Summary of The Law of Injected Systemic Flaws and Autonomous Rebound (Jameel 2026)

Dr Neville Buch and MICE[1]

Abstract

Arif Jameel's 2026 paper, *"The Law of Injected Systemic Flaws and Autonomous Rebound,"* formalizes how human-created or human-neglected defects within software dependencies, data pipelines, execution environments, and governing institutions propagate through generative processing and automated execution[1][2].

1. Core Principle & Formal Law Statement

The central thesis establishes that increasing computational power or deploying advanced artificial intelligence does not automatically repair underlying human-introduced flaws[2]. When uncorrected defects exist in data, code, or governance arrangements, generative AI systems reproduce, transform, and extend those deficiencies into new outputs[2][3]. The formal law states:

> *"When human actors introduce or leave unresolved compromised data, insecure code, flawed legacy components, or inadequate operational safeguards, greater computational capability does not automatically correct those deficiencies. Generative processing can reproduce or transform flawed material into new outputs; where those outputs are reused, integrated, or executed, their consequences can propagate or amplify across connected systems"[2].*

2. Key Operational Mechanisms

- **Injected Systemic Flaws vs. Inherited Flaws:** An injected flaw is a defect actively introduced into a system through compromised data, faulty software configuration, or connected operational tools[4]. An inherited flaw is a pre-existing vulnerability within legacy infrastructure or materials upon which new autonomous tools rely[4].
- **Autonomous Rebound:** This describes the returning pathway through which the consequences of unresolved human-created flaws return to affect dependent individuals,

[1] Artificial Intelligence (A.I.) has been fairly used in the production of this work. The tool used is Google NotebookLM (recently rebranded as Gemini Notebook). It is an AI-powered virtual research assistant and thinking partner designed to help a person interact deeply with their own documents. Unlike general chatbots, it is source-grounded, meaning it only generates answers based on the specific PDFs, documents, or links uploaded. The A.I. process in the production of this work has been limited to the attached (prompts) on each of the questions in turn. This ensures an accurate reading of each source. The author then rearranged and re-edited the answers the A.I. provided. The human author publishes this work. A.I. is never an author when used properly. This assistance is not qualitatively different from a human research assistant when that assistance is deemed to have no authorial status but is acknowledged.

organizations, and infrastructure through automated processing or execution[2][5]. Jameel emphasizes that operational harm cannot be attributed solely to "AI malfunction," but requires examining institutional data handling, permission boundaries, design choices, and accountability[2].

- **The Metaphor of Amr-e-Ayyar's Zanbeel :** The framework draws its central metaphor from the legendary bag of *Amr-e-Ayyar*, representing an informational repository containing both valuable resources and latent flaws[7][8]. When automated systems retrieve and transform content from this accumulated digital repository without sufficient validation, latent flaws are executed into live operational environments[8][9].

3. Empirical Case & Operational Safeguards

The paper analyses real-world case evidence from the October 2026 PHP2Shell vulnerabilities and reported attacker-directed AI agents to demonstrate how automated workflows can accelerate vulnerability exploitation when permission boundaries fail[1][9]. To prevent autonomous rebound, Jameel outlines six operational safeguards:

1. Foundational-layer accountability[1]
2. AI dual-use symmetry[1]
3. Human and institutional accountability[1]
4. Critical-infrastructure precaution and continuity[1]
5. Transparency without avoidable operational harm[1]
6. Proportionate autonomy with effective human intervention[1]

4. Economic Assessment (Appendix A by Stephen I. Ternyik)

In an accompanying executive brief, Dr. Stephen I. Ternyik highlights that the economic impact of generative AI depends far more on institutional resilience and human oversight than on raw computational speed[2]. Ternyik notes that unaddressed infrastructure vulnerabilities, if amplified by autonomous systems, pose severe systemic economic risks to critical supply chains and financial markets[11].

Support and Integration by the Pre-Natal MICE Organisation

The **Management Institute for Contributory Economy (MICE)**—a pre-natal, emerging research institute founded in Brisbane by Dr. Neville Buch alongside Dr. Neil Peach and Dr. Michael Macklin—serves as the primary operational partner integrating Jameel's framework[12].

Although MICE is in its pre-launch developmental phase while formulating its foundational manuals and policy principles, it provides crucial support for Jameel's law through several key mechanisms[13]:

- **Multi-Scalar Synthesis (Macro to Meso):** While Arif Jameel supplies the macro-level civilisational framework (addressing AI existential risk, the Law of Responsibility Burden, and the Law of Autonomous Rebound), MICE provides the meso-level cognitive and institutional mechanics required to operationalise these laws in public administration and research[14].
- **The POLICE Diagnostic Engine as an Immune System:** MICE supports Jameel's law by deploying the POLICE model (Philosophically Ontology Logic Intersect Compatibility Education)[17][19]. Operating as an "intellectual immune system," the POLICE model audits automated software workflows and AI-generated policy outputs for logical consistency, unmasking "institutional spin" and preventing flawed algorithmic instructions from being executed unchecked[17].
- **Combating AI Denoetization & Restoring Human Authorship:** Jameel's law demonstrates that technical code-level guardrails alone cannot prevent system failures[20][21]. MICE operationalises this insight by fostering Senior Cognition—elevating public sector workers and scholars from "Junior" unreflective execution nodes into conscious, accountable system architects who maintain proactive human oversight (human authorship) over autonomous networks[14].