INTELLIGENCE · ANALYSIS AND TRADECRAFT

"Source Evaluation: Reliability, Access, and Corroboration"

Every intelligence judgement is only as good as the sources behind it. This article explains how analysts evaluate sources by their reliability, their access to the information and the degree to which independent sources corroborate it, and how the same principles apply to business research.

ModQu research article · 1,249 words · 13 references (APA 7th edition)

Intelligence is built from reports: a human source describes a meeting, a document reveals a plan, a website publishes a figure, a survey records what customers say. Before any of this can support a judgement, the analyst must ask how far it can be trusted. **Source evaluation** is the discipline of answering that question systematically. It rests on three ideas: the **reliability** of the source, the source's **access** to the information it reports, and **corroboration** by other, independent sources. This article explains each and shows how they apply beyond government intelligence.

Why source evaluation matters

Some of the most serious intelligence failures have turned on poorly evaluated sources. Before the 2003 Iraq war, American assessments of Iraqi biological weapons relied heavily on a single human source, later known by the code name "Curveball", whom American analysts had never met and whose reporting proved to be fabricated (Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005). The British review found that the validation of human sources had been inadequate and that some reporting was later withdrawn as unreliable (Butler, 2004). In both cases, the problem was not a lack of information but too much trust in information that had not been properly assessed.

Following these failures, the American intelligence community set out formal sourcing requirements. Intelligence Community Directive 206 requires analytic products to describe the quality and credibility of the sources on which key judgements rest, so that readers can judge for themselves how much weight to give them (Office of the Director of National Intelligence, 2015).

Reliability and credibility

The best-known grading system, widely used by NATO and police forces and often called the Admiralty system, assesses each report on two separate scales (Capet & Delavallade, 2014). The first grades the **reliability of the source**, based on its track record. The second grades the **credibility of the information**, based on whether it is confirmed by other sources and consistent with what is already known.

The two-part grading system for intelligence reports

Each report is graded on its source and, separately, on the information itself

Grade	Source reliability	Grade	Information credibility
A	Completely reliable	1	Confirmed by other sources
B	Usually reliable	2	Probably true
C	Fairly reliable	3	Possibly true
D	Not usually reliable	4	Doubtful
E	Unreliable	5	Improbable
F	Reliability cannot be judged	6	Truth cannot be judged

A report graded B2 comes from a usually reliable source and is probably true.

Based on the NATO 'Admiralty' system as described in Capet and Delavallade (2014); table by ModQu

ModQu.com

Figure 1. The two-part grading system. Separating the source from the information prevents a trusted source's error, or an unreliable source's accurate report, from being misjudged. Based on the NATO system as described in Capet and Delavallade (2014); table by ModQu.

Keeping the two scales separate is important. A usually reliable source can still pass on false information, perhaps because it was itself deceived; an unknown source can provide accurate information. Capet and Delavallade (2014) note several weaknesses in practice: grades are applied inconsistently by different analysts, the two scales are often merged in readers' minds, and the system says little about how to combine many graded reports into a judgement.

Breaking down credibility

Schum (1994), in work on evidence, offered a more detailed account of what makes testimony credible. Schum distinguished three attributes of a human source:

- **Veracity**: does the source believe what it reports, or is it lying?
- **Objectivity**: did the source form its belief on the basis of the evidence, or on what it expected or wanted to see?
- **Observational sensitivity**: were the source's senses and circumstances good enough to observe accurately?

A truthful source can still be wrong if it misunderstood what it saw or was too far away to see clearly. Asking about each attribute separately helps analysts locate where a report might have gone wrong. Vrij (2008) adds a caution: people are poor at judging veracity from demeanour, so assessments should rest on the content of reports and their consistency with other evidence rather than on impressions of honesty.

Access

Access is the question of how the source came to know what it reports. A source who attended a meeting has direct access; one who heard about it from a colleague has indirect access; one who read about it in the press has no special access at all. Pherson and Heuer (2021) stress that analysts should trace each piece of information as close to its origin as possible and ask whether the source was in a position to know.

Access also changes over time. A source who once worked inside an organisation may have lost contact with it. A report that describes plans in detail but comes from someone with no plausible route to that knowledge should raise suspicion, however reliable the source has been in the past.

Corroboration

Corroboration means confirmation by an independent source. The key word is independent. Heuer (1999) warned that analysts tend to give too much weight to the amount of information and too little to its diagnostic value. Several reports that agree may look like strong confirmation, but if they all trace back to a single original source, they add nothing to it. This is known as **circular reporting**.

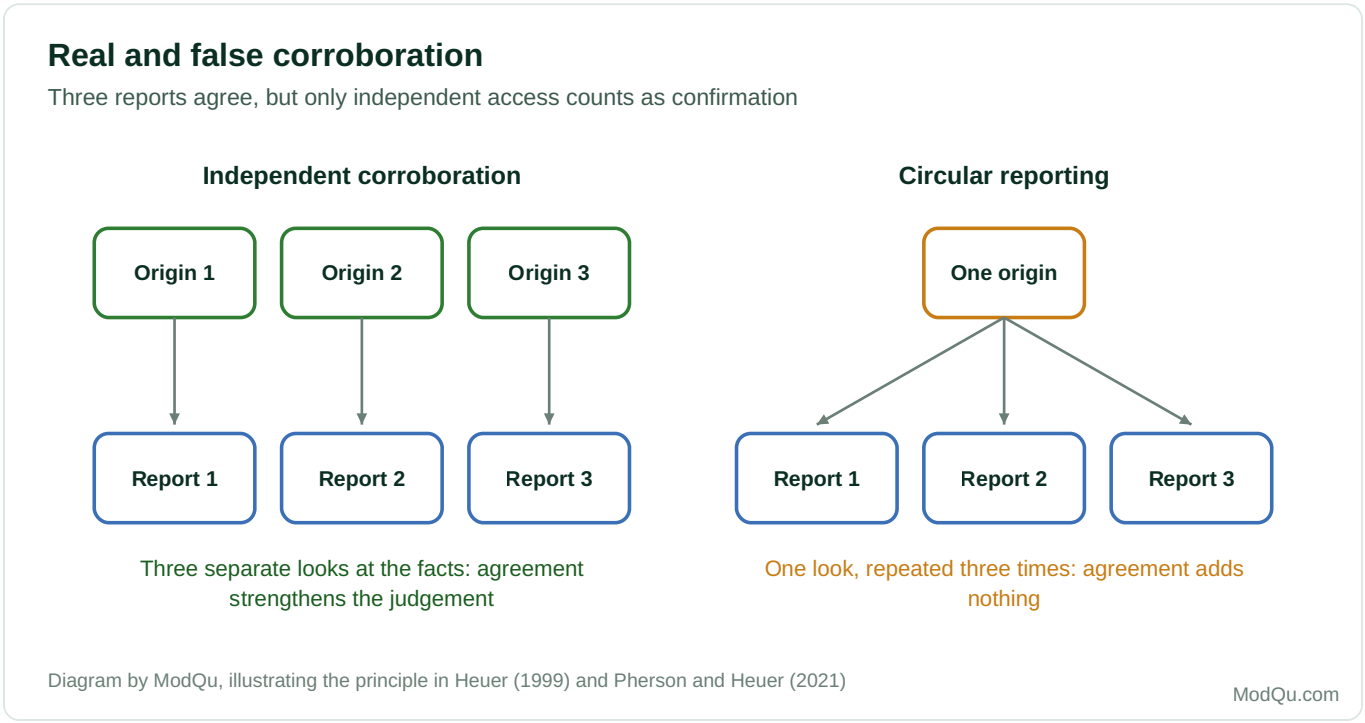


Figure 2. Real and false corroboration. Agreement between reports confirms a judgement only if the reports had independent access to the facts. Diagram by ModQu, illustrating the principle in Heuer (1999) and Pherson and Heuer (2021).

Circular reporting is common in the age of online media, where a single claim can be repeated by many websites within hours. Lowenthal (2022) notes that open sources are abundant but that their volume does not guarantee independent confirmation.

Evaluating open and online sources

Journalists and researchers have developed practical methods for evaluating online sources. Silverman (2014) sets out a verification routine: identify the original source, check when and where content was created, look for earlier versions and consider why it was published. Kovach and Rosenstiel (2014) describe a **discipline of verification** as the essence of journalism, distinguishing it from entertainment or propaganda.

Wineburg and McGrew (2019) compared how professional fact-checkers, historians and university students evaluated unfamiliar websites. The fact-checkers were far more accurate, largely because they practised **lateral reading**: instead of studying the website itself, they quickly left it to find out what other sources said about who was behind it. Metzger et al. (2010) showed that most people instead rely on surface cues, such as professional design or the number of others sharing content, which are easy to fake.

Applying the principles in business

Businesses evaluate sources constantly: market reports, competitor gossip, customer feedback, analyst commentary and online reviews. The same three questions apply.

1. **Reliability.** Has this source been accurate before? Is it a reputable research organisation, a trade publication with a good record or an anonymous post?
2. **Access.** How would this source know? A distributor may know a rival's shipment volumes; a journalist may only be repeating a press release.
3. **Corroboration.** Is the information confirmed by a source with independent access? Several news articles quoting the same company statement are one source, not several.

For survey data, the equivalent questions concern sampling, question design and data quality: who answered, whether they were in a position to know, and whether the results agree with other evidence such as sales figures.

Common mistakes

- **Trusting the source and not the report.** Even reliable sources make mistakes.
- **Counting reports rather than origins.** Ten echoes of one rumour are still one rumour.
- **Losing the grading.** Caveats about sources often disappear as judgements are summarised (Butler, 2004).
- **Judging by appearance.** Professional presentation is not evidence of accuracy.

Conclusion

Source evaluation asks three questions of every report: is the source reliable, did it have access, and is the information confirmed by someone else with independent access? Formal grading systems help, though they are applied inconsistently. The underlying discipline is simple to state and hard to practise: trace information to its origin, assess each link in the chain and count only independent confirmation as corroboration.

References

Butler, R. (2004). *Review of intelligence on weapons of mass destruction* (HC 898). The Stationery Office.

Capet, P., & Delavallade, T. (Eds.). (2014). *Information evaluation*. ISTE; Wiley.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. (2005). *Report to the President of the United States*. U.S. Government Printing Office.

Heuer, R. J., Jr. (1999). *Psychology of intelligence analysis*. Center for the Study of Intelligence, Central Intelligence Agency.

Kovach, B., & Rosenstiel, T. (2014). *The elements of journalism: What newspeople should know and the public should expect* (3rd ed.). Three Rivers Press.

Lowenthal, M. M. (2022). *Intelligence: From secrets to policy* (9th ed.). CQ Press.

Metzger, M. J., Flanagin, A. J., & Medders, R. B. (2010). Social and heuristic approaches to credibility evaluation online. *Journal of Communication, 60*(3), 413–439. https://doi.org/10.1111/j.1460-2466.2010.01488.x

Office of the Director of National Intelligence. (2015). *Intelligence Community Directive 206: Sourcing requirements for disseminated analytic products*.

Pherson, R. H., & Heuer, R. J., Jr. (2021). *Structured analytic techniques for intelligence analysis* (3rd ed.). CQ Press.

Schum, D. A. (1994). *The evidential foundations of probabilistic reasoning*. Wiley.

Silverman, C. (Ed.). (2014). *Verification handbook: A definitive guide to verifying digital content for emergency coverage*. European Journalism Centre.

Vrij, A. (2008). *Detecting lies and deceit: Pitfalls and opportunities* (2nd ed.). Wiley.

Wineburg, S., & McGrew, S. (2019). Lateral reading and the nature of expertise: Reading less and learning more when evaluating digital information. *Teachers College Record, 121*(11), 1–40.