SECURITY & DEFENCE QUARTERLY

Capital flows and blockchain forensics on decentralised prediction markets as a potential source of early warning in the era of disinformation

Krzysztof Trzcianowski[1], Przemysław Janiszewski[2]

[1]trzciano@student.agh.edu.pl

[1]https://orcid.org/0009-0000-7341-0105

[2]https://orcid.org/0009-0007-3537-7923

[1,2]Faculty of Metals Engineering and Industrial Computer Science, AGH University of Krakow, Czarnowiejska 66, 30-054, Kraków, Poland

Abstract

This study inquires how far public prediction-market data can detect anomalous trading and attribute it to identifiable actors. It develops a forensic attribution framework and tests what such observations add as potential early-warning indicators under conditions of disinformation. A purposive, retrospective, and qualitative design covers six trading episodes and two contract-design illustrations. We independently reconstruct Ukrainian price and trade records, the Venezuelan account identified in legal filings, five reported Iranian accounts, and the trading and Polygon transfers of one Hungarian account; the other episodes are assessed through published reporting. Evidence, alternative explanations, and confidence are evaluated separately. Public records reproduce the indicted Venezuelan trading exactly, and five accounts reported before the strikes on Iran bought 1,065,775 shares for a net USD 928,559. The Hungarian funding chain traces through a single Polygon address to a regulated exchange, the point at which identification requires legal process rather than public data. Ukrainian prices went up from 0.380 to 0.905 within 5 minutes as twenty-eight addresses bought; across 18,462 windows that increase occurs once, yet all twenty-eight traded other markets and most gained little; so, the pattern alone does not separate informed from ordinary trading. Public reporting preceded the earliest market rule by about 10 hours. Public data supports detection, reproducible measurement, and tracing to a regulated intermediary where attribution can continue. They do not establish insider activity or validated warning performance, so operational use requires corroboration, treatment of false alarms, and resistance to fabricated signals. A domestic market with identity verification remains a research hypothesis.

Keywords:

prediction markets, early warning, blockchain forensics, attribution, disinformation

Article info
Received: 14 June 2026
Revised: 15 September 2026
Accepted: 30 September 2026
Available online: 09 November 2026

Citation: K. Trzcianowski, P. Janiszewski (2026) 'Capital flows and blockchain forensics on decentralised prediction markets as a potential source of early warning in the era of disinformation', *Security and Defence Quarterly*, 56(4). doi: 10.35467/sdq/240535.

© 2026 K. Trzcianowski and P. Janiszewski. Published by War Studies University, Poland.
This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

Introduction

In prediction markets, participants commit money to the outcomes of events that matter for national security, such as military action, elections, and control of territory. Their prices can be followed alongside news reports, and public blockchain records allow some of the associated capital flows to be traced. This creates an analytical opportunity, because an unusually timed position may point to activity worth examining before an event becomes widely known. A large position, however, may reflect privileged information, quick use of open sources, hedging, chance, or an attempt to mislead observers, and these possibilities have to be separated before a market movement is treated as a warning.

In a standard binary contract, a winning share pays one unit and a losing share pays nothing, so prices are often read as probabilities. That reading depends on incentives, liquidity, risk preferences, and settlement rules. Prediction markets were designed to aggregate dispersed information, and evidence from electoral markets supports their forecasting potential (Arrow *et al.*, 2008; Berg *et al.*, 2008; Vaughan Williams and Reade, 2016). An accurate forecast, however, reveals neither who supplied the information nor how it was obtained, nor whether unusual trading signals a security threat.

Our principal contribution is a forensic attribution framework with a potential warning application. It separates three steps, namely behavioural screening, tracing of capital flows on the public ledger, and identification through additional records, and it is neither a validated prediction model nor a complete surveillance system. Two research questions guide the analysis. First, how far can anomalous trading be detected and attributed to identifiable actors using public data alone? Second, which forms of anomalous activity can be distinguished by their information source, intervention point, and evidentiary status? For national security, the answers show what such observations can responsibly add to intelligence assessment.

We use early warning to mean information that reaches a decision-maker before a relevant event becomes public knowledge, and a potential early-warning indicator to mean an observable pattern whose practical warning value has not been validated. Anomaly detection identifies departures from a specified reference profile; as none is measured here, our indicators remain qualitative screening criteria. Informed trading exploits an informational advantage—public or non-public. Insider activity denotes the suspected use of restricted information in breach of a duty, and its legal character depends on the facts and the applicable law. Attribution links activity to an actor; attributing an address is distinct from identifying a natural person. Manipulation is the intentional distortion of trading signals or settlement inputs, and disinformation is deliberately false information intended to influence others.

Related research and conceptual framework

Research on prediction markets shows both their potential and their limits. Berg *et al.* (2008) examine forecasting accuracy across several elections, and Page and Clemen (2013, p. 506) show why calibration has to be assessed across forecast horizons. Lee *et al.* (2020) find anomalies in probability estimates that persist even in heavily traded markets. Neither heavy turnover nor an accurate outcome should therefore be read as evidence of superior information.

Market microstructure offers a complementary view. Kyle (1985) models how informed trading, liquidity trading, and price formation interact, and Meulbroek (1992) studies

the price effects of detected illegal insider trading. Bogousslavsky *et al.* (2024) estimate informed-trading intensity from patterns in volume and volatility, while Rothschild and Sethi (2016), using account-level prediction-market data, find indications that one large trader may have tried to manipulate prices. This literature explains why informed activity can leave observable traces, but it does not turn concentrated profits into a diagnostic test. Evidence from detected offences is itself selective, because only part of insider trading is ever detected (Katselas and Osborne, 2025), and findings from securities markets cannot simply be transferred to event contracts.

Blockchain forensics links transactions and services through public records and clustering heuristics (Nicholls *et al.*, 2024). Meiklejohn *et al.* (2013) show the investigative value of combining transaction analysis with information about services, and their Bitcoin-based approach also shows why methods must be adapted to the ledger and wallet architecture under study (Akcora *et al.*, 2022; Linoy *et al.*, 2021). Anti-money-laundering investigation and market surveillance similarly combine transaction patterns with contextual evidence; the present framework organises these evidentiary steps for event markets and does not claim a new clustering algorithm.

Warning theory adds the decision problem. Choo (2009) examines the conditions under which information contributes to effective warning; Paté-Cornell (2002) explains why evidence must be combined with prior probabilities; and Gentry and Gordon (2019) treat strategic warning as a distinct intelligence function. The operational value of a signal depends on false alarms, missed events, and the consequences of acting, and repeated false alarms erode the credibility of later warnings (Breznitz, 1984). Open-source intelligence (OSINT) offers a competing explanation for rapid trading: open sources combined with satellite imagery can produce added-value battlefield intelligence (Kotaridis and Benekos, 2023, p. 4), and public information can be processed unevenly without any unlawful advantage. Strategic deception offers another. Deception has frequently accompanied strategic surprise (Whaley, 2007), disinformation is an established instrument of hybrid warfare (Dov Bachmann *et al.*, 2023), and an adversary may fabricate the appearance of privileged knowledge to influence an analyst, even if the resulting market distortion is short-lived.

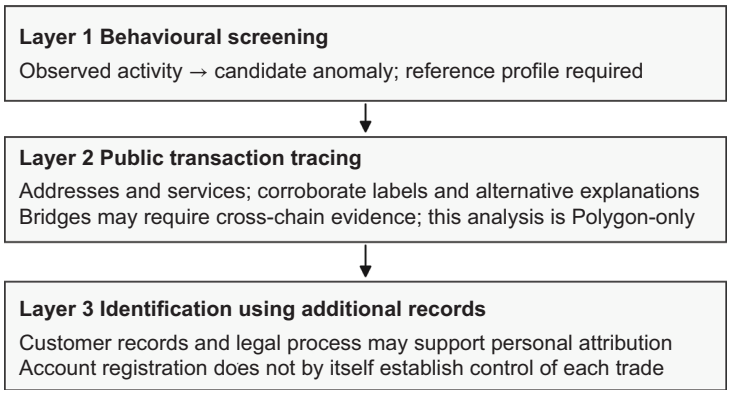
These strands yield a conditional sequence. An informational advantage, another trading motive, or an attempt at manipulation produces observable activity. Compared with a reference profile, the activity may be flagged as a potential anomaly, and corroboration together with an assessment of alternative explanations then determines whether further monitoring is justified. Tracing can connect addresses and services, but identifying a person requires additional evidence, and no step follows automatically from the prior one. Figure 1 presents the framework.

Methods

Design and scope

We use a qualitative, purposive case design to examine mechanisms, not to estimate prevalence. Six trading episodes concern Venezuela, Iran, Ukraine, Russia, France, and Hungary, and two further illustrations concern contract wording and settlement rules. The case material covers November 2025–May 2026. A case was included if it was relevant to information use, settlement integrity, or attribution and had an identifiable documentary source. Selection was exploratory, with no systematic search denominator or exhaustive log of exclusions.

Figure 1. Conditional stages of the attribution framework.
***Source*: Authors' elaboration.**



The analysis distinguishes episodes, markets, and addresses. It covers seven individually specified binary markets in the Venezuelan, Iranian, Ukrainian, and Hungarian episodes, a Russian market described in reporting, and French temperature contracts linked to two event dates. The two contract-design illustrations concern separate binary questions. For the Russian and French cases, we analyse the reported mechanism rather than individual trades.

Independent trading analysis covers the Venezuelan account identified in a regulatory complaint, five Iranian accounts named in reporting, one Hungarian proxy wallet, and twenty-eight Ukrainian addresses that bought in the focal interval. The Venezuelan dataset comprises nineteen activity records: thirteen purchases, two sales, and four redemptions; the Iranian accounts made 190 purchases in the focal market. Hungarian data comprise 145 activity records (141 of them trades), one closed-position record, and four Polygon transfers documenting funding and withdrawals. For Ukraine, the dataset comprises 1,196 price observations and 2,000 retrieved trade records, of which 115 purchases meet the focal filter.

Sources and procedures

Market data come from Polymarket's (2026) application programming interfaces (APIs) and from Polygon transaction records. The Gamma API supplies market descriptions and identifiers, the central limit order book (CLOB) endpoint supplies price history, and the Data API supplies trades and account activity; Polygon records document transfers. API records are a historical extract and remain subject to changes in indexing and pagination, whereas ledger records provide transaction evidence. Amounts are denominated in USD Coin Ethereum/*Bridged* (USDC.e), a stablecoin pegged to the US dollar.

All analytical times are in Greenwich Mean Time/coordinated universal time (UTC), and prices are used without interpolation. Ukrainian trades are filtered to purchases (side BUY) of the YES outcome on 6 March 2026, from 16:05:00 inclusive to 16:11:00 exclusive. Records identical in transaction hash, wallet, asset, side, size, price, and timestamp are collapsed, which leaves 1,974 of the 2,000 records; none of the twenty-six collapsed records meets the focal filter. Price history covers 00:00–20:00 UTC on 6 March 2026 at fidelity = 1, and four pages of 500 records each. Hungarian activity covers 8–24 April 2026 (limit = 500, offset = 0), and the activity of twenty-eight Ukrainian addresses covers 1 February–1 April 2026 in pages of 500 records; four of them exceeded the record

limit of that endpoint, so their focal purchases are not reachable. Iranian accounts were located among trades of at least USD 500 and matched to reported share counts. Trades are ordered by timestamp and summed by side, and non-trade activity is excluded from cash flow. Sale proceeds minus purchase expenditure are reported separately from the closed-position profit given by the platform. Gamma records are labelled v1, whereas the CLOB and Data API endpoints publish no version identifier.

Behavioural screening considers recent account activity, concentration, unusually large executions, and changes in execution price. These are candidate cues rather than calibrated thresholds: first activity within the analysed window does not prove when an account was created, and activity in one market says nothing about the concentration of a whole portfolio. Polygon tracing follows the four documented transfers through Relay's public request records and the USDC transfer logs of the addresses they reveal. A shared infrastructure address is not treated as evidence of common beneficial ownership.

For each episode we distinguish direct observations, reported claims, interpretation, and legal status. Confidence is qualitative and attached to a specific proposition: high for a reproducible observation or the existence of a document, moderate for an interpretation with incomplete corroboration, and low or indeterminate for an untested attribution. Wherever relevant, we consider public information, chance, hedging, coordination, market making, and account migration. An allegation is not a conviction, and the absence of a publicly identified suspect does not imply legality. Table 1 summarises the evidence.

Results

Reported information advantages

The Venezuelan episode shows the difference between detection and legal identification. In United States v. Van Dyke (United States District Court for the Southern District of New York, 2026, pp. 5–6), the indictment alleges that a member of the US service

Table 1. Evidence and financial scale of six trading episodes.
Note. ISW: Institute for the Study of War.
***Source*: Authors' synthesis of the cited case sources and the calculations reported in the "Results."**

Episode	Evidence and scale	Attribution limit	Confidence
Venezuela	Indictment and public trades: thirteen purchases, USD 33,934; USD 409,881 above cost.	Account linked to defendant by legal filings only; guilt not established.	High for trades and allegation; guilt undetermined.
Iran	Reporting and public trades: five of the six accounts; net USD 928,559.	Common funding and information source not verified independently.	High for trades; low for coordination.
Ukraine	API: price 0.380 to 0.905; twenty-eight buying addresses.	Address independence unproven; trigger of the move unresolved.	High for calculations; moderate for cause.
Russia	ISW acknowledged an unauthorised edit to the settlement map.	Market identifier not recovered; beneficiary link unresolved.	High for the edit; beneficiary indeterminate.
France	Météo-France complaint after readings on two dates.	Investigation reported; personal responsibility unresolved.	High for the complaint; responsibility indeterminate.
Hungary	API: trade cash-flow difference 118,152.92 USDC.e; four transfers.	Funding traced via one address to a Binance hot wallet; holder unidentified.	High for transfers; controller indeterminate.

used restricted information about an operation involving Nicolás Maduro to trade-related contracts, committing approximately USD 33,900 on thirteen occasions across four markets for approximately USD 409,900 in profit (p. 8). A parallel civil complaint gives the account's truncated wallet address (Commodity Futures Trading Commission, 2026, p. 12), which matches one Polymarket account. Its public records show thirteen purchases in the same four markets between 27 December 2025 and 3 January 2026 (UTC), amounting to USD 33,934.34, and sales and redemptions that exceed this cost by USD 409,880.95. Public data thus reproduces the alleged trading exactly, but the link between the account and the defendant comes from the legal filings.

Timing and concentration would have justified scrutiny, but public reporting of a months-long US military build-up, strikes on alleged drug boats, and a strike on a Venezuelan dock in late December 2025 (Associated Press [AP], 2025) signalled that the US action was possible and thus offered an alternative explanation for a bullish position. Confidence is high in the reconstructed trades and in what the filings allege, while culpability remains a matter for the court.

In the Iranian episode, Rodrigues (2026) reported that six recently funded wallets took positions before the strikes of 28 February 2026 and made substantial profits, and Bubblemaps named the accounts (Abrams, 2026). We matched five of them with public account records. Between 25 February 2026 and 04:48 UTC on 28 February 2026, before the market price jumped at 06:13 UTC, these accounts bought 1,065,775 YES shares for USD 137,216 and redeemed them for a net gain of USD 928,559, close to the reported estimates, and four of them show no platform activity in the retrieved window prior to 24 February 2026. The clustering and timing are consistent with coordination, but we did not test common funding, and nothing in the records shows access to restricted information. A common service, lawful coordination, or a rapid reading of public signals could produce the same picture, so coordination remains a reported hypothesis and the origin of any advantage is indeterminate.

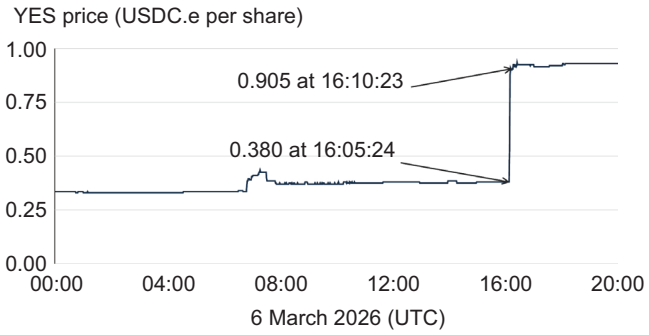
Ukrainian price movement

The Ukrainian contract asked whether Ukrainian forces would re-enter Novomykolaivka in Dnipropetrovsk Oblast by 31 March 2026. Its rules named the Institute for the Study of War's (ISW) map as the primary settlement source, and the market resolved YES on 8 March 2026. On 6 March 2026 the price increased from 0.380 at 16:05:24 UTC to 0.905 at 16:10:23, an increase of about 138% (Figure 2). The focal filter identifies 115 purchases by twenty-eight distinct proxy wallets, and confidence in these calculations within the analysed dataset is high.

Institute for the Study of War's assessment for 6 March 2026, with a data cut-off of 16:15 UTC, cites a report by the Ukrainian observer Kostyantyn Mashovets that Ukrainian forces had advanced into central Novomykolaivka, and ISW's map timed 18:30 UTC shows these advances as claimed Ukrainian counteroffensives, a layer that the contract accepted for settlement (Institute for the Study of War, 2026). The cited Telegram post appeared at 06:06 UTC, about 10 hours prior to rise in price, and the channel posted nothing further on the town that day (Mashovets, 2026). Public information thus preceded the move but does not explain its timing. Coordinated trading remains an alternative explanation; so, confidence that public information drove the move is moderate.

The twenty-eight addresses are the complete set of buyers in the focal window, which permits a contrast without choosing cases. Each of them traded other contracts between

Figure 2. Ukrainian YES price on 6 March 2026 from 00:00 to 20:00 UTC. *Source:* Authors' calculations from Polymarket price history; 1,196 observations.



1 February 2026 and 1 April 2026, from nine to 1,664 distinct markets, so none was opened for this question alone. Among the twenty-four addresses whose focal purchases are reachable, three ended below cost, although the market resolved YES, eleven gained less than one-tenth of what they spent, and the largest position, 11,174 USDC.e, returned 3.4%. Buying during the spike therefore does not separate informed trading from ordinary activity.

Simpler rules behave differently on the same series. A volume rule ranks the focal interval only fourth, because the three largest 6-minute volumes fell on 8 March 2026, the day of settlement. A count of distinct participants separates it unambiguously, ninety-six addresses against at most thirty-eight elsewhere. Public reporting preceded all of them by at least 10 hours; so in this episode, open-source monitoring would have been earlier than any market rule. This is a comparison on one contract, not a measure of performance.

Interference with settlement sources

The Russian episode concerns an edit to ISW's interactive map on the night of 15–16 November 2025 that showed a Russian advance in Myrnohrad and allowed a related Polymarket question to resolve (Gault, 2025). ISW stated that the edit was "unauthorized and unapproved" and removed it before its next update (Cleveland-Stout, 2025); the market itself could not be located. The episode shows how interference with a settlement source can affect a contract without conveying any knowledge of the battlefield, and the rules of the Ukrainian contract exclude temporary glitches or errors in the map. Confidence is high that an unauthorised edit occurred, while the link between its author and the accounts that benefited remains indeterminate; assigning responsibility would require evidence connecting the alteration to control an account.

A similar problem of source integrity arose with temperature contracts settled on readings at Charles de Gaulle airport. After sudden spikes on 6 and 15 April 2026, Météo-France filed a complaint for tampering with an automated data processing system (Kennedy *et al.*, 2026), and from 19 April 2026, the rules of Polymarket's Paris contracts named the Le Bourget station instead. Altering a measurement used for settlement could thus change contract outcomes. Equipment malfunction and deliberate interference remain competing explanations, because no cause or perpetrator is established publicly; confidence in its relevance is high, and responsibility is indeterminate.

These episodes link the integrity of external information to the procedure by which it is accepted. Polymarket's (2026) documentation describes outcome proposals submitted to

the UMA Optimistic Oracle (OO) and a dispute mechanism that can escalate to a vote of UMA token holders. Thus, a map or sensor reading is evidence under the contract rules rather than an automatic trigger for payment, and an investigation must follow the source and the process of proposal, challenge, and resolution.

Contract interpretation

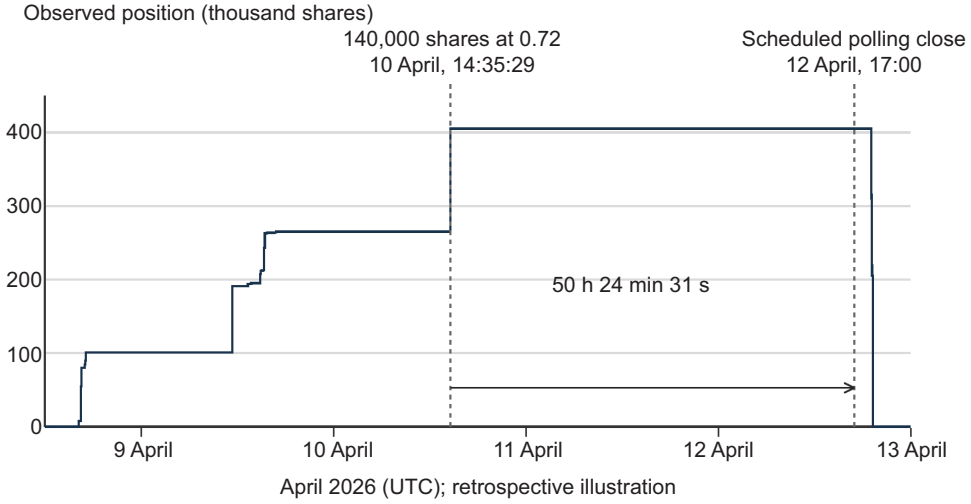
Two contract illustrations show why a market title cannot always be read as a simple statement of probability. The published rules for a question on the return of Jesus Christ rely on a consensus of credible sources, which leaves room for judgement about evidence and interpretation. An analyst must therefore identify the decision rule that the contract actually implements and ask whether it matches the event of intelligence interest.

The second illustration asks whether Jesus Christ will return before Grand Theft Auto VI is released; if neither occurs by 31 July 2026, the contract settles at 0.5. In a simplified undiscounted model, a YES share is therefore worth the probability of a YES outcome plus half the probability that neither event occurs; so a price near 0.5 may reflect this substitute clause rather than a belief that the nominal event is possible.

Hungarian trading and tracing

In the Hungarian case, we independently reconstruct the recorded activity of the account labelled pcpc on the NO side of the question whether Viktor Orbán would become the next prime minister. Ninety-five purchase records between 8 April 2026 and 10 April 2026 total 405,156.796641 shares for an expenditure of 280,952.240363 USDC.e. The largest purchase record, 140,000 shares at 0.72, dates from 10 April 2026 at 14:35:29 UTC (Figure 3). Forty-six sale records on 12 April 2026 yield proceeds of 399,105.158284 USDC.e, which exceed purchase expenditure by 118,152.917921 USDC.e. The platform's separate closed-position field reports 118,158.563 USDC.e; the discrepancy of 5.645079 USDC.e remains unexplained.

Figure 3. Hungarian NO position and hypothetical monitoring interval. *Source*: Authors' calculations from Polymarket activity; ninety-five purchases and forty-six sales.



Two inbound Polygon transfers on 8 April and 9 April 2026 total 399,919.995093 USDC.e. Relay's public request records show that these were swaps within Polygon rather than cross-chain transfers: a smart-contract account paid 150,000 USDC and 250,000 USDC, which Relay delivered to the Hungarian account as USDC.e. Both tranches reached that account seconds before each swap from one unlabelled address, which also received both outbound transfers of 24 April 2026, amounting to 518,163.649481 USDC.e and swapped back to USDC. The capital therefore left from, and returned to, the same address. Each tranche had reached that address after a small test transfer: 150,000 USDC from an unlabelled high-volume address and 250,000 USDC from an address labelled Binance: Hot Wallet 34. These transfers are not trading profit, because they include principal and other account balances. Thus, the trace reaches an exchange whose customer records could identify the account holder, although public data does not. Confidence is high in the documented transfers, the common address, and the exchange link, and indeterminate for personal attribution.

The large purchase is consistent not only with conviction or an informational advantage but also with a reaction to polling, liquidity needs, or a trader moving activity to a new account. Selling before resolution can release capital, reduce settlement risk, or reflect inexperience, and is not in itself evidence of concealment. A hypothetical monitoring decision could have followed that execution, which preceded scheduled polling closure at 17:00 UTC on 12 April 2026 by 50 hours, 24 minutes and 31 seconds (National Election Office, 2026). This is a retrospective interval to a known schedule, not a measured warning, and no alert was generated or prospectively evaluated.

Discussion

What the framework establishes

The answer to the first research question is limited. Public data allowed us to detect observable movements, reconstruct reported trades, and trace the Hungarian account's capital through a single address to an exchange, but not to identify the natural person controlling it. Tracing an address, attributing a service, and identifying a person in law are therefore separate achievements.

For the second question, Table 2 separates information-based hypotheses, interference with settlement sources, and the interpretation of contractual payoffs. These categories concern different intervention points and are not interchangeable types of trader. An information-based hypothesis may involve public, non-public, or uncertain sources; a settlement-source incident may benefit an unrelated opportunist; and a confusing payoff can produce unusual prices without any deception. Instead of inferring illegality from a behavioural signature, the framework specifies what further evidence is needed.

Disinformation and strategic deception

An adversary could deliberately build a concentrated position on a newly used address, accept an unfavourable price, and publicise the trade as evidence of privileged knowledge. Such activity might divert analytical resources, shape expectations, or reinforce a deception campaign, with trading losses accepted as the cost of influence. Conversely, an informed actor could evade a screening rule by splitting activity, using established accounts, or trading through intermediaries. Neither the presence of an anomaly nor its absence is therefore a sufficient basis for a security conclusion.

Table 2. Dimensions of analytical classification. ***Source:*** **Authors' synthesis. Case-specific evidence and confidence are discussed in the "Results."**

Mechanism	Information and intervention	Analytical purpose
Information-based hypothesis	Public, restricted, or unknown; trader behaviour.	Detection; warning after corroboration; attribution where justified.
Settlement-source interference	Potentially falsified; external source and acceptance process.	Detection of interference; attribution and accountability through beneficiary links.
Contract interpretation	Explicit but potentially ambiguous rules; payoff design.	Interpretation of expected payoff before reading price as probability.

Different mechanisms require different data. Spoofing consists of orders placed with no intention of execution and cannot be diagnosed from executed trades alone; studies that detect it rely on order-book messages (Debie *et al.*, 2023; Martínez Miranda *et al.*, 2019). Wash trading creates apparent activity between accounts under related control (O'Leary, 2018), and shared funding infrastructure alone does not prove such control. Deliberate signalling uses genuine, risk-bearing trades to influence observers, whereas data poisoning or interference with a settlement source targets the information accepted under the contract rules. The present datasets do not test these mechanisms but they indicate what evidence an investigation would need.

Manipulation need not produce a lasting forecasting error. Hanson and Oprea (2009) show that, under certain market conditions, informed traders' responses can offset manipulation. This does not remove the security concern, because a transient disturbance may mislead an observer before it is corrected. Treating each alarm as a revisable hypothesis separates market correction from analytical success and exposes repeated false signals aimed at the monitoring process itself.

Domestic markets and jurisdiction

One response to the limit that stopped the Hungarian trace at an exchange beyond domestic reach would be a regulated domestic prediction market with identity verification, but it is a policy hypothesis, not a proven remedy. Differences in population, liquidity, incentives, contract wording, and access to information would prevent its automatic use as a control sample. A useful comparison would match contracts and horizons, measure participation and liquidity, and assess alternative explanations before inferring leakage or manipulation. We do not claim that such a market would be better calibrated or could replace conventional polling.

Cross-jurisdictional enforcement would remain difficult. A domestic regulator may supervise a licensed operator and local intermediaries, yet lack direct authority over foreign participants, records, or infrastructure. Blocking a website or payment provider need not prevent trading by other routes. Public settlement, the operator's domicile, and its regulatory status are separate questions and should not be collapsed into a single jurisdiction. Cooperation and lawful access to records may support identification but neither guarantees that all relevant evidence can be recovered. A domestic venue would also compete with global liquidity.

Identity verification cannot prevent informed trading, guarantee that the account holder controls the activity, or persuade informed actors to use the regulated venue. Any proposal

must address the eligible sensitive contracts, restrictions for public officials and military personnel, position limits, surveillance, auditability, data protection, and anti-money-laundering duties. Independent oversight would be particularly important for contracts concerning government decisions.

Limitations and validation

Purposive selection, hindsight, and confirmation bias are the central limitations. The cases were chosen after they became notable, not sampled from a defined population. There is no denominator across markets, and within the Ukrainian contract the pattern is rare: across 18,462 6-minute windows from 24 February 2026 to resolution, a rise of at least 100% occurs only in the episode examined here, three times at a threshold of 50% and ten times at 20%, most of them in the first hours of trading. A rule strict enough to isolate the episode therefore leaves a single observation, and a looser one multiplies alarms, so no error rate can be estimated from one contract. Chance, hedging, market making, account migration, lawful coordination, and liquidity constraints are not excluded systematically. The findings therefore state nothing about prevalence or success rates, and the relative frequencies of false positives and false negatives are unknown.

The main quantitative reconstruction rests on platform APIs and public ledger records, while several other case claims rely on journalism. Neither an API nor a reported cluster has the standing of a peer-reviewed measurement or an adjudicated fact. The analysis is specific to one platform, metadata may change, and trade histories do not preserve full order books. An unexplained lag between public reporting and the price move limits causal inference in the Ukrainian episode, and the Hungarian exercise relies on post-event retrieval without a pre-registered alert rule.

A prospective evaluation should define eligible markets, observation intervals, and alert criteria before outcomes are known, and preserve the public information available at the time. Every interval should be retained, with or without an alert. Performance should be compared with baselines based on price changes, volume, and conventional OSINT at the same observation horizon and decision cost. Lead time should be measured to an independently defined event. Such a design would show whether combining behavioural and capital-flow information adds value beyond simpler monitoring.

Conclusions

Public prediction market and ledger data can reveal trading patterns and trace a funding path to an exchange, but in the cases examined they did not identify the natural person behind a position. Reported legal attribution and reproducible transaction observations must therefore be kept apart. The proposed framework links detection, tracing, and possible identification, and states the evidence required at each stage. Its taxonomy separates uncertain information advantages, interference with settlement sources, and problems of contract interpretation, none of which can be reliably diagnosed from profit, account novelty, or timing alone. In the contract examined in maximum detail, the pattern occurred once and most of those who traded it were ordinary participants.

The Hungarian chronology illustrates a hypothetical opportunity for closer monitoring before scheduled polling closure, not validated early-warning effectiveness. More broadly, these markets may supply complementary indicators whose interpretation depends on corroboration, alternative explanations, and resistance to fabricated signals. A domestic

venue with identity verification merits comparative and legal research, but no policy benefit has been demonstrated. Prospective testing with negative cases and simple baselines is needed before the framework can support operational warning decisions.

Acknowledgements

The authors would like to thank the anonymous reviewers and the Editors of Security and Defence Quarterly for their valuable comments, which helped to improve the manuscript.

Funding

This research received no external funding.

Author Contributions

Conceptualisation, K.T. and P.J.; methodology, K.T. and P.J.; software, K.T. and P.J.; validation, K.T. and P.J.; formal analysis, K.T. and P.J.; investigation, K.T. and P.J.; resources, K.T. and P.J.; data curation, K.T. and P.J.; writing—original draft preparation, K.T. and P.J.; writing—review and editing, K.T. and P.J.; visualisation, K.T. and P.J.; supervision, K.T. and P.J.; project administration, K.T. and P.J. Both authors read and agreed to the published version of the manuscript.

Data Availability Statement

Data and code reproducing all reported calculations are openly available in Zenodo at https://doi.org/10.5281/zenodo.22767261

Disclosure Statement

No potential conflict of interest was reported by the authors.

AI Use Disclosure

The research question, the selection of cases, the attribution framework and the interpretation of the evidence are the authors' own. During the revision, the authors used Claude Opus 5.5 (Anthropic) and GPT-6 Astra (OpenAI) as assistive tools for three tasks: language editing and restructuring of the revised text in response to the reviewers' comments; suggesting additional literature, each item of which the authors checked against the original publication; and preparing code for the reproducibility package, whose results the authors verified by rerunning the analysis. The authors reviewed and revised all output and take full responsibility for the content of the manuscript.

References

Abrams, Z. (2026) 'Fresh accounts netted $1 million on Polymarket hours before US airstrikes on Iran: Bubblemaps', *The Block*, 28 February. Available at: https://www.theblock.co/post/391650/fresh-accounts-netted-1-million-on-polymarket-hours-before-us-airstrikes-on-iran-bubblemaps (Accessed: 14 September 2026).

Akcora, C.G., Gel, Y.R. and Kantarcioglu, M. (2022) 'Blockchain networks: Data structures of Bitcoin, Monero, Zcash, Ethereum, Ripple, and Iota', *WIREs Data Mining and Knowledge Discovery*, 12(1), p. e1436. doi: 10.1002/widm.1436.

Arrow, K.J., Forsythe, R., Gorham, M., Hahn, R., Hanson, R., Ledyard, J.O., Levmore, S., *et al.* (2008) 'The promise of prediction markets', *Science*, 320(5878), pp. 877–878. doi: 10.1126/science.1157679.

Associated Press (AP) (2025) 'CIA behind strike at Venezuelan dock that Trump claims was used by drug smugglers, AP sources say', *NPR*, 31 December. Available at: https://www.npr.org/2025/12/31/g-s1-104073/cia-behind-strike-at-venezuelan-dock-that-trump-claims-was-used-by-drug-smugglers-ap-sources-say (Accessed: 14 September 2026).

Berg, J.E., Nelson, F.D. and Rietz, T.A. (2008) 'Prediction market accuracy in the long run', *International Journal of Forecasting*, 24(2), pp. 285–300. doi: 10.1016/j.ijforecast.2008.03.007.

Bogousslavsky, V., Fos, V. and Muravyev, D. (2024) 'Informed trading intensity', *The Journal of Finance*, 79(2), pp. 903–948. doi: 10.1111/jofi.13320.

Breznitz, S. (1984) *Cry wolf: The psychology of false alarms*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Choo, C.W. (2009) 'Information use and early warning effectiveness: Perspectives and prospects', *Journal of the American Society for Information Science and Technology*, 60(5), pp. 1071–1082. doi: 10.1002/asi.21038.

Cleveland-Stout, N. (2025) 'Think tanker altered Ukraine war map before big Polymarket payout', *Responsible Statecraft*, 11 December. Available at: https://responsiblestatecraft.org/isw-polymarket-ukraine-war-map/ (Accessed: 14 September 2026).

Commodity Futures Trading Commission (2026) *Complaint for injunctive and other equitable relief and for civil monetary penalties, CFTC v. Van Dyke*, *No. 26-cv-3369*. United States District Court for the Southern District of New York, 23 April. Available at: https://www.cftc.gov/media/13761/EnfGannonKenVanDykeComplaint042326/download (Accessed: 14 September 2026).

Debie, P., Gardebroek, C., Hageboeck, S., van Leeuwen, P., Moneta, L., Naumann, A., Pennings, J.M.E., Trujillo-Barrera, A.A., and Verhulst, M.E. (2023) 'Unravelling the JPMorgan spoofing case using particle physics visualization methods', *European Financial Management*, 29(1), pp. 288–326. doi: 10.1111/eufm.12353.

Dov Bachmann, S.-D., Putter, D. and Duczynski, G. (2023) 'Hybrid warfare and disinformation: A Ukraine war perspective', *Global Policy*, 14(5), pp. 858–869. doi: 10.1111/1758-5899.13257.

Gault, M. (2025) '"Unauthorized" edit to Ukraine's frontline maps point to Polymarket's war betting', *404 Media*, 1 December. Available at: https://www.404media.co/unauthorized-edit-to-ukraines-frontline-maps-point-to-polymarkets-war-betting/ (Accessed: 1 May 2026).

Gentry, J.A. and Gordon, J.S. (2019) *Strategic warning intelligence: History, challenges, and prospects*. Washington, DC: Georgetown University Press. doi: 10.2307/j.ctvb4bsfx.

Hanson, R. and Oprea, R. (2009) 'A manipulator can aid prediction market accuracy', *Economica*, 76(302), pp. 304–314. doi: 10.1111/j.1468-0335.2008.00734.x.

Institute for the Study of War (ISW) (2026) *Russian offensive campaign assessment,* March 6, 2026. Available at: https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment-march-6-2026/ (Accessed: 14 September 2026).

Katselas, D. and Osborne, S. (2025) 'Insider trading footprints: An empirical look at detected cases in Australia', *International Review of Finance*, 25(2), p. e70013. doi: 10.1111/irfi.70013.

Kennedy, N., Courbebaisse, L. and Baudier Kim, E. (2026) 'France investigates suspected tampering with weather sensors after Polymarket bets', *CNN*, 23 April. Available at: https://edition.cnn.com/2026/04/23/europe/france-weather-sensor-polymarket-bet-intl-latam (Accessed: 1 May 2026).

Kotaridis, I. and Benekos, G. (2023) 'Integrating Earth observation IMINT with OSINT data to create added-value multisource intelligence information: a case study of the Ukraine–Russia war', *Security and Defence Quarterly*, 43(3), pp. 1–21. doi: 10.35467/sdq/170901.

Kyle, A.S. (1985) 'Continuous auctions and insider trading', *Econometrica*, 53(6), pp. 1315–1335. doi: 10.2307/1913210.

Lee, H.C.B., Stallaert, J. and Fan, M. (2020) 'Anomalies in probability estimates for event forecasting on prediction markets', *Production and Operations Management*, 29(9), pp. 2077–2095. doi: 10.1111/poms.13175.

Linoy, S., Stakhanova, N. and Ray, S. (2021) 'De-anonymizing Ethereum blockchain smart contracts through code attribution', *International Journal of Network Management*, 31(1), e2130. doi: 10.1002/nem.2130.

Martínez Miranda, E., Phelps, S. and Howard, M.J. (2019) 'Order flow dynamics for prediction of order cancelation and applications to detect market manipulation', *High Frequency*, 2(1), pp. 4–36. doi: 10.1002/hf2.10026.

Mashovets, K. (2026) Telegram Post on the War in Ukraine, 6 March. Available at: https://t.me/zvizdecman-hustu/3279 (Accessed: 14 September 2026).

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. and Savage, S. (2013) 'A fistful of bitcoins: Characterizing payments among men with no names', in Proceedings of the 2013 Internet Measurement Conference (IMC '13). New York, NY: ACM, pp. 127–140. doi: 10.1145/2504730.2504747.

Meulbroek, L.K. (1992) 'An empirical analysis of illegal insider trading', *The Journal of Finance*, 47(5), pp. 1661–1699. doi: 10.1111/j.1540-6261.1992.tb04679.x.

National Election Office (2026) *FAQ*. Available at: https://www.valasztas.hu/en/general-faq (Accessed: 12 September 2026).

Nicholls, J., Kuppa, A. and Le-Khac, N.-A. (2024) 'The next phase of identifying illicit activity in Bitcoin', *International Journal of Network Management*, 34(5), p. e2259. doi: 10.1002/nem.2259.

O'Leary, D.E. (2018) 'Open information enterprise transactions: Business intelligence and wash and spoof transactions in blockchain and social commerce', *Intelligent Systems in Accounting, Finance and Management*, 25(3), pp. 148–158. doi: 10.1002/isaf.1438.

Page, L. and Clemen, R.T. (2013) 'Do prediction markets produce well-calibrated probability forecasts?', *The Economic Journal*, 123(568), pp. 491–513. doi: 10.1111/j.1468-0297.2012.02561.x.

Paté-Cornell, E. (2002) 'Fusion of intelligence information: A Bayesian approach', *Risk Analysis*, 22(3), pp. 445–454. doi: 10.1111/0272-4332.00056.

Polymarket (2026) *Resolution*. Available at: https://docs.polymarket.com/concepts/resolution (Accessed: 11 September 2026).

Rodrigues, F. (2026) 'Suspected insiders make over $1.2 million on Polymarket by betting on US's Iran strike', *CoinDesk*, 28 February. Available at: https://www.coindesk.com/markets/2026/02/28/suspected-insiders-make-over-usd1-2-million-on-polymarket-ahead-of-u-s-strike-on-iran (Accessed: 1 May 2026).

Rothschild, D. and Sethi, R. (2016) 'Trading strategies and market microstructure: Evidence from a prediction market', *The Journal of Prediction Markets*, 10(1), pp. 1–29. doi: 10.5750/jpm.v10i1.1179.

United States District Court for the Southern District of New York (2026) *United States v. Van Dyke. Indictment. 26 Cr. 156, unsealed*, 23 April. Available at: https://www.justice.gov/usao-sdny/media/1437781/dl (Accessed: 11 September 2026).

Vaughan Williams, L. and Reade, J.J. (2016) 'Forecasting elections', *Journal of Forecasting*, 35(4), pp. 308–328. doi: 10.1002/for.2377.

Whaley, B. (2007) *Stratagem: Deception and surprise in war*. Boston, MA: Artech House.