INTELLIGENCE · CONCEPTS AND HISTORY

Lessons for Business From the History of State Intelligence

Governments have spent a century learning, often painfully, how to collect, analyse and use intelligence. This article draws eight lessons from that history, from Pearl Harbor to Iraq, and shows how each applies to companies trying to understand markets, competitors and risks.

ModQu research article · 2,027 words · 22 references (APA 7th edition)

State intelligence services are among the most studied information organisations in the world. When they fail, the consequences can be catastrophic, and the failures are often examined by commissions, historians and scholars in great detail. The result is a large body of evidence about why organisations misread their environment and what helps them read it better. Businesses face many of the same problems: incomplete information, competitors who conceal their plans, internal politics that distort analysis and leaders who hear what they want to hear. Calof and Wright (2008) note that competitive intelligence as a field has drawn heavily on government practice, but the most useful transfers are often the lessons from failure rather than the techniques of collection. This article draws eight such lessons and shows how each applies to business.

1. Warnings are usually present; the problem is recognising them

The classic study of intelligence failure is Wohlstetter's (1962) analysis of the Japanese attack on Pearl Harbor in 1941. Wohlstetter found that American agencies had collected many signals pointing to an attack, including intercepted diplomatic messages, but that these signals were scattered across organisations and surrounded by a much larger volume of irrelevant or misleading information, which Wohlstetter called noise. The signals made sense only in hindsight, once the attack had shown which ones mattered.

The 9/11 Commission reached a similar conclusion about the attacks of September 2001. It found that pieces of relevant information were held by different agencies but never brought together, and it famously described the most important failure as one of imagination: officials had not seriously considered that terrorists might use hijacked airliners as weapons (National Commission on Terrorist Attacks Upon the United States, 2004). Zegart (2007) argues that the deeper cause was organisational: agencies built for the Cold War had failed to adapt their structures, incentives and cultures to a new kind of threat.

For business: Disruptive competitors, shifts in customer behaviour and supply chain risks usually announce themselves through weak signals: a few customers asking about a new product, an unusual pattern of hiring by a rival, a supplier's late payments. These signals are often visible somewhere in the organisation, in sales notes, customer service logs or procurement records, but they are rarely assembled. Grabo (2002), writing about strategic warning, stresses that warning depends on systematically tracking indicators and having someone responsible for putting them together.

2. Assumptions are more dangerous than missing facts

In September 1962 the American intelligence community judged that the Soviet Union was unlikely to place offensive missiles in Cuba, largely because doing so would be out of character and too risky. The judgement was wrong. Allison (1969) showed how different assumptions about how governments make decisions lead to different readings of the same evidence. Jervis (2010), studying the Central Intelligence Agency's failure to anticipate the Iranian revolution of 1979 and its mistaken assessment of Iraq's weapons programmes before 2003, concluded that the core problem in both cases was not a shortage of information but unexamined assumptions that shaped how the information was read.

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (2005) found that analysts had worked from the assumption that Iraq was continuing its programmes and had interpreted ambiguous evidence in that light, without asking what the evidence would look like if the assumption were false. The British Butler review of the same intelligence reached comparable conclusions about the weight placed on a small number of sources (Butler, 2004).

For business: Many strategic failures rest on assumptions no one stated: that customers will not switch, that a new technology is too expensive to matter, that a competitor will behave as it always has. Pherson and Heuer (2021) recommend a **key assumptions check**: listing the assumptions behind a judgement, asking how confident one is in each and what would happen if it were wrong. It is one of the cheapest and most effective analytic tools available to any business.

3. Some failure is inevitable; design for resilience

Betts (1978), in one of the most cited articles in intelligence studies, argued that intelligence failures are inevitable. Evidence is ambiguous, adversaries deceive, and every reform designed to fix one kind of failure creates vulnerabilities elsewhere. Making analysts more sensitive to warning produces more false alarms; making them more cautious produces more missed threats.

For business: No market intelligence system will foresee every competitive move or demand shock. The appropriate response is not to promise certainty but to build resilience: decisions that perform reasonably across several possible futures, early indicators that trigger review, and the flexibility to change course quickly when a surprise occurs.

4. Say how likely, in numbers

Kent (1964) discovered that colleagues who had agreed on the phrase "serious possibility" in an estimate interpreted it as anything from roughly a one-in-five to a four-in-five chance. Friedman and Zeckhauser (2012) argue that vague language about uncertainty remains one of the main weaknesses of intelligence reporting. Research from forecasting tournaments funded by the American intelligence community showed that well-trained people who give explicit probabilities can forecast political events with measurable and improvable accuracy (Mellers et al., 2014; Tetlock & Gardner, 2015).

For business: Phrases such as "likely", "possible" and "significant risk" in board papers and market reports are read very differently by different people. Agreeing on numerical ranges for probability words, or simply stating probabilities, makes judgements clearer, allows them to be checked against outcomes and improves accountability.

5. Keep score and learn

The forecasting tournaments also showed that accuracy improves when forecasts are scored and forecasters receive feedback. Kahneman and Klein (2009) argue that expert intuition can be trusted only in environments that are regular enough to learn from and where experts receive timely feedback on their judgements. Much intelligence work, and much business strategy, lacks that feedback: forecasts are made, decisions are taken and no one checks afterwards how accurate the forecasts were. Dhami et al. (2015) argue that intelligence agencies should borrow from decision science by measuring the accuracy of their judgements systematically.

For business: Keep a record of important forecasts, such as sales projections, competitor responses and project timelines, with explicit probabilities, and review them when outcomes are known. The aim is not to blame individuals but to learn which methods and sources produce reliable judgements.

Eight lessons from state intelligence

What governments learned the hard way, and how businesses can use it

Lesson	Historical case	Business application
1. Warnings are present but unrecognised	Pearl Harbor; 9/11	Assemble weak signals from sales, service and procurement
2. Assumptions mislead more than gaps	Cuba 1962; Iraq 2002	Run a key assumptions check before big decisions
3. Some failure is inevitable	Betts (1978)	Build decisions that survive several futures
4. Say how likely, in numbers	Kent's 'serious possibility'	Agree probability ranges for words like 'likely'
5. Keep score and learn	Forecasting tournaments	Record forecasts and review them against outcomes
6. Build in challenge	Bay of Pigs	Use devil's advocates and competitor role-play
7. Protect analysis from wishes	Iraq dossier caveats lost	Separate analysis from advocacy; reward bad news
8. Organisation matters	Agencies not sharing	Name owners; share one repository

Compiled from Wohlstetter (1962), Betts (1978), Kent (1964), Janis (1972), Jervis (2010) and others cited in the text

ModQu.com

Figure 1. Eight lessons from state intelligence and how they apply in business. Compiled from the sources cited in the text; table by ModQu.

6. Beware groupthink and the pressure to agree

Janis (1972) coined the term **groupthink** for the tendency of cohesive groups to suppress doubts and converge on a shared view, using cases such as the failed Bay of Pigs invasion of Cuba in 1961, in which a small group of advisers approved a plan whose flaws were apparent to outsiders. Intelligence reviews of the Iraq weapons assessments found related problems: a shared assumption went unchallenged across agencies and countries.

Intelligence services have developed structured ways to introduce challenge, including devil's advocacy, red teams that argue the adversary's case, and analysis of competing hypotheses, which forces analysts to test every plausible explanation against the evidence (Heuer, 1999; Pherson & Heuer, 2021).

For business: Before a major decision, assign someone to argue the opposite case seriously, or ask a small team to play the role of a key competitor and predict how it will respond. These methods cost little and surface weaknesses that a harmonious planning team might miss.

7. Protect analysis from the answer the boss wants

Davis (2006) describes the tension between analysts and policymakers as inherent: policymakers want support for their plans, while analysts are supposed to tell them unwelcome truths. When analysts become too close to their users, or are rewarded for agreeing with them, intelligence becomes politicised. The Butler review warned about the way caveats in intelligence assessments were lost when material was used to make a public case (Butler, 2004).

For business: Market and competitor analysis is equally vulnerable. Analysts who know that the chief executive favours an acquisition, or that the sales director has promised growth, face pressure to shade their conclusions. Clear separation between analysis and advocacy, and leaders who reward honest bad news, are the main protections.

8. Organisation matters as much as method

Ghoshal and Kim (1986), studying intelligence systems in large companies, found that many firms gathered extensive environmental information but failed to deliver it in a form that shaped decisions at the top. Zegart (2007) and the 9/11 Commission showed the same pattern in government: information held in one part of an organisation never reached the people who needed it. Treverton (2003) argues that in an age of abundant information the scarce resource is not data but the attention and analysis needed to make sense of it.

For business: Who owns intelligence? Who makes sure that what the sales team hears reaches the strategy team, and that what the strategy team concludes reaches the sales team? Many companies have analysts in finance, marketing, sales operations and strategy who rarely talk to each other. Simple measures, such as a shared repository, a regular cross-functional intelligence meeting and a named owner for each key intelligence topic, often add more value than new data sources.

Putting the lessons together: an illustration

Consider a hypothetical mid-sized retailer of home furnishings that wants to know whether an online competitor will expand into its main regional market. A traditional approach would ask an analyst to produce a profile of the competitor, perhaps once a year, and present it at a strategy meeting. Applying the lessons above changes the work in several ways.

First, the retailer defines a short list of **indicators** that would signal expansion: warehouse leases in the region, job advertisements for local delivery staff, targeted online advertising to local postcodes, and changes in delivery promises on the competitor's website. Store managers, the property team and the marketing team are asked to report any of these when they see them, and one analyst is responsible for assembling the reports (lessons 1 and 8).

Second, the strategy team writes down the **assumptions** behind its current plan, including that the competitor's delivery costs make the region unprofitable for it, and asks what evidence would show each assumption to be wrong (lesson 2).

Third, the analyst states a **probability**: for example, a 35% chance that the competitor opens a regional distribution centre within eighteen months. The figure is recorded, together with the reasoning, and reviewed every quarter as indicators arrive (lessons 4 and 5).

Fourth, a small group is asked to **play the competitor** for an afternoon and decide how it would enter the market, which reveals an option the strategy team had not considered: partnering with an existing local logistics firm rather than building its own warehouse (lesson 6).

Finally, the retailer plans a response that would work whether or not the competitor arrives, such as improving its own delivery times, rather than staking everything on a single forecast (lesson 3), and the chief executive makes clear that an analysis showing a higher risk than expected is welcome (lesson 7). None of these steps requires secret information or large budgets; all of them reflect what state intelligence learned at great cost.

Caution about borrowing

Not every government practice transfers well. State intelligence relies heavily on secret collection, which is neither legal nor appropriate for companies seeking information about competitors. Classification and compartmentalisation, which protect sources in government, can stifle the sharing that businesses need. And the scale of government intelligence, with its specialised agencies and large analytic staffs, has no counterpart in most firms. The lessons that transfer best are about thinking and organising, not about collecting secrets.

Conclusion

The history of state intelligence is largely a history of learning from failure. Its central lessons are that warning signs are usually present but unrecognised, that hidden assumptions mislead more than missing facts, that uncertainty must be stated clearly, that judgements should be scored and learned from, that challenge must be built in, that analysis must be protected from the wishes of its users, and that organisation determines whether knowledge reaches decision-makers. Businesses can apply all of these lessons with modest effort and without any secret sources.

References

Allison, G. T. (1969). Conceptual models and the Cuban missile crisis. *American Political Science Review, 63*(3), 689–718. https://doi.org/10.2307/1954423

Betts, R. K. (1978). Analysis, war, and decision: Why intelligence failures are inevitable. *World Politics, 31*(1), 61–89. https://doi.org/10.2307/2009967

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

Calof, J. L., & Wright, S. (2008). Competitive intelligence: A practitioner, academic and inter-disciplinary perspective. *European Journal of Marketing, 42*(7/8), 717–730. https://doi.org/10.1108/03090560810877114

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.

Davis, J. (2006). Intelligence analysts and policymakers: Benefits and dangers of tensions in the relationship. *Intelligence and National Security, 21*(6), 999–1021. https://doi.org/10.1080/02684520601046325

Dhami, M. K., Mandel, D. R., Mellers, B. A., & Tetlock, P. E. (2015). Improving intelligence analysis with decision science. *Perspectives on Psychological Science, 10*(6), 753–757. https://doi.org/10.1177/1745691615598511

Friedman, J. A., & Zeckhauser, R. (2012). Assessing uncertainty in intelligence. *Intelligence and National Security, 27*(6), 824–847. https://doi.org/10.1080/02684527.2012.708275

Ghoshal, S., & Kim, S. K. (1986). Building effective intelligence systems for competitive advantage. *Sloan Management Review, 28*(1), 49–58.

Grabo, C. M. (2002). *Anticipating surprise: Analysis for strategic warning*. Joint Military Intelligence College.

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

Janis, I. L. (1972). *Victims of groupthink: A psychological study of foreign-policy decisions and fiascoes*. Houghton Mifflin.

Jervis, R. (2010). *Why intelligence fails: Lessons from the Iranian Revolution and the Iraq War*. Cornell University Press.

Kahneman, D., & Klein, G. (2009). Conditions for intuitive expertise: A failure to disagree. *American Psychologist, 64*(6), 515–526. https://doi.org/10.1037/a0016755

Kent, S. (1964). Words of estimative probability. *Studies in Intelligence*, *8*(4), 49–65.

Mellers, B., Ungar, L., Baron, J., Ramos, J., Gurcay, B., Fincher, K., Scott, S. E., Moore, D., Atanasov, P., Swift, S. A., Murray, T., Stone, E., & Tetlock, P. E. (2014). Psychological strategies for winning a geopolitical forecasting tournament. *Psychological Science, 25*(5), 1106–1115. https://doi.org/10.1177/0956797614524255

National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission report*. W. W. Norton.

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

Tetlock, P. E., & Gardner, D. (2015). *Superforecasting: The art and science of prediction*. Crown.

Treverton, G. F. (2003). *Reshaping national intelligence for an age of information*. Cambridge University Press.

Wohlstetter, R. (1962). *Pearl Harbor: Warning and decision*. Stanford University Press.

Zegart, A. B. (2007). *Spying blind: The CIA, the FBI, and the origins of 9/11*. Princeton University Press.