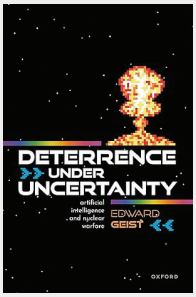
Deterrence under Uncertainty:
Artificial Intelligence and Nuclear Warfare

By Edward Geist
Oxford University Press, 2023, 271 pages, £83.00, ISBN: 9780192886323

Reviewed by Çise Karadeniz, İstanbul University

DOI: 10.25253/99.2025272.23



Once based on the bilateral symmetry of the Cold War, the logic of deterrence now faces layered ambiguity, cognitive manipulation, and pervasive uncertainty as the international system transforms into a multipolar and multi-domain order with overlapping spheres of technological, strategic, and normative contestation. The fundamental tenets of nuclear deterrence are under pressure in accordance with this new reality, in which cyber and artificial intelligence (AI) technologies are speeding up, improving the accuracy, and expanding the scope of conflict.

Edward Geist's *Deterrence under Uncertainty* critically investigates the long-standing belief that emerging technologies, particularly AI and advanced surveillance systems, can "lift the fog of war" and make deterrence strategies more precise and stable (p. 70). He examines how new technologies are changing long-held beliefs about deterrence, decision-making, and strategic stability by fusing conceptual analysis with actual military situations.

Geist's methodology combines theoretical models, historical case studies, and hypothetical situations to create a novel language of deterrence. He prefers mapping epistemic hazards and strategic unknowns over predictive modeling. His method demonstrates an intellectual heritage shaped by Clausewitzian fog and friction, Thomas Schelling's strategic dilemmas, and more modern developments in cybernetics and information theory.

The book consists of six chapters, which are followed by a conclusion, methodically examining how underlying epistemological and strategic limitations frequently cause technological solutions to deterrence problems to fall short. Geist's criticism centers on the persistent military ideal of "splendid situational awareness," which holds that it may be feasible to completely understand the battlefield and eradicate strategic uncertainty with the use of cutting-edge information and communication technologies (p. 2). He demonstrates in Chapter 2, "No Place to Hide?" that this perspective is not novel. From the Semi-Automatic Ground Environment (SAGE) system in the 1950s to the Gulf War's legacy of imagined "dominant battlespace knowledge," the urge to see and understand everything has repeatedly collided with theoretical and practical constraints. He claims that adversaries continue to avoid detection by taking advantage of ambiguity, mobility, and environmental complexity despite notable advancements in automated targeting, sensor fusion, and persistent monitoring. He argues that the epistemological and ontological limits of these technologies, which are rooted in the problem of reasoning under

uncertainty, render the dream of total awareness unreachable.

The book's idea of "fog-of-war machines," which are largely discussed in Chapter 5, is among its most inventive contributions. These are systems of deception and strategic illusion, not individual technologies, that use a combination of AI-generated deepfakes, signal spoofing, radar deception, and cognitive overload to take advantage of adversaries' perceptual blind spots. Geist divides them into a number of operational elements, including real-time information poisoning, hostile physical objects intended to trick AI classifiers, SIGINT deepfakes, and GAN-based picture manipulation. Instead of outright destroying the opponent, these technologies aim to distort their reality and influence their strategic choices before conflicts even break out.

In this vein, Geist reflects on the cultural significance of the 1983 film *WarGames*, which suggested that the only winning move in nuclear conflict is "not to play." However, he flips this insight on its head. The real task, Geist implies, is not to build a superintelligent War Operation Plan Response (WOPR) system to control the battlefield, but rather to undermine the adversary's WOPR, which is for deceiving, misleading, and blinding the opposing eye. This counter-strategy is termed "Anti-WOPR," where success lies not in achieving omniscience, but in preventing the adversary from achieving it (p. 167). It turns out that the same techniques that might accomplish such feats as finding submarines hiding at sea are also the most powerful tools to thwart themselves. States will be forced to seek security by reducing their adversaries' situational awareness rather than safeguarding their arsenals by denying them a dependable way to destroy them.

Geist's investigation of how developing technologies can not only fail to make the strategic environment clearer but perhaps actively increase its instability is made possible by this analytical framework. The fact that strategic actors work in circumstances where data is imperfect, deceptive, or purposefully distorted raises issues with the notion that having more information results in better choices. Here, Geist introduces the central insight of the book: We are moving into a deception-dominant world (p. 196). The secret to strategic advantage in such circumstances is not clarity but invisibility, and not visibility but hiding. States are increasingly attempting to blind and deceive opposing systems of perception rather than simply destroy enemy capabilities.

This new state gives rise to cognitive warfare, in which the opponent's capacity for accurate world perception is the goal rather than merely their armament or infrastructure. Geist shows that although AI-enabled systems are frequently commended for their accuracy and speed, they can also be particularly susceptible to manipulation. Heuristic shortcuts and weak assumptions are used in the attempt to combine enormous amounts of sensor data into a cohesive image of battlespace. These flaws give attackers the opportunity to use decoys, distortions, or synthetic signals, which are the strategies that might cause uncertainty, impede judgment, or elicit incorrect reactions. The act of perceiving itself becomes a disputed area in such a setting.

Geist argues that to adapt to this new environment, the logic of deterrence must change. He presents the concept of *reconstructivism* here, which is a framework that transcends the conventional ideas of deterrence-by-retaliation or deterrence-by-denial. Reconstructivist deterrence aims to change the funda-

mental framework of the adversary's thinking rather than just changing their cost-benefit analysis. It seeks to affect adversaries' cognitive filters, value systems, and interpretative frameworks to affect not only what they think but also how they come to hold those ideas. According to this perspective, deterrence is much less mechanical and more psychological than its Cold War equivalent, and instead becomes a struggle for meaning, identity, and perception

Such a transformation is made operational through what Geist calls *engineered multistability*. This term, which comes from cognitive science, describes situations that allow for several reasonable interpretations, none of which can be immediately verified or refuted. Actors might weaken hostile confidence and stop the enemy's decision cycles by purposefully creating unclear strategic circumstances. Ambiguity in designed multistability is a state to be weaponized rather than a problem to be resolved. States construct conditions where every sensor reading or intelligence cue could point to various, contradictory conclusions rather than attempting to eliminate uncertainty (p. 219).

Nevertheless, the book is not without its limitations. Geist's treatment of non-Western perspectives is limited, and the implications of AI-powered deterrence in regional contexts such as South Asia or the Middle East remain underexplored. Additionally, despite the book's strong conceptual foundations, it does not provide specific policy recommendations for crisis management, arms control, or norm-building in the era of intelligent machines. These omissions demonstrate the book's intention to inspire strategic creativity rather than prescribe ideology.

Deterrence under Uncertainty is a seminal work that is worth reading in the field of strategic studies. It encourages academics and professionals to examine the cognitive and epistemic flaws that underline contemporary strategic interaction and questions widely held beliefs about the ability of technology to address deterrence issues. Geist concludes by cautioning that uncertainty is a characteristic of strategic reality rather than a disadvantage that should be eliminated. Instead of looking for technological solutions, he supports a more realistic strategy that views ambiguity, deception, and perception as necessary components of the system rather than as flaws in it. Geist contends that in a society where deception is prevalent, security is more dependent on our interpretations than on what we see. As he stated, "Rather than securing their arsenals by depriving their opponents of a reliable means of destroying them, states will have no choice but to seek security by impairing their adversaries' situational awareness" (p. 80). Security is no longer about denying the attacker; it's about blinding the observer.