Precision-Guided Predictions: Intelligence Risk in Prediction Markets

Description

What if an alarm in the presidential residence in Caracas didnâ??t come from a radar hit or a defecting general, but came from a smartphone? Imagine if the security detail for NicolÃ¡s Maduro was monitoring the prediction markets when suddenly they witnessed a vertical spike. The probability of Maduroâ??s â??removal from powerâ?• on January 3rd surged from 7 percent to 38 percent in less than 120 minutes. There was no corresponding news, no force movements detected by the media, and no diplomatic shifts. But the market knew.

In this case, from the moment the contract value spiked, the security detail would have had precisely forty minutes to relocate the target before the U.S. special operations team hit the objective. The element of surprise, the most difficult and fragile asset in warfare, was potentially compromised by a $436,000 payout that occurred under highly scrutinized circumstances. Just two months later, surprise was put at risk again when 12 new Polymarket accounts bet on the first airstrike in Iran, netting a gain of $330,000.

While these cases rely more on circumstantial evidence, February 2026 indictments in Israel provided the first empirical confirmation of â??insider tradingâ?• in a kinetic environment. An IDF reservist and a civilian were charged with â??severe security offensesâ?• after allegedly using classified operational data to make bets on Polymarket regarding the timing of Israeli strikes against Iran. The user correctly front-ran four separate military developments with striking accuracy, netting $150,000 and creating a digital signature of intent accessible to any adversary who happened to be monitoring these markets.

These incidents are structural warnings regarding the â??weaponization of salience.â?• Prediction markets have effectively commoditized state intent, creating a friction point where the volume of the trade provides a more agile sensor than traditional intelligence indications and warning. This shift demands a strategic pivot: the national security establishment should move beyond viewing these platforms as speculative novelties and recognize them as real-time indicators of an ethical and operational crisis.

Whatâ??s Old is New Again

The current alarm over prediction markets echoes an attempt to use betting markets as intelligence from decades ago. In 2003, DARPAâ??s Policy Analysis Market (PAM) was designed as an internal intelligence analysts tool to forecast Middle Eastern stability through a similar price mechanism. However, PAM became a political casualty before it could prove its operational worth. As noted in comprehensive reviews of the program, PAM failed not because of an analytical deficit, but because the optics of â??betting on deathâ?• triggered public and congressional backlash. The program was shuttered in July 2003, less than two years after its inception and only a day after its public unveiling.

Following the PAM fallout, the CIAâ??s Center for the Study of Intelligence continued to explore these mechanisms internally. Their research concluded that prediction markets could â??overcome many of the institutional and psychological barriersâ?• to effective analysisâ??specifically the tendency toward bureaucratic consensus and the â??echo chamberâ?• effect. The intelligence community recognized that markets prioritize accuracy over hierarchy. But the negative perception of PAM hampered these tools within formal intelligence analysis.

Today, the emergence of private, decentralized platforms like Polymarket contends with the past governmental control over market-based predictions. Furthermore, the barriers to entry evaporated. In 2003, participation required specialized access and a desktop terminal; in 2026, every individual with a smartphone is effectively a distributed sensor. The analytical power that DARPA once sought is now being wielded by a global, hyper-connected public, but without the security protocols or ethical guardrails that a state-run program would have required.

The Market as a High-Fidelity Sensor

In traditional intelligence parlance, indications and warning (I&W) are the process of monitoring specific â??signaturesâ?• like troop consolidations, encrypted traffic surges, or diplomatic evacuations to predict an adversaryâ??s next move. Historically, the state held a monopoly on the most sensitive indicators. However, the rise of high-liquidity platforms like Polymarket and Kalshi democratized this signal by allowing any individual, many of whom have inside knowledge of upcoming policy or event outcomes, to place bets.

Prediction markets operate on the Hayekian principle that information is widely dispersed and can only be effectively aggregated through a price mechanism. In a military context, this means that a logistics officer in Norfolk, a junior analyst at Fort Meade, and a contractor in Florida each hold a fragment of the truth. Individually, they possess educated guesses. Collectively, when they stake capital on a specific outcome, they create a high-confidence signal that bypasses the bureaucratic friction of traditional intelligence reporting.

Measuring Salience: Dollars Do Not Lie

To understand the empirical value of these markets, we must shift from viewing them as mere probability machines to viewing them as attention aggregators . In academic and intelligence contexts, probability is a measure of likelihood, but salience is a measure of prominence and relevance. It is the degree to which a specific piece of information or an event stands out from its environment to capture the cognitive attention of an observer.

Traditional intelligence often struggles with salience bias, which is the tendency to focus on information that is vibrant or recent rather than structurally significant. Analysts are frequently trapped responding to the loudest data point. Salience is notoriously difficult to quantify because it lives in the subjective weight an observer gives to a fact.

Prediction markets can solve this by converting subjective weight into objective At-Stake Capital (ASC) . In this framework, the *price* of a contract reflects the aggregated probability, but the *volume and liquidity* reflect its salience. If a market on civil unrest in a remote region has a 15 percent probability but only $5,000 in volume, the event is statistically unlikely and socially ignored. However, if that same 15 percent probability is backed by $15 million in volume, the event has achieved hyper-salience. Even if the price does not move, the capital influx tells the observer that someone with significant resources believes they have an information advantage strong enough to predict an outcome.

The Ethical Dilemma: Defining the Information Privilege

In prediction markets, defining the â??information privileged individualâ?• is a significant legal and conceptual grey area that diverges from traditional securities law. Unlike the stock market, where an insiderâ??s fiduciary duty is tied to an issuer or a specific asset, the prediction market â??insiderâ?• is anyone whose professional role grants access to non-public, outcome-determinative informationâ??be they a diplomat, a data analyst, or an operator. Currently, no federal legal standard defines this role; it exists in a regulatory vacuum between the CFTCâ??s oversight of commodities and â??event contractsâ?• and the varying state-level definitions of gambling. This lack of a formal â??insiderâ?• definition means that while a trade might be ethically fraught, it often falls outside the reach of existing anti-fraud statutes, creating a significant enforcement gap where informational â??edgeâ?• is functionally indistinguishable from â??privilegedâ?• leakage. And while the STOCK Act of 2012 codified the â??dutyâ?? of federal employees to avoid profiting from non-public information, the law is anchored to the definition of â??securitiesâ?? and provides no clear jurisdiction over modern prediction markets.

This dynamic introduces ethical risk as it represents a psychological and institutional shift where government employees may begin to view sensitive policy outcomes and human lives as mere payout variables. When an individual has a financial stake in the success or failure of a specific state action, the incentive structure for neutral, professional judgment is potentially jeopardized. This creates a friction between public duty and private interest that compromises the integrity of the governmentâ??s entire decision-making process. These concerns echo the failures of DARPAâ??s PAM project.

In economic terms, an insider is harvesting the â??Ignorance Premiumâ?• of the public. But when they are a government employee, they take an event that is highly probable in their world, potentially a secret, and sell that certainty to a market that still views it as a low probability. The ethical breach occurs when access to a non-public â??signalâ?• is used to capture capital, effectively front-running reality. The collision of prediction marketsâ?? core value proposition of unfiltered information discovery with national security requirements creates a systemic vulnerability that threatens to inadvertently leak undisclosed and potentially secret government information. In short, public servants with inside information can legally and easily make money by using that information to bet on events they know are going to happen but the public views as unlikely. The public and visible nature of such high conviction bets creates a substantial risk to intelligence and operational security.

Strategic Imperatives and Policy Responses

Prediction markets represent a profound opportunity for academia and intelligence professionals to quantify salience, a metric traditionally relegated to subjective assessment. By observing the volume of at-stake capital, observers can filter the signal from the noise, identifying which geopolitical events are viewed as worth the risk by those with skin in the game. This provides a dynamic, real-time measure of strategic priority that static reports and traditional modeling cannot match, offering a rare window into the collective perception of informed actors.

However, this utility is double-edged. For an adversary, these markets function as an inadvertent but high-fidelity I&W system. When government personnel are presumed to participate, they create an ethical paradox that erodes institutional integrity and compromises operational security. Suspicious trading patterns, like those seen in the Maduro case, suggest that every dollar staked by a cleared individual on a non-publicly foreseeable event is a data point gifted to the enemy, potentially signaling imminent action and liquidating the element of surprise long before the first kinetic movements occur.

Given these high stakes, the Department of Defense should immediately address the use of prediction markets within its ranks. While legislative efforts like the *Public Integrity in Financial Prediction Markets Act of 2026* provide a framework for punishing enrichment by public figures, they do not resolve the

counter-intelligence threat. The Department should move decisively to establish clear policy guidelines, including the explicit integration of prediction market activity into the Standard Form 312 (Classified Information Nondisclosure Agreement). Policy should be updated to state that the use of non-public information to influence or profit from event contracts is a direct violation of the NDA and the broader trust inherent in the security clearance process. To go further, the SF-86 (Questionnaire for National Security Positions) could be revised to require the disclosure of high-volume or â??privilegedâ?• accounts on the prediction markets, treating these digital stakes as a material financial interest and a potential counter-intelligence vulnerability.

Organizational leaders should also take note. Commanders of organizations with specialized knowledge, particularly within the intelligence community and operational units, should consider clearly addressing the ethical issues with prediction market participation with their members. Organizational leaders must stress that in this domain, a single memberâ??s intellectual curiosity or financial opportunism can compromise operational security.

Secrecy in a â??Predictionâ?• Era

The Maduro and Israeli incidents confirm that the security of state intent is no longer a matter of hardening internal controls, but of managing data-driven salience in a world where every smartphone acts as a distributed sensor. In this era of weaponized transparency, prediction markets represent a new frontline for irregular warfare, providing an uncompromising, empirical assessment of intent that no official narrative can counteract. Secrecy is no longer defined by the ability to hide facts, but by the institutional discipline required to manage the visibility of those facts in a market that treats every secret as a tradable asset. As an enterprise, the Department of Defense must now decide: will it remain a passive victim of this transparency, or will it evolve the doctrine and clearance protocols necessary to command the signal?

Peter Burns is the Chief Operating Officer of the Irregular Warfare Initiative.

The views expressed are those of the author(s) and do not reflect the official position of the Irregular Warfare Initiative, Princeton Universityâ??s Empirical Studies of Conflict Project, the Modern War Institute at West Point, or the United States Government.

Main Image generated using Gemini by Google (February 2026).

If you value reading the Irregular Warfare Initiative, please consider supporting our work. And for the best gear, check out the IWI store for mugs, coasters, apparel, and other items.

Date Created
2026/03/06