, eds. 2009. *Rare Event Simulation Using Monte Carlo Methods.* Chichester: Wiley.
23. Shiryaev, Albert N. 1996. *Probability.* 2nd ed. New York: Springer.
24. Stefanov, Vesselin T. 2019. *Semi-Markov Processes and Applications to Stochastic Systems: Performance and Reliability.* Cham: Springer. https://doi.org/10.1007/978-3-030-17817-3.
25. Trivedi, Kishor S., and Andrea Bobbio. 2017. *Reliability and Availability Engineering: Modeling, Analysis, and Applications.* Cambridge: Cambridge University Press.
26. Vasicek, Oldrich. 1977. “An Equilibrium Characterization of the Term Structure.” *Journal of Financial Economics* 5 (2): 177–188.

27. Wooldridge, Jeffrey M. 2010. *Econometric Analysis of Cross Section and Panel Data.* 2nd ed. Cambridge, MA: MIT Press.
28. Zhang, Chen, Jie Chen, and Ness Shroff. 2021. "Semi-Markov Models for Adaptive Cyber Defense with Non-Exponential Intrusion Durations." *ACM Transactions on Privacy and Security* 24 (3): 1–28. https://doi.org/10.1145/3432345.
29. Zio, Enrico. 2016. "Reliability Engineering: Old Problems and New Challenges." *Reliability Engineering & System Safety* 152: 1–10. https://doi.org/10.1016/j.ress.2016.02.009.