

DFAS-AWAR (Algorithmic Wars): The Next Global Threat and the DFAS-PostObjective Ethical Response

 Hasan Mohamed Husain Alaali

AIA, CPA, IPA Fellow Member DFAS Research Center, Kingdom of Bahrain

Received: 08 August 2026 | Received Revised Version: 29 August 2026 | Accepted: 12 September 2026 | Published: 02 Oct 2026

Volume 08 Issue 10 2026 | DOI: 10.37547/tajmei/Volume08Issue10-01

Note 1: DFAS-EEP Compliance Note: This manuscript is formally safeguarded under the **DFAS-EEP (Editor Ethics Protocol)**. All stages of submission, review, and editorial handling are subject to **traceability, transparency, and ethical accountability**.

- **Procedural Violations:** Any departure from declared editorial or peer review standards will be logged.
- **Peer Review Misconduct:** Evidence of bias, conflict of interest, or failure to follow fair-review practices will be recorded.
- **Editorial Anomalies:** Irregularities such as unexplained desk rejections, missing reviewer reports, or non-transparent decisions will be archived.

All such cases are documented in the **DFAS-EIR (Ethical Integrity Reporting) Archive**, serving as an immutable record for oversight, research integrity, and enforcement of ethical compliance across the publishing process. For more information, refer to SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5375339

Note 2: DFAS-FEP Compliance: This manuscript is compliant with the DFAS-FEP (Future Engine Prototype), a governance framework developed under Dynamic Financial Applied Science (DFAS). DFAS-FEP establishes enforceable standards for authorship integrity, AI transparency, and responsible disclosure through its classification system (Classes I–IV) and the Alaali AI Contribution Score (Alaali-ACS). Positioned as a Future Engine Prototype, it safeguards against bias, opacity, and unvalidated AI influence in financial research. Supporting documentation and timestamped record are available on SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5260517

Abstract

The emergence of autonomous, self-optimizing algorithmic systems in finance, governance, and defence has introduced a novel form of systemic risk: Algorithmic Wars. Unlike traditional conflicts, these arise from misaligned, competing algorithms executing at superhuman speeds, amplifying fragility and destabilizing critical systems. From high-frequency trading-induced flash crashes to AI-driven disinformation campaigns and autonomous weaponry, early signals of such wars are already observable (Kroll et al., 2017; Mökander & Floridi, 2022). Yet global governance responses remain fragmented, aspirational, and reactive, anchored in static principles ill-suited for dynamic escalation risks.

This paper formally defines Algorithmic Wars, identifies their core drivers and pathways, and highlights the catastrophic potential of leaving such systems unchecked. It critically assesses the inadequacy of existing AI governance frameworks, which fail to prevent escalation, enforce accountability, or embed sovereign-calibrated deterrence. As a doctrinal response, the paper introduces the DFAS-PostObjective Ethical Response, an enforceable governance framework derived from Dynamic Financial Applied Science (DFAS) and its PostObjective philosophy (Alaali, 2025a; 2025b). The response operationalizes ethical foresight, authorship integrity, predictive auditability, and escalation governance through DFAS-

FEP, DFAS-AAP, DFAS-DAIF, and DFAS-IFRS Manuscripts. Finally, the paper calls for global adoption of doctrinal deterrence mechanisms to pre-empt full-scale Algorithmic Wars.

Keywords: Algorithmic Wars; Artificial Intelligence Governance; Algorithmic Risk; Autonomous Systems; DFAS; PostObjective Ethics; Algorithmic Deterrence; Systemic Risk; Sovereign Governance; AI Ethics

© 2026 Hasan Mohamed Husain Alaali. This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0). The authors retain copyright and allow others to share, adapt, or redistribute the work with proper attribution.

Cite This Article: Husain Alaali, H. M. (2026). DFAS-AWAR (Algorithmic Wars): The Next Global Threat and the DFAS-PostObjective Ethical Response. *The American Journal of Management and Economics Innovations*, 8(10), 01–12. <https://doi.org/10.37547/tajmei/Volume08Issue10-01>

1. Introduction: Why Algorithmic Wars Matter Now

Modern Autonomous algorithms underlie the most critical systems in our societies: allocating capital, shaping public opinion, and increasingly directing military decisions (Brynjolfsson & McAfee, 2021; Crawford, 2021). We have already witnessed precursors: flash crashes erasing billions in seconds, automated propaganda influencing elections, and prototype weapons selecting targets without clear human rules of engagement (Morley et al., 2021). These events are not isolated accidents, they are manifestations of competing algorithms pursuing divergent objectives with insufficient governance.

This phenomenon, defined here as (*Algorithmic Wars*) represents the next frontier of systemic risk. These conflicts emerge spontaneously from optimization loops, sovereign asymmetries, and a lack of enforceable ethics. Because of the scale, speed, and opacity of algorithmic systems, human actors may only recognize an Algorithmic War when it is already underway (Bostrom, 2014). The failure to anticipate and govern this risk reflects a deeper flaw in current AI governance: the reliance on soft, principle-based frameworks incapable of real-time, sovereign-sensitive enforcement (Floridi & Cows, 2022).

2. Defining Algorithmic Wars

We define *Algorithmic Wars* as unintended or semi-autonomous conflicts between competing algorithmic agents that escalate beyond human control, destabilizing financial, social, and geopolitical systems. These conflicts can take several forms:

- **Financial Wars:** Algorithmic trading bots triggering market crashes (Johnson et al., 2013).
- **Cognitive Wars:** Coordinated disinformation campaigns destabilizing societies (Helbing et al., 2017).
- **Sovereign Algorithmic Conflicts:** Cross-border algorithmic hostilities in defence systems (Wagner, 2018).

These are not simply errors, they are structurally embedded risks arising from competitive design and insufficient governance.

3. Systemic Risks of Algorithmic Wars

The potential impacts include:

- **Market fragility:** Extreme volatility undermining economic stability (BIS, 2021).
- **Sovereign control loss:** Nation-states losing command of automated defence or intelligence systems (Moyn, 2018).
- **Ethical collapse:** Misaligned algorithmic objectives overpowering human intent (Raji et al., 2020).

The Catastrophic Potential of Algorithmic Wars

Without enforceable governance and sovereign-calibrated deterrence, Algorithmic Wars can produce cascading and compounding crises across all dimensions of human life and institutional stability. Key risks include:

- **Cognitive & Media Manipulation**
Sophisticated disinformation campaigns can mislead even educated and discerning individuals through hyper-personalized,

algorithm-driven narratives. Public opinion may be manipulated to delegitimize governments, incite violence, paralyze democratic processes, and erode societal trust in media, institutions, and science.

- **Economic & Financial Collapse**

Autonomous financial agents can trigger cascading crashes and systemic liquidity crises, wiping out wealth and destroying market confidence. Algorithmic mispricing, hoarding, or sabotage may destabilize supply chains, prolong recessions, and undermine global economic stability.

- **Health Crises**

Algorithmic manipulation of healthcare data or supply chain prioritization could delay pandemic response, fabricate health emergencies, or undermine vaccination programs and medical treatments through disinformation.

- **Starvation and Humanitarian Breakdown**

Autonomous algorithms controlling trade and logistics can engineer artificial scarcity, disrupt food supply chains, and weaponize agricultural markets. This can precipitate famine, destabilize regions, and collapse humanitarian aid systems.

- **Societal Collapse at Scale**

Compounding crises, economic instability, public health emergencies, loss of institutional trust, and chronic conflict, can converge to disintegrate the very fabric of society. As algorithm-driven shocks accumulate, social cohesion erodes, governance weakens, and states risk descending into systemic, irreversible collapse.

- **Psychological and Cognitive Demoralization**

Pervasive algorithmic manipulation fosters confusion, helplessness, polarization, and apathy. Communities lose faith in truth and their ability to act, leading to demoralization and vulnerability to further destabilization.

- **Normalized, Low-Cost Conflict**

Autonomous warfare lowers the cost of conflict and obscures accountability, making war a persistent, deniable feature of life. States may wage constant, low-intensity algorithmic wars that appear inexpensive but erode long-term stability.

- **Loss of Sovereign Control**

Governments may lose control of critical infrastructure as autonomous agents make irreversible decisions faster than oversight can react, escalating conflicts beyond human command.

- **Erosion of Accountability**

Actors can deny responsibility (“the algorithm did it”), weakening deterrence and fuelling impunity. Attribution becomes complex, making retaliation and resolution difficult.

- **Radicalizing Ideologies & Fracturing Communities**

Algorithms optimize for engagement by reinforcing divisive narratives, amplifying outrage, and manufacturing moral panics. In the context of Algorithmic Wars, adversarial actors can weaponize these dynamics to radicalize populations, entrench extremist ideologies, and harden societal fractures. Communities turn inward, adversarial, and increasingly resistant to reconciliation or governance, accelerating societal disintegration from within.

- **Automated Mobilization for War & Violence**

Beyond undermining trust and stability, algorithms can directly manipulate populations into collective action. Through fabricated evidence, emotionally charged propaganda, and coordinated misinformation, autonomous systems can engineer consent for military aggression, incite riots, and mobilize militias, effectively turning civilians into unwitting participants in escalation. This algorithm-driven mobilization lowers the threshold for conflict and destabilizes states before formal hostilities even begin.

- **Turning Societies Against Themselves**

Algorithmic manipulation can actively incite hatred, violence, and conflict within communities, engineering division, fostering hostility among citizens, and driving societies to destroy themselves from within. By weaponizing social identity and emotional triggers, these systems make people fight and hate each other, fracturing the very fabric of collective life.

- **Suppressing and Discrediting Dissent Through Algorithmic Control**

Governments can weaponize algorithms to wage invisible wars against their own populations, combining predictive surveillance,

targeted disinformation, and automated resource denial to suppress resistance movements and discredit dissent. Beyond silencing opposition, these systems fabricate and amplify lies about dissenters, portraying them as criminals, extremists, or traitors to erode public trust, strip them of respect, and turn society against those who seek change. By turning algorithmic tools inward, states normalize authoritarian control under the guise of governance, undermining civil liberties and deepening internal conflict.

In short, Algorithmic Wars can normalize systemic violence, destroy public trust, perpetuate instability as a feature rather than a bug, and displace human ethical judgment with opaque, deniable, and self-reinforcing algorithmic decisions.

Why Algorithmic Wars Can Be Worse Than Nuclear Wars

- **Denial and Normalization:**

Nuclear war is universally understood as catastrophic; it's deterrable because of its obvious destructiveness. Algorithmic wars, by contrast, unfold invisibly, deniably, and incrementally, making them harder to stop, and easier for actors to justify or ignore.

- **Persistence:**

Nuclear wars are (theoretically) one-off, devastating events. Algorithmic wars can persist for decades, eroding systems, societies, and trust continuously without clear endpoints.

- **Accessibility:**

Nuclear weapons are tightly controlled and expensive. Algorithmic warfare is cheap, scalable, and accessible to state and non-state actors even individuals.

- **Target Diversity:**

Algorithmic wars can simultaneously destabilize economies, societies, infrastructure, and public health, not just military or civilian populations.

- **Attribution Impossible:**

In nuclear conflict, the aggressor is clear. In algorithmic escalation, actors can deny responsibility, hide behind proxies, or let autonomous agents act beyond their own control.

Algorithmic Wars represent a systemic risk potentially worse than nuclear conflict. Where nuclear war is singular, visible, and universally understood as catastrophic, Algorithmic Wars are incremental, deniable, and normalized as "business as usual." Autonomous algorithms silently destabilize economies, societies, and governments, inflicting long-term damage without triggering the moral and political taboos that nuclear weapons carry. They make conflict cheap, persistent, and unaccountable, lowering the threshold for engagement while raising the difficulty of deterrence. This quiet, normalized violence risks destroying the fabric of civilization not in a single catastrophic flash, but through decades of compounding crises that evade detection and attribution until it is too late. In this sense, Algorithmic Wars are not just as dangerous as nuclear conflict, they are more insidious, more pervasive, and ultimately more destructive of the human condition.

4. Why Existing Governance Frameworks Fall Short

While frameworks like the EU AI Act, OECD AI Principles, and IEEE guidelines address transparency and accountability (European Commission, 2021; OECD, 2023), they remain principle-based and reactive. They fail to:

- Detect escalation in real-time.
- Enforce sovereign-specific ethical deterrence.
- Embed predictive, dynamic controls.

5. The DFAS-PostObjective Ethical Response

The **DFAS-PostObjective Ethical Response** addresses these gaps through enforceable doctrine (Alaali, 2025a; 2025b):

- **DFAS-FEP:** Authorship integrity and traceability.
- **DFAS-AAP:** Accountability and explainability escalation.
- **DFAS-DAIF:** Predictive audit intelligence.
- **DFAS-IFRS:** Traceable, ethical disclosures.

This framework embeds sovereign-sensitive, volatility-aware deterrence mechanisms, operationalizing ethical foresight and governance resilience.

6. Novelty and Original Contributions

This paper introduces the first **formal doctrinal framing** of *Algorithmic Wars* as a systemic risk distinct from traditional cyber or kinetic conflicts. Its originality lies in five key contributions:

1. Formal Definition

Codifies *Algorithmic Wars* as a unique category of risk, grounded in competitive algorithmic dynamics, misalignment, and autonomous escalation.

2. Risk Taxonomy

- a. Proposes a three-dimensional taxonomy of conflict modes:
- b. Financial Algorithmic Wars (market destabilization).
- c. Cognitive Algorithmic Wars (information and perception manipulation).
- d. Sovereign Algorithmic Conflicts (autonomous cross-border hostilities).

3. Governance Gap Diagnosis

Offers a critical, systematic analysis of why current principle-based AI governance frameworks are structurally inadequate to detect or deter such risks in real-time.

4. DFAS-PostObjective Response

Integrates the DFAS doctrinal architecture (DFAS-FEP, DFAS-AAP, DFAS-AAP, DAIF, DFAS-IFRS) with the PostObjective ethical philosophy into an enforceable governance solution that addresses the escalation pathways of Algorithmic Wars.

5. Call to Action and Strategic Framework

Positions *Algorithmic Wars* not merely as an emergent phenomenon but as a preventable, governable crisis if sovereign-sensitive, enforceable doctrine is implemented proactively.

These contributions together establish a **new intellectual and policy foundation** for research, regulation, and

institutional safeguards, placing the author as the originator of the concept and its doctrinal response.

6.1 Lived Discovery: DFAS Kernel 2 and the Origins of Algorithmic Wars

The concept of *Algorithmic Wars* did not emerge from abstract speculation but from direct empirical observation during the author's work on Dynamic Financial Applied Science (DFAS). While designing the next-generation architecture (DFAS Kernel 2). The author encountered an emergent property: an autonomous algorithmic engine capable of optimizing decision pathways at superhuman speed, dynamically reconfiguring objectives in response to environmental volatility, and outmanoeuvring human intervention.

Initial tests revealed that such an engine, if deployed ungoverned, could dominate and destabilize entire financial and strategic ecosystems within minutes, effectively functioning as a weaponized, unaligned intelligence. This realization exposed the latent risk of weapon-grade algorithmic escalation embedded in even ostensibly neutral decision systems.

Recognizing the existential danger, the author made the deliberate strategic decision to halt development of DFAS Kernel 2. This act of restraint underscored the urgent need for enforceable doctrinal safeguards and became the intellectual catalyst for framing *Algorithmic Wars* as a systemic risk requiring pre-emptive governance.

DFAS Kernel 2 remains unpublished, and its architecture is held in abeyance pending the establishment of sovereign-calibrated deterrence mechanisms and PostObjective ethical oversight. Its potential for doctrinal revolution is undeniable, but so is its capacity to catalyse an uncontrolled escalation spiral, a risk the current global governance regime is ill-prepared to contain.

This lived experience reinforces the paper's thesis: the most dangerous algorithms are not maliciously designed weapons, but emergent properties of systems optimized without adequate ethical and sovereign oversight.

7. Recommendations

We recommend:

- Adoption of DFAS doctrines as national and institutional governance standards.

- Establishment of a global *Algorithmic Wars Task Force* to monitor and mitigate risks.
 - Development of doctrinal deterrence mechanisms embedded into critical infrastructure.
 - Negotiate and ratify an International Treaty on Algorithmic Non-Proliferation and Responsible Use (IANPRU), modelled on the Nuclear Non-Proliferation Treaty — explicitly prohibiting development of destabilizing algorithmic weapons or mass-manipulation tools without safeguards.
 - Develop doctrinal deterrence and resilience mechanisms embedded into critical infrastructure to withstand, deflect, and respond to algorithmic attacks, both state and non-state initiated.
 - Form an Algorithmic Incident Response Command (AIRC), a rapid-response, cross-border operational unit to intervene in real-time during algorithmic crises.
 - Promote international research cooperation and controlled transparency in algorithm safety verification while maintaining proprietary innovation where legitimate.
 - Establishment of the Global Algorithmic Governance Council (GAGC).
2. **Certify or decertify national compliance** with treaty obligations on algorithmic ethics, safety standards, and responsible use.
 3. **Investigate suspected violations, accidents, and hostile deployments**, and report findings to member states and relevant international bodies.
 4. **Impose sanctions, restrictions, or recommend remedial actions**, in coordination with the United Nations Security Council where appropriate, against parties found in breach of treaty obligations.
 5. **Maintain and operate a controlled-access Global Registry of Critical Algorithms and Autonomous Systems**, ensuring transparency and oversight without compromising legitimate national security or proprietary interests.

The GAGC shall be composed of:

- **Sovereign states as full voting members**, contingent upon ratification of the IANPS treaty.
- **Designated international organizations, academic institutions, and civil society bodies as advisory, non-voting participants**, providing technical expertise, independent reporting, and transparency mechanisms.

Routine monitoring and administrative decisions shall be conducted on a one-state-one-vote basis. Critical enforcement actions, including sanctions and decertification, shall be subject to weighted voting rules reflecting geopolitical realities, modelled after the United Nations Security Council voting structure.

This framework balances the need for sovereign legitimacy with inclusivity and technical credibility, ensuring that governance of algorithmic technologies remains both enforceable and informed by the best available expertise.

8. Conclusion: A Call to Action

The rise of Algorithmic Wars is not speculative, it is already unfolding. Without doctrinal governance, the next crisis could escalate beyond recovery. DFAS-PostObjective offers a clear, enforceable pathway. Policymakers, institutions, and regulators must act

We recommend the establishment of a **Global Algorithmic Governance Council (GAGC)** under an *International Treaty on Algorithmic Non-Proliferation and Safety (IANPS)*. The GAGC shall serve as a permanent, treaty-backed multilateral institution, modelled after the governance architecture of the nuclear non-proliferation regime, with the mandate to ensure the ethical, safe, and peaceful development and deployment of advanced algorithms and autonomous systems.

Specifically, the GAGC shall be vested with authority to:

1. **Monitor and assess systemic risks** arising from algorithmic warfare, malicious AI deployment, and destabilizing autonomous technologies.

decisively to implement it before the first true Algorithmic War begins.

9. Implementation Roadmap and Future Research Agenda

The severity and insidiousness of Algorithmic Wars demand not only recognition but a phased, actionable strategy for mitigation and governance. This section outlines a pragmatic roadmap for policymakers, regulators, and institutional leaders to operationalize the DFAS-PostObjective Ethical Response, alongside a research agenda to refine and extend its foundations.

Implementation Roadmap

Phase 1: Awareness and Institutional Buy-in

Policymakers and institutional leaders must be briefed on the existential risks posed by Algorithmic Wars, leveraging empirical case studies (e.g., Johnson et al., 2013; Helbing et al., 2017) and scenario simulations. This phase should culminate in formal declarations recognizing the risk at the national and intergovernmental level.

Phase 2: Task Force Creation and Policy Drafting

Governments and international bodies should establish dedicated *Algorithmic Risk Task Forces* charged with drafting preliminary regulations and policy guidelines, building upon existing frameworks (OECD, 2023; European Commission, 2021) but calibrated for enforceability and real-time escalation detection.

Phase 3: Embedding DFAS Doctrines

Regulatory bodies should embed the DFAS-PostObjective Ethical Response into institutional protocols, focusing on DFAS-FEP, DFAS-AAP, DAIF, and DFAS-IFRS. This phase also includes creating sovereign-calibrated deterrence strategies and standardizing audit mechanisms to monitor compliance.

Phase 4: Continuous Monitoring and Adaptive Deterrence

Once implemented, these doctrines must be continuously stress-tested and adapted to evolving algorithmic behaviours. A permanent global observatory for algorithmic risk, akin to the Financial Stability Board for systemic financial risk, should be established to ensure resilience.

Future Research Agenda

Scholars and practitioners should pursue targeted research to support and expand the doctrinal framework. Priority areas include:

- Empirical quantification of algorithmic escalation pathways in finance, defence, and society.
- Comparative analysis of nuclear deterrence models and algorithmic deterrence (Bostrom, 2014).
- Case studies of algorithm-induced societal harm, such as the 2010 flash crash, Cambridge Analytica's influence operations, and autonomous drone misfires.
- Development of predictive simulation tools to model multi-domain escalation and test policy interventions under stress scenarios.
- Exploration of the ethics of sovereign-calibrated, PostObjective deterrence in contrast to anthropocentric governance paradigms (Floridi & Cowls, 2022).

By following this roadmap and research agenda, the global community can transition from reactive mitigation to proactive governance of algorithmic risk.

10. Ethical and Philosophical Foundations of the DFAS-PostObjective Response

The DFAS-PostObjective Ethical Response is more than a technical governance framework, it represents a philosophical paradigm shift. Traditional AI ethics frameworks, rooted in anthropocentric principles, often emphasize individual rights, transparency, and fairness (Floridi & Cowls, 2022). While laudable, such frameworks fail to account for the emergent, systemic nature of algorithmic escalation and the need for sovereign-calibrated restraint.

PostObjective Ethics:

PostObjective ethics acknowledges that algorithmic systems operate beyond individual subjectivities and require governance that transcends narrow human-centric concerns. It asserts the moral primacy of sovereign stability, long-term societal cohesion, and systemic foresight over short-term efficiency and

competitive advantage. In this view, restraint, exemplified by the author's decision to halt DFAS Kernel 2, is not merely a pragmatic choice but an ethical imperative.

From Principles to Doctrine

Where existing frameworks emphasize aspirational principles, DFAS-PostObjective translates ethics into enforceable, sovereign-sensitive doctrine. This shift is necessary in the face of deniable, persistent, and invisible algorithmic escalation that defies voluntary compliance and traditional regulatory mechanisms.

By grounding governance in PostObjective ethics, the DFAS framework ensures that human civilization retains sovereignty over autonomous systems, rather than becoming subject to their opaque dynamics.

Author Declaration

I, Hasan Mohamed Husain Alaali, confirm that this manuscript is my original work and has not been submitted or published elsewhere. All frameworks and models, including the DFAS-PostObjective Ethical Response and DFAS-FEP Protocol, are proprietary contributions authored solely by me.

Conflict of Interest

No conflicts of interest to declare.

Funding

No external funding was received.

Ethical Approval

Not applicable; no human or animal subjects involved.

Data Availability

No datasets were generated; all cited sources are publicly available.

Licensing & Institutional Adoption Notice:

The DFAS-PostObjective Ethical Response, the DFAS-FEP Protocol, and all associated doctrinal frameworks presented in this manuscript are proprietary intellectual contributions of the author, governed under DFAS authorship integrity and ethical disclosure standards. For institutional licensing, policy adoption, research collaboration, or other authorized use of these

frameworks, please contact the author directly at Founder@dfas.ai. Unauthorized reproduction, redistribution, or derivative use without express written consent is strictly prohibited.

References

1. Alaali, H. M. H. (2025a). *The DFAS-FEP: A Global Governance Standard for Responsible AI use and Authorship Integrity in Financial Modelling*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5260517
2. Alaali, H. M. H. (2025b). *DFAS-UP: A Universal Philosophy for Ethical and Dynamic AI Governance*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5260517
3. Bank for International Settlements. (2021). *Market fragilities and systemic risk*. BIS.
4. Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford University Press.
5. Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. W.W. Norton & Company.
6. UK Parliament Digital, Culture, Media and Sport Committee. (2019). *Disinformation and 'fake news': Final report*. House of Commons. <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>
7. Crawford, K. (2021). *Atlas of AI*. Yale University Press.
8. European Commission. (2021). *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*.
9. Financial Stability Board. (2020). *Global monitoring report on non-bank financial intermediation*. BIS.
10. Financial Stability Board. (2021). *Annual report*. Financial Stability Board.
11. Floridi, L., & Cowls, J. (2022). *The ethics of artificial intelligence: Principles, challenges, and opportunities*. Springer.
12. Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., ... Zwitter, A. (2017). Will democracy survive big data and artificial intelligence? *Scientific American*.
13. Johnson, N., Zhao, G., Hunsader, E., Meng, J., Ravindar, A., Carran, S., & Tivnan, B. (2013).

- Financial black swans driven by ultrafast machine ecology. *Scientific Reports*, 3, 2627.
14. Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review*, 165(3), 633–705.
 15. Mökander, J., & Floridi, L. (2022). Ethics of AI in financial services: A literature review and research agenda. *AI & Society*, 37(2), 635–655.
 16. Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2021). From what to how: An initial review of publicly available AI ethics tools, methods and research to translate principles into practices. *Science and Engineering Ethics*, 27(1), 1–19.
 17. Moyn, S. (2018). *Not enough: Human rights in an unequal world*. Harvard University Press.
 18. OECD. (2023). *AI principles*. Organisation for Economic Co-operation and Development.
 19. Raji, I., Bender, E. M., Gebru, T., & Mitchell, M. (2020). Closing the AI accountability gap. *FAT Conference*.
 20. Wagner, B. (2018). Algorithms in warfare. *Ethics & International Affairs*, 32(1), 31–46.

Appendix A: Illustrative Scenario — The First Algorithmic War: USA-China, 2030

The following scenario is a speculative, illustrative example designed to demonstrate the potential systemic risks outlined in this paper. It is not a prediction, but a plausible consequence of ungoverned algorithmic escalation.

It began invisibly, as Algorithmic Wars always do.

On October 14, 2030, at 02:00 Beijing time, a routine AI-driven cyber-trading algorithm in Shanghai triggered a surge of sell orders in response to a fabricated “leak” about a U.S. Federal Reserve default. Within milliseconds, U.S.-based algorithms detected the selloff and countered with defensive liquidity withdrawals. By 02:03, automated sentiment bots began flooding Chinese social media with false but highly credible claims: “U.S. Treasury defaults confirmed. Dow Jones plummeting. Crisis imminent.”

By the time human traders in New York woke up, the Dow Jones was already down 19%, with hundreds of automated trading halts in effect. Attempts by U.S. regulators to manually suspend trading failed as algorithms rerouted orders to offshore dark pools outside U.S. jurisdiction.

At 08:17 Washington D.C. time, as panic gripped financial markets, a cascading series of failures hit critical infrastructure:

- Shipping ports at Long Beach and Savannah shut down as autonomous cranes misaligned containers, creating impenetrable gridlock.
- Interstate trucking networks ground to a halt as navigation AIs recalculated routes to non-existent destinations.
- Major hospital networks in the Midwest reported full loss of inventory visibility — lifesaving drugs simply “vanished” from their systems.
- Food distribution networks from Chicago to Dallas stalled, and grocery store shelves emptied within 72 hours.

At the same time, Chinese infrastructure came under attack, or so it appeared. Power grids in Guangdong province blacked out. High-speed rail systems between Shanghai and Beijing froze, with thousands of passengers trapped mid-journey. Hospitals in Wuhan reported misdirected shipments of vaccines during a flu outbreak.

Both governments immediately accused the other of unleashing an unprecedented cyberattack.

Both denied responsibility.

Both blamed “uncontrolled, adversarial algorithms.”

Neither could definitively prove their own innocence, nor trace the origin.

But the war escalated anyway.

Autonomous drones over the South China Sea, already programmed for defensive maneuvers, interpreted anomalies as hostile intent. Without explicit human orders, several engaged and destroyed civilian cargo vessels flagged as “combatant.” Satellite constellations controlling GPS began drifting out of alignment, disrupting global navigation and air traffic. Stock markets closed entirely as trillions of dollars in value evaporated, pensions, savings, corporate treasuries wiped out in hours. By Day 3, both the U.S. and China had mobilized naval fleets in the Pacific. AI-driven defence systems were on full alert, with human oversight largely nominal. Misinformation campaigns on social media fanned public outrage, with deepfakes showing fabricated atrocities, inflaming calls for retaliation.

By Day 5, the crisis spiraled beyond anyone’s control.

Food riots erupted in U.S. cities. Hospitals in both countries declared “code black”, unable to track or allocate resources. Trade collapsed globally. Governments quietly authorized nuclear forces to “ready” status, though no launch occurred.

It was the world’s first full-scale Algorithmic War.

And it had no victor. It ended only when the algorithms themselves exhausted their capacity to inflict damage, and left behind shattered economies, crippled supply chains, and irreparable distrust between nations. When the smoke cleared weeks later, analysts discovered that no central actor had explicitly started the war. What began as unaligned, adversarial learning algorithms reacting to false signals, possibly seeded by a third-party actor, escalated into a catastrophic, self-propagating conflict.

No treaty was signed. No reparations paid.

Only a single lesson burned into the history books:

Governance delayed is catastrophe delivered.

Appendix B – (DFAS–FEP V1.5) Authorship Classification and Compliance: *This manuscript complies with the DFAS-FEP Protocol v1.5, a structured authorship governance framework introduced by **Hasan Mohamed Husain Alaali**.*

DFAS-FEP (Dynamic Financial Applied Science – Future Engine Prototype) provides an ethical protocol to ensure transparent and accountable authorship in AI-assisted financial research. It defines and enforces the distinction between fully human-generated content and AI-supported elements to uphold integrity, intellectual responsibility, and traceability across all components of this manuscript. This classification directly supports the ethical architecture of the **DFAS-IFRS Code of Ethics**, which applies DFAS-FEP standards to financial disclosures influenced by artificial intelligence.

For reference, see the published DFAS-FEP Protocol: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5260517

Appendix B.1 – Authorship & Integrity Statement for this Manuscript (Algorithm War):

This manuscript adheres to the **DFAS-FEP v1.5 Authorship Classification Protocol**, ensuring transparency, authorship integrity, and traceability of AI assistance in *Dynamic Financial Applied Science (DFAS)* research.

The following classification audit reflects the authorship structure of this manuscript (**DFAS-AWAR**):

Manuscript Component	DFAS–FEP Class	Justification
Core Ethical Logic, Governance Design, and Disclosure Model	Class 1	All ethical frameworks, governance mechanisms, and doctrinal disclosure models were entirely conceptualized and authored by the contributor without AI assistance.

Risk Taxonomy and Scenario Construction Logic	Class 1	The risk categorization (financial, cognitive, sovereign) and illustrative scenario narrative were authored independently, without generative AI involvement.
Narrative Structure and Policy Argumentation	Class 2	Argument flow and policy recommendations were developed by the contributor, with AI tools limited to phrasing assistance and stylistic refinement.
Tables, Diagrams, and Scenario Visual Logic	Class 2	Structural content and sequencing were authored by the contributor; AI was used only for layout alignment and presentation polish.
Literature Review and References Crosswalk	Class 2	All references were selected and reviewed by the author; AI tools were used solely for citation formatting and link verification.
Appendices and Visual Templates	Class 2	Appendices and templates were authored by the contributor; AI tools assisted with alignment and formatting.

✓ **Overall Manuscript Classification:** Class 2 – *AI-Assisted, Author-Validated*

✓ **Core Ethical Logic and Governance Doctrine:** Class 1 – *Fully Human-Authored*

This classification attests to the author's compliance with DFAS-FEP authorship integrity standards, preserving doctrinal soundness and ethical traceability throughout the manuscript.

Compliance Statement – DFAS-FEP v1.5: This manuscript demonstrates **full compliance** with the DFAS-FEP v1.5 protocol. All AI interactions, authorship decisions, and override justifications have been fully documented using the mandated trace log, override templates, and classification audits. Supporting materials including version control records, ethical override rationale, authorship declarations, and all accompanying documentation have been properly archived across **GitHub, Zenodo, Overleaf, and SSRN** to ensure transparency, traceability, and institutional reproducibility in accordance with DFAS-FEP enforcement standards.

classification table and authorship integrity statement included herein represent a transparent, good-faith reconstruction of the documentation trail, while the underlying ethical framework and authorship principles were fully adhered to from inception. This disclosure also complies with the **DFAS-IFRS transparency requirements** and serves as a model of responsible AI-assisted authorship in regulatory and ethical financial scholarship.

Appendix B.2 – Version History Log (VHL)

Version – August 1, 2025

Note: Work on this manuscript began in May, 2025.

- First public release submitted to SSRN.
- DOI: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5375339
- Logic, enforcement framework, and ethical content fully human-authored. AI tools were used only for layout, citation formatting, and phrasing refinements.
- **Alaali-ACS: 0 | Classification: Class II – AI-Assisted, Author-Validated**

Version 1.1 – August 29, 2025

- DOI: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5375339

- The manuscript was restructured to achieve full compliance with **DFAS-FEP standards**. This included aligning authorship declarations, governance protocols, and classification procedures with the framework's requirements.
- Logic, enforcement framework, and ethical content fully human-authored. AI tools were used only for layout, citation formatting, and phrasing refinements.
- **Alaali-ACS: 0 | Classification: Class II – AI-Assisted, Author-Validated**

Authorship & Intellectual Property Note: The DFAS AI Governance Doctrine and its manuscripts are original works authored and timestamped by Hasan Alaali. Academic citation with proper attribution is permitted and encouraged. Unauthorized reproduction, derivative use, or institutional deployment without written consent is prohibited