

Subject: A disciplined way to test whether isolated intrusions form one operation

Treat the first incident as a hypothesis trigger, not a conclusion: the defensible theory emerges when tools, people, money, timing, and independent records converge-and survives credible alternatives.

Subject: A disciplined way to test whether isolated intrusions form one operation

The Watergate chronology offers a useful investigative pattern for the access events you are examining-not as an attribution analogy, but as a model for how a seemingly bounded incident can change scale without requiring premature certainty.

The initial event was concrete: five people were arrested inside Democratic National Committee offices with surveillance equipment, burglary tools, sequentially numbered cash, cameras, film, and tear-gas guns. One suspect was also a paid security coordinator for President Nixon's reelection committee. Those were observations with relatively strong evidentiary footing. The early interpretation-that the operation was connected to Republican organizations-was contested by official denials, and investigators initially did not know the objective or who directed it.

The important move was to preserve that uncertainty while testing the broader hypothesis. By October 1972, FBI findings reportedly connected the break-in to a campaign-wide program of political spying and sabotage. The evidence expanded across several dimensions: targeting of all major Democratic presidential contenders, activity continuing since 1971, hundreds of thousands of dollars allegedly set aside for undercover work, at least 50 operatives, and links to the White House and Nixon's reelection committee. The theory became more defensible because independent relationship, duration, scope, and financial signals reinforced one another-not because one dramatic clue settled attribution.

For your current cases, I would structure the working model in three layers:

- Observation: what the artifact, account, infrastructure, financial record, or timeline directly establishes, with provenance and collection limits.
- Interpretation: what that observation makes more or less likely, including confidence and the assumptions required.

- Hypothesis: the broader explanation-shared operator, coordinated campaign, common sponsor, or unrelated activity-that must compete with alternatives.

The Watergate record also shows why decisive evidence can become a separate investigative problem. The discovery that Nixon routinely recorded conversations created a potential way to resolve conflicting accounts about when he knew of the cover-up. Nixon resisted release, invoking executive privilege and the private nature of the conversations. Investigators escalated from requests to subpoenas because the recordings were considered essential to a full inquiry. The Supreme Court ultimately held that a broad privilege claim yielded to a demonstrated, specific need for evidence in a pending criminal trial.

The operational implication is not that every collection gap warrants escalation. It is to identify which missing source could discriminate between competing explanations, document why it matters, and state what result would weaken the leading theory. A theory that cannot specify disconfirming evidence is closer to conjecture than analysis.

A practical next step is to build one cross-case timeline and relationship map, then mark each edge as verified, inferred, or assumed. Rank collection by discriminatory value: what would most clearly distinguish coordinated activity from coincidence? Keep the strongest alternative visible alongside the lead theory, and revise confidence only when corroboration crosses independent domains.