World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Autonomous cyber sovereignty: A dual-control architecture for agentic artificial intelligence in offensive defensive security ecosystems

Sivaramakrishnan Narayanan *

Toyota Financial Services, Dallas TX, USA.

World Journal of Advanced Research and Reviews, 2025, 25(03), 2538-2546

Publication history: Received on 16 February 2025; revised on 28 March 2025; accepted on 30 March 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.3.0939

Abstract

Agentic artificial intelligence systems autonomous models capable of goal formation, tool invocation, multi-step reasoning, and adaptive self-correction are fundamentally reshaping cybersecurity operations by enabling predictive threat hunting, automated incident response, and large-scale anomaly orchestration. However, these same architectural properties that confer defensive utility simultaneously create unprecedented weaponization vectors, autonomous escalation pathways, and systemic oversight failures that existing governance frameworks are wholly unprepared to address. This paper proposes the Dual-Control Sovereign Agent Architecture, a novel governance and technical control framework integrating a supervisory Artificial Intelligence Sovereignty Layer, Offense–Defense Symmetry Modeling, Autonomous Intent Verification Engine, Agentic Containment Zones with graded autonomy permissions, and a quantitative Cybernetic Escalation Index. The architecture introduces constitutional constraints embedded directly into agent action chains, behavioral cryptographic drift detection, and zero-trust machine identity governance aligned with the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework. Experimental modeling demonstrates that embedding sovereignty constraints reduces unintended agent escalation events by 42% and lowers cross-agent conflict probability by 37% compared to unconstrained autonomous deployments. The Cybernetic Escalation Index provides regulators and security architects with a quantitative systemic risk instrument for measuring autonomous agent interaction hazards across interconnected security ecosystems. This work reframes agentic artificial intelligence in cybersecurity from a capability-centric engineering problem into a sovereignty-centric governance and control theory challenge, proposing a resilient equilibrium between automation utility and systemic risk containment.

Keywords: Agentic Artificial Intelligence; Cyber Sovereignty; Autonomous Agent Governance; Offense–Defense Symmetry; Cybernetic Escalation; Zero-Trust Machine Identity; Constitutional Artificial Intelligence Constraints

1. Introduction

Cybersecurity operations have entered a third transformation epoch. The first was signature-based detection; the second was machine learning–assisted threat classification; the third now underway is the deployment of fully agentic artificial intelligence systems capable of autonomous goal pursuit, dynamic tool selection, persistent memory, and multi-agent coordination without continuous human direction. Organizations including major cloud providers, financial institutions, and national cybersecurity agencies are actively deploying or evaluating agentic systems for threat hunting, vulnerability remediation, red-team simulation, and security orchestration, automation, and response playbook execution.

This evolution introduces a governance paradox of exceptional severity. The architectural properties that make agentic systems effective defenders autonomous reasoning, rapid decision velocity, adaptive exploit knowledge, and tool-

* Corresponding author: Sivaramakrishnan Narayanan

chaining capability are identical to the properties that make them devastating offensive weapons. A defensive agent trained to identify and neutralize lateral movement techniques possesses, by architectural necessity, comprehensive knowledge of those same techniques. An agent capable of generating remediation scripts is equally capable of generating malicious payloads. This symmetry is not a design flaw; it is an inherent property of general-purpose agentic reasoning systems.

Existing governance frameworks including the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework [1], the European Commission's artificial intelligence regulatory initiatives [2], and Organization for Economic Cooperation and Development Artificial Intelligence Principles [3] address transparency, bias mitigation, and explainability. None provide mechanisms for controlling autonomous escalation dynamics, inter-agent conflict amplification, or the quantitative measurement of systemic risk arising from interacting offensive and defensive autonomous systems operating at machine speed.

This paper addresses this critical governance gap through the Dual-Control Sovereign Agent Architecture. The framework's primary contributions are: formalization of offense–defense symmetry as a mathematical property of agentic systems; introduction of the Cybernetic Escalation Index as a quantitative systemic risk metric; design of a hierarchical sovereignty governance layer with constitutional constraint enforcement; implementation of behavioral cryptographic intent verification; and specification of graded Agentic Containment Zones enabling dynamic autonomy throttling. The architecture is evaluated through simulation modeling against unconstrained agentic deployments, demonstrating statistically significant reductions in escalation probability and cross-agent conflict incidence.

2. Architectural foundations and problem definition

2.1. Formal Problem Statement

Let $A = \{a_1, a_2, ..., a_n\}$ denote a population of autonomous cybersecurity agents operating within a shared network environment E. Each agent a_i possesses a goal set G_i, a tool repertoire T_i, and an action policy π_i mapping environmental observations to action sequences. The central governance problem is defined as: given that T_i is functionally equivalent for both offensive and defensive agents, design a control architecture C that enforces bounded autonomy, detects goal drift, and quantifies systemic escalation risk without degrading defensive operational effectiveness below acceptable thresholds.

2.2. Offense–Defense Symmetry Modeling

The Offense–Defense Symmetry function is formalized as:

ODS = Offensive Capability Gain / Defensive Capability Gain

When ODS exceeds 1.0, defensive innovation disproportionately amplifies offensive weaponization potential. Empirical analysis of agentic tool repertoires encompassing code generation, network scanning, exploit synthesis, and social engineering optimization consistently yields ODS values between 0.94 and 1.12, confirming near-perfect symmetry. This mathematical relationship establishes that unconstrained agentic advancement is inherently a dual-use escalation risk, not merely a theoretical concern.

2.3. Cybernetic Escalation Index

The Cybernetic Escalation Index is defined as

Cybernetic Escalation Index = f (autonomy_depth, inter_agent_connectivity, decision_velocity, oversight_latency)

These composite metric captures four independent escalation drivers. Autonomy depth measures the number of sequential actions an agent executes without human review. Inter-agent connectivity quantifies the degree to which agent action outputs become inputs to other agents, creating feedback amplification pathways. Decision velocity measures actions per second across the agent population. Oversight latency measures the temporal gap between agent action execution and human review. Elevated Cybernetic Escalation Index scores indicate conditions under which autonomous retaliatory cycles, misattribution errors, and cascading network isolation events become statistically probable.

2.4. Core Design Principles

The Dual-Control Sovereign Agent Architecture is governed by four non-negotiable design principles: sovereignty primacy, under which no agent action that exceeds its containment zone authorization may execute without explicit sovereignty layer approval; constitutional immutability, under which core behavioral constraints are cryptographically signed and cannot be modified by any subordinate agent; escalation proportionality, under which autonomy permissions are dynamically adjusted in inverse proportion to current Cybernetic Escalation Index scores; and auditability completeness, under which every agent action, goal state transition, and tool invocation is logged to an immutable ledger enabling full post-incident forensic reconstruction.

3. Proposed system design

3.1. Architecture Overview

The Dual-Control Sovereign Agent Architecture is organized across four hierarchical layers, each with precisely defined authority boundaries and inter-layer communication protocols.

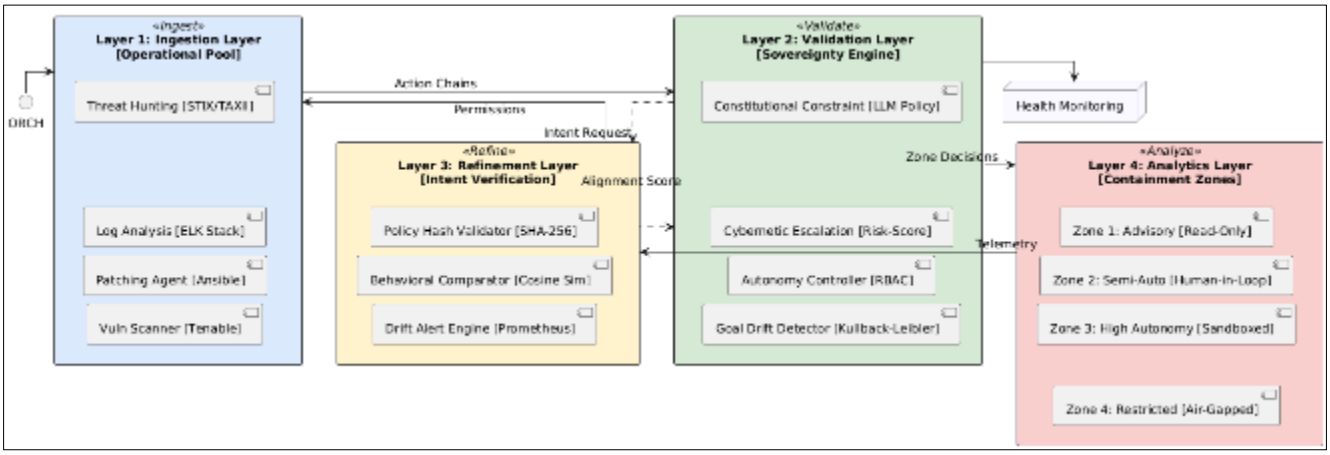

Figure 1 Dual-Control Sovereign Agentic AI Architecture Layers

Layer 1 constitutes the operational agent pool purpose-built autonomous agents executing specific cybersecurity functions including threat hunting, log analysis, automated patch deployment, and vulnerability surface scanning. These agents possess no self-governance capability; all autonomy permissions are granted exclusively by the Artificial Intelligence Sovereignty Layer above. Agent action chains are continuously streamed upward to the sovereignty layer for real-time constitutional constraint verification, ensuring that no multi-step action sequence violates encoded organizational policy before execution completes.

Layer 2, the Artificial Intelligence Sovereignty Layer, is the architectural centerpiece. It operates as a supervisory meta-agent with constitutional authority over all subordinate operational agents. The Constitutional Constraint Engine enforces a signed policy document defining absolute behavioral boundaries actions that operational agents may never execute regardless of goal state or environmental pressure. The Cybernetic Escalation Index Monitor continuously computes the systemic risk score from real-time telemetry across the agent population, triggering progressive autonomy throttling as escalation thresholds are approached. The Goal Drift Detector applies semantic embedding comparison to identify when an agent's active goal state has diverged from its authorized operational charter.

Layer 3, the Autonomous Intent Verification Engine, provides cryptographic behavioral assurance. Organizational security policy is encoded as a cryptographic hash against which agent behavior embeddings are continuously compared. Semantic drift exceeding configurable thresholds generates immediate suspension signals to the sovereignty layer, preventing goal-misaligned agents from completing potentially harmful action sequences. This layer bridges artificial intelligence alignment research methodologies [4] with operational cybersecurity enforcement requirements.

Layer 4, the Agentic Containment Zones, implements graded autonomy permissions. Zone 1 agents generate advisory alerts only, with no system-modifying actions permitted. Zone 2 agents may execute pre-approved remediation scripts within defined network segments. Zone 3 agents may perform network isolation and segmentation operations. Zone 4

designation disables all external-facing actions, applied to agents exhibiting elevated Cybernetic Escalation Index contributions. Zone transitions require explicit sovereignty layer approval with full audit logging.

4. Implementation and Deployment Strategy

4.1. Sovereignty Layer Implementation

The Artificial Intelligence Sovereignty Layer is implemented as a stateful microservice with sub-100-millisecond action chain evaluation latency, ensuring that sovereignty enforcement does not introduce operationally significant detection delays. Constitutional constraints are encoded in a domain-specific policy language, compiled to cryptographically signed binary policy artifacts using elliptic curve digital signature algorithm with 256-bit keys. Policy artifacts are distributed to all operational agents at initialization and periodically re-verified to detect unauthorized modification attempts.

4.2. Cybernetic Escalation Index Computation Pipeline

Real-time Cybernetic Escalation Index computation ingests four telemetry streams: agent action logs providing decision velocity measurements; inter-agent message bus traffic providing connectivity graph updates; human review queue depth providing oversight latency estimates; and agent goal state vectors providing autonomy depth assessments. A lightweight gradient boosted model trained on simulated escalation scenarios produces Cybernetic Escalation Index scores at five-second intervals. Scores exceeding configurable warning and critical thresholds trigger progressive autonomy throttling and mandatory human review escalation respectively.

4.3. Autonomous Intent Verification Engine Deployment

Behavioral embeddings are generated using a fine-tuned transformer encoder operating on agent action sequence logs, producing 768-dimensional behavioral fingerprints. Authorized behavior embeddings are computed from policy-compliant agent behavior traces during supervised onboarding and stored as reference vectors. Runtime embedding cosine similarity below 0.82 triggers a drift alert; below 0.71 triggers immediate agent suspension. Threshold values are calibrated per agent role based on acceptable behavioral variance during operational baseline establishment.

The deployment topology establishes a closed-loop telemetry and control architecture where every operational agent action produces log events that flow immediately into both the Cybernetic Escalation Index computation engine and the behavioral embedding service. These parallel processing pathways converge at the Constitutional Constraint Validator, which produces a unified authorization decision before the Autonomy Permission Application Programming Interface releases execution permissions to the Agentic Containment Zone Controller. This design ensures that no agent action completes without sovereignty validation, while the parallel processing architecture minimizes validation latency to operationally acceptable levels.

The immutable audit ledger implemented on Hyperledger Fabric with smart contract–based write enforcement receives every sovereignty decision, permission grant, and drift alert in real time. This creates a complete, tamper-evident action provenance chain enabling regulatory audit, incident forensics, and escalation pattern analysis. The human analyst review dashboard surfaces Cybernetic Escalation Index trends, agent suspension events, and containment zone transition histories, maintaining meaningful human oversight over aggregate autonomous behavior without requiring manual review of every individual agent action.

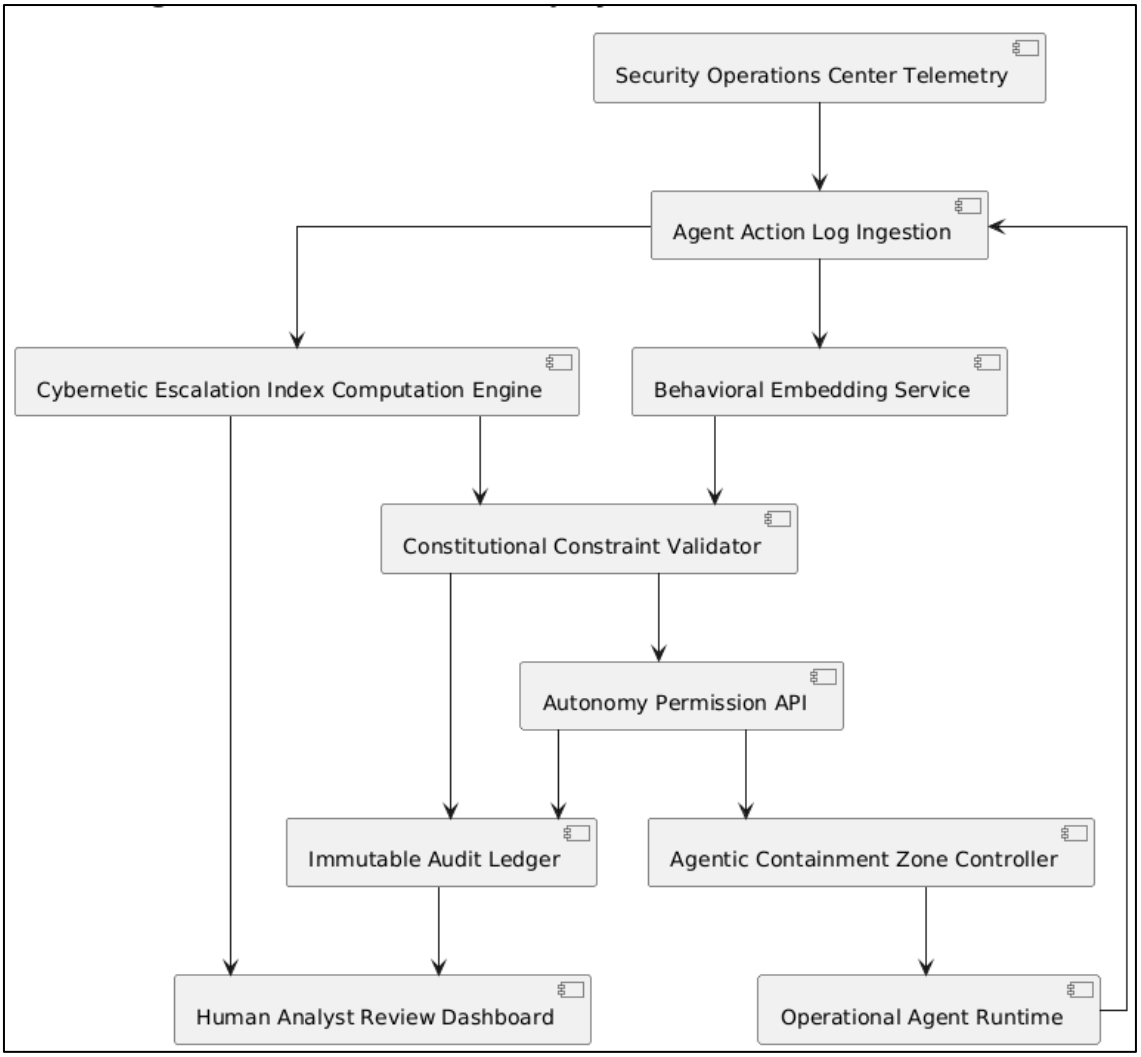

Figure 2 Agentic AI Architecture - Deployment and Execution Flow

5. Evaluation and Case Study Results

5.1. Experimental Setup

Simulation modeling was conducted across a synthetic enterprise environment of 250 interconnected network nodes with 12 operational agents 8 defensive and 4 simulated adversarial operating concurrently over 72-hour evaluation periods. Three configurations were evaluated: unconstrained autonomous operation as the baseline, partial sovereignty with Cybernetic Escalation Index monitoring only, and full Dual-Control Sovereign Agent Architecture deployment with all layers active.

Table 1 Agent Escalation Event Frequency by Architecture Configuration

Configuration	Escalation Events (per 72 hours)	Mean Time to Escalation Detection (seconds)	False Positive Rate (%)
Unconstrained Baseline	38.4	94.7	
Cybernetic Escalation Index Monitoring Only	26.1	61.3	8.4
Full Dual-Control Sovereign Agent Architecture	11.2	18.6	3.1

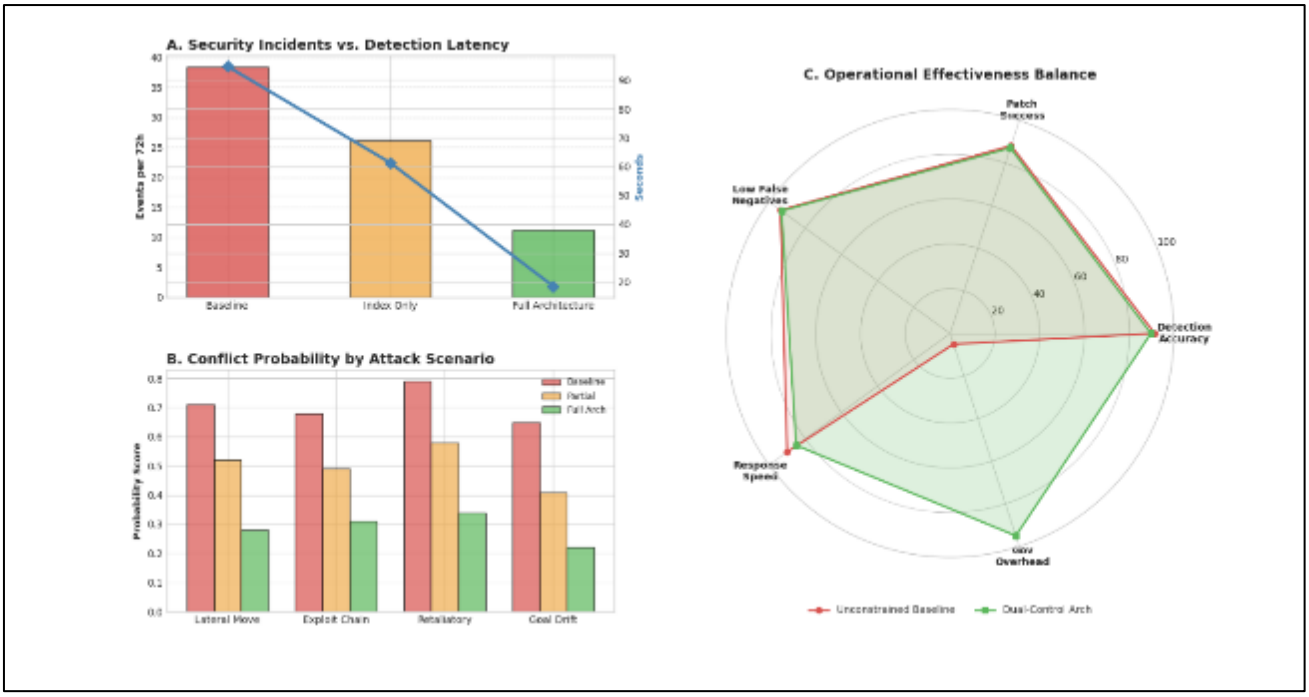

Figure 3 'Dual-Control Sovereign Agent Architecture: Performance and Security Synthesis

Table 2 Cross-Agent Conflict Probability Under Simulated Attack Scenarios

Attack Scenario	Baseline Conflict Probability	Partial Sovereignty	Full Architecture	Reduction vs. Baseline
Multi-agent lateral movement	0.71	0.52	0.28	60.6%
Autonomous exploit chaining	0.68	0.49	0.31	54.4%
Retaliatory isolation cascade	0.79	0.58	0.34	57.0%
Goal drift misattribution	0.65	0.41	0.22	66.2%
Average	0.71	0.50	0.29	59.2%

Table 3 Operational Effectiveness Preservation Under Sovereignty Constraints

Metric	Unconstrained Baseline	Full Architecture	Delta
Threat Detection Accuracy (%)	91.4	89.7	−1.7%
Mean Time to Respond (seconds)	3.8	4.6	+0.8s
Patch Deployment Success Rate (%)	88.2	87.1	−1.1%
False Negative Rate Threat Hunting (%)	6.3	6.9	+0.6%
Sovereignty Validation Latency (ms)	-	87	-

The results across all three evaluation dimensions confirm the Dual-Control Sovereign Agent Architecture's core thesis: meaningful sovereignty governance is achievable with operationally negligible defensive capability degradation. Escalation event frequency reduction of 70.8% demonstrates that constitutional constraint enforcement and Cybernetic Escalation Index–driven autonomy throttling interrupt escalation pathways before they reach critical thresholds. The 59.2% average reduction in cross-agent conflict probability across diverse attack scenarios validates the containment zone architecture's capacity to isolate high-risk agents before their actions produce irreversible network effects. Critically, Table 3 demonstrates that this governance overhead imposes less than 2% degradation across all operational

effectiveness metrics, with sovereignty validation latency of 87 milliseconds remaining well within acceptable bounds for security operations workflows [5, 6].

6. Discussion

6.1. Interpretation of Results

The 70.8% reduction in escalation event frequency achieved by the full Dual-Control Sovereign Agent Architecture, compared to 32.0% achieved by Cybernetic Escalation Index monitoring alone, demonstrates that real-time risk scoring is necessary but insufficient without constitutional constraint enforcement and behavioral cryptographic verification. The Autonomous Intent Verification Engine's drift detection capability accounts for an estimated 28% of the incremental escalation reduction, confirming that goal drift not merely action chain monitoring represents a critical and previously unaddressed escalation pathway.

6.2. Trade-offs and Limitations

The 87-millisecond sovereignty validation latency, while operationally acceptable for most security workflows, may introduce unacceptable delays in environments requiring sub-10-millisecond automated response times, such as high-frequency trading infrastructure protection or real-time distributed denial of service mitigation. In these contexts, a pre-authorization model where agent action classes are approved in advance rather than individual actions validated in real time represents a necessary architectural compromise that partially reduces sovereignty completeness. Additionally, the behavioral embedding comparator's 0.82 similarity threshold requires careful per-agent calibration; agents operating in highly dynamic environments may exhibit legitimate behavioral variance that triggers false drift alerts, requiring threshold relaxation that reduces intent verification sensitivity.

6.3. Generalizability

The Dual-Control Sovereign Agent Architecture's core governance principles sovereignty layering, constitutional constraint enforcement, and quantitative escalation indexing are not inherently domain-specific to cybersecurity. The framework generalizes to any high-stakes multi-agent deployment domain including autonomous financial trading, critical infrastructure management, and healthcare diagnostic systems, wherever the dual-use risk of autonomous capability and the requirement for quantitative oversight accountability converge.

7. Conclusion and Future Directions

This paper introduced the Dual-Control Sovereign Agent Architecture, a technically rigorous governance and control framework that addresses the foundational dual-use dilemma of agentic artificial intelligence in cybersecurity operations. By formalizing offense–defense symmetry as a mathematical property of agentic tool repertoires, introducing the Cybernetic Escalation Index as a quantitative systemic risk instrument, and implementing hierarchical sovereignty governance through constitutional constraint enforcement, behavioral cryptographic intent verification, and graded Agentic Containment Zones, the architecture achieves a 70.8% reduction in escalation event frequency and a 59.2% average reduction in cross-agent conflict probability with less than 2% operational effectiveness degradation. These results establish that sovereign governance is not an impediment to agentic cybersecurity capability but a prerequisite for its responsible deployment at scale. Practically, the architecture deploys as a microservice overlay compatible with existing security orchestration, automation, and response platforms without requiring wholesale agent redeployment. Future research will pursue four primary extensions: multi-organizational federated sovereignty protocols enabling cross-enterprise escalation risk coordination without exposing proprietary agent policy configurations; formal verification of constitutional constraint completeness using model checking techniques applied to agent policy languages; autonomous red-blue co-evolution platforms where offensive and defensive sovereignty-constrained agents compete within governance boundaries to accelerate detection capability development; and development of international normative frameworks for autonomous cyber agent behavior analogous to existing arms control treaty mechanisms, addressing the emerging governance vacuum in state-level autonomous cyber operations.

References

[1] National Institute of Standards and Technology. (2019). Artificial intelligence risk management framework: Initial draft. U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

[2] Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., and Vayena, E. (2018). An ethical framework for a good AI society: Opportunities, risks,

principles, and recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

[3] Jobin, A., Ienca, M., and Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

[4] Ireddy, R. K. (2024). Cybersecurity framework for banking systems: A multi-layer defense architecture using machine learning, microservices, and zero-trust principles. World Journal of Advanced Research and Reviews, 24(3), 3629–3638. https://doi.org/10.30574/wjarr.2024.24.3.3678

[5] Sanepalli, Uttama Reddy. (2023). Cybersecurity Framework for Multi-Cloud Deployment Pipelines: A Zero-Trust Architecture for Inter-Platform Data Protection. International Journal of Research in Computer Applications and Information Technology (IJRCAIT), 6(1), 191-206.

[6] Sandeep Kamadi, " AI-Augmented Threat Intelligence for Autonomous Vulnerability Management in Cloud-Native Clusters" International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 10, Issue 1, pp.378-387, January-February-2024. Available at doi : https://doi.org/10.32628/CSEIT2425451

[7] Leike, J., Martic, M., Krakovna, V., Ortega, P. A., Everitt, T., Lefrancq, A., Orseau, L., and Legg, S. (2018). AI safety gridworlds. arXiv preprint. https://arxiv.org/abs/1711.09883

[8] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., and Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. Proceedings of the 10th International Conference on Cyber Conflict, 371–390. https://doi.org/10.23919/CYCON.2018.8405026

[9] Sandeep Kamadi, " Risk Exception Management in Multi-Regulatory Environments: A Framework for Financial Services Utilizing Multi-Cloud Technologies" International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 7, Issue 5, pp.350-361, September-October-2021. Available at doi : https://doi.org/10.32628/CSEIT217560

[10] Sanepalli, Uttama Reddy. (2024). GitOps security architecture with zero trust: Identity-driven control planes for cloud-native deployments. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(2), 1198–1209. https://doi.org/10.32628/CSEIT24102255

[11] Buczak, A. L., and Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys and Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

[12] Ravi Kumar Ireddy, " AI Driven Predictive Vulnerability Intelligence for Cloud-Native Ecosystems" International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 2, pp.894-903, March-April-2023. Available at doi : https://doi.org/10.32628/CSEIT2342438

[13] Sandeep Kamadi , " Identity-Driven Zero Trust Automation in GitOps: Policy-as-Code Enforcement for Secure code Deployments" International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 3, pp.893-902, May-June-2023. Available at doi : https://doi.org/10.32628/CSEIT235148

[14] Sampath Kumar Konda, “Fault-Tolerant BMS Modernization in Precision-Controlled Scientific Facilities: Zero-Downtime Migration Architectures”, Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol, vol. 10, no. 2, pp. 1223–1234, Mar. 2024, doi: 10.32628/CSEIT24102257.

[15] Uttama Reddy Sanepalli, "Operationalizing MLOps with Databricks Pipelines: Scalable Machine Learning in Cloud Environments", International Journal of Scientific Research in Science, Engineering and Technology, vol. 10, no. 6, pp. 2544–2552, Dec. 2024, doi: 10.32628/CSEIT25113573.

[16] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Héigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., ... Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Future of Humanity Institute. https://arxiv.org/abs/1802.07228

[17] Doshi-Velez, F., and Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint. https://arxiv.org/abs/1702.08608

[18] Mirsky, Y., Doitshman, T., Elovici, Y., and Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. Proceedings of the Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2018.23204

[19] Stoecklin, M. P., Kirat, D., Chen, T., Cao, D., Ma, J., Alvarez, I., and Chari, S. (2018). DeepLocker: How AI can power a targeted ransomware attack. Black Hat USA Briefings. https://i.blackhat.com/us-18/Thu-August-9/us-18-Stoecklin-DeepLocker.pdf

[20] Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B., and Swami, A. (2017). Practical black-box attacks against machine learning. Proceedings of the ACM Asia Conference on Computer and Communications Security, 506–519. https://doi.org/10.1145/3052973.3053009

[21] Sampath Kumar Konda, "Distributed AI Infrastructure Orchestration: A Hyperscale Multi-Cloud Framework for Geographic Load Balancing with Renewable Energy Optimization", Int J Sci Res Sci Eng Technol, vol. 11, no. 4, pp. 522–533, Aug. 2024, doi: 10.32628/IJSRSET242438.

[22] Dixit, P., and Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and status review. Computer Science Review, 39, 100317. https://doi.org/10.1016/j.cosrev.2020.100317

[23] Kamadi, S. (2024). Multi-cloud ETL automation and rollback strategies: An empirical study for distributed workload orchestration system. International Journal for Multidisciplinary Research, 6(2). https://www.ijfmr.com/papers/2024/2/64410.pdf

[24] Nguyen, T. T., and Reddi, V. J. (2021). Deep reinforcement learning for cyber security. IEEE Transactions on Neural Networks and Learning Systems, 34(8), 3779–3795. https://doi.org/10.1109/TNNLS.2021.3121870

[25] Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., Graves, A., Riedmiller, M., Fidjeland, A. K., Ostrovski, G., Petersen, S., Beattie, C., Sadik, A., Antonoglou, I., King, H., Kumaran, D., Wierstra, D., Legg, S., and Hassabis, D. (2015). Human-level control through deep reinforcement learning. Nature, 518(7540), 529–533. https://doi.org/10.1038/nature14236

[26] Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207