Red-Teaming Thinking

Idea In Short

Before committing to a major strategy, assign a small group outside the planning team to attack it. Give the group a written mandate, a deadline of two to three weeks, direct access to the executive sponsor, and an obligation to report what it finds, including unwelcome conclusions. Require the sponsor to answer each finding in writing by accepting it, rejecting it with reasons, or deferring it with a date. The exercise exposes unexamined assumptions, tests the plan from a competitor's viewpoint, and builds a record of why leaders proceeded. Reserve it for decisions that are costly to reverse, and protect the people who deliver the criticism from any penalty.

Every plan reflects the assumptions of the people who wrote it. Those people also review it, defend it, and eventually commit money to it, which explains why flaws survive so well. Red teaming offers a remedy by asking someone else to attack the plan before reality does. The practice began in military and intelligence settings, and it has moved into corporate strategy, cybersecurity, and public policy. This article traces its history, explains what the term covers, and shows how leaders can set up a red team that changes decisions rather than decorating them.

Where red teaming comes from

The approach took shape in the United States in the early 1960s, when the RAND Corporation ran Cold War simulations for the military and labeled the Soviet side red and the American side blue.1 Israel supplied a second root after the surprise of the 1973 Yom Kippur War. Its Intelligence Directorate formed a unit called Ipcha Mistabra, a phrase that roughly means on the contrary, and assigned it to produce contrarian, unorthodox readings of intelligence reports so that discarded assumptions would be revisited. After the Iraq War, red teaming spread in the United States Army, which created its first service-level red team in 2004. The practice then reached corporations, government agencies, and nonprofits, and it became especially common in cybersecurity.

Two meanings of the term

The same words describe two different activities. One is the vulnerability probe, in which a team simulates an attack to test defenses, as in penetration tests of computer networks. The other is decision-support red teaming, also called alternative analysis, in which a team challenges a plan, an assessment, or a strategy to improve the decision behind it. Business leaders usually need the second. A probe asks whether the walls hold. Decision support asks whether the plan inside the walls makes sense. The two share methods, but they answer different questions and they require different skills from the people involved.

What a formal definition requires

The United Kingdom's Ministry of Defence publishes a handbook that defines red teaming as the independent use of structured, creative, and critical thinking techniques to help an end user make a better-informed decision or produce a more robust product.2 Two words in that definition carry weight. Independent means the team does not report to the planners it evaluates. Structured means the work follows techniques rather than opinion. The handbook lists several purposes:

- Uncover hidden biases
- Challenge assumptions and beliefs
- Identify flaws in logic
- Widen the search for information
- Identify alternative options
- Stress-test a plan
- Understand the situation from an adversary's or stakeholder's perspective

The same publication separates a red team from a red team mindset. The mindset is a habit of applying quick challenge techniques to everyday problems at every level, while a red team is a separate group that tackles complex problems over several hours or longer.

Techniques any team can borrow

The handbook names methods that fit ordinary meetings. One rule has everyone speak once before anyone speaks twice, with senior people speaking last so that their views do not anchor the room. An assumptions check lists each belief the plan depends on and rates how

well the evidence supports it. What-if analysis imagines pathways to failure, and high impact, low probability analysis looks at events that are unlikely but would be damaging. Devil's advocacy assigns someone the explicit task of arguing the other side. Practitioner workbooks add simple routines such as writing individually before sharing, which reduces groupthink by protecting each person's view before the group begins to converge.3

Why leaders resist

Micah Zenko of the Council on Foreign Relations summarized several observations from conversations with officials and executives. Many say they value critical thinking but rarely encourage it, because they believe they already understand their organizations or expect early warning of problems. Leaders accept red teaming of workflows and daily tasks but resist scrutiny of the underlying ideas, analogies, and assumptions behind the institution. Organizations also find it easier to study outside rivals than to examine themselves, and they invest heavily in the first while neglecting the second.4 The result is a gap between stated openness and actual practice. A chief executive who says she welcomes challenge but never funds a dissenting voice has already answered the question.

Building a red team that works

A policy paper from Vanderbilt University's institute on national security argues that strategic failures often come from institutional blind spots and groupthink rather than a shortage of information. Its examples are the 2003 invasion of Iraq and the October 2023 Hamas attacks, where, the paper contends, decision makers had extensive intelligence but did not sufficiently challenge prevailing narratives. Its remedies apply well beyond government. Red teams should be built into decision structures rather than treated as symbolic exercises, operate as independent units with direct access to senior leadership, and hold a clear mandate to deliver unwelcome findings.5 Corporate leaders can translate those points directly. Give the group a written charter, protect its members from retaliation, and require the sponsor to respond to each finding.

An illustration from retail

Imagine a retailer preparing to enter a new region with forty stores. The planning team has built a case around brand awareness, store economics, and supplier terms. A red team of four people from finance, operations, and a rival's former staff receives the plan for two

weeks. It writes the competitor's response in detail: a price cut in the ten most contested locations, an exclusive supplier agreement, and a loyalty offer aimed at the retailer's first customers. It also tests the assumptions, finding that the plan counts on a labor pool that two other employers are already recruiting.

The sponsor must answer each finding. She accepts the labor concern and adds a hiring plan, rejects the supplier concern with documented evidence, and defers the price response to a review after the first six months. The plan changes in three places, and the record shows why.

A working cadence

A short sequence keeps the practice credible and limits the burden on the sponsor. Across the whole engagement, she needs to spend only a few hours: briefing the reviewers, hearing their report, and writing her response. The charter should also state what the red team may not do, such as contacting customers or circulating drafts, so that confidentiality is protected. The steps are:

1. Choose a decision that is costly to reverse and name the sponsor
2. Write a charter that states the scope, the deadline, and the right to deliver unwelcome findings
3. Select three to five reviewers from outside the planning team
4. Give the group the plan and allow direct questions to its authors
5. Receive a written report and respond to every finding in writing
6. Record which changes were made and which findings were rejected

The reviewers should be given the same material the board will see, no more and no less, so that their findings reflect the real decision. Review the record twice a year. If the red team never changes anything, the cause may be a charter that is too timid or a sponsor who is not listening. If it finds many flaws, the planning process upstream deserves attention.

Limits and risks

Red teaming costs time and attention, and it can feed a culture of suspicion if it is used on every decision. Reserve it for the few that are hard to reverse. A red team can also be captured, drifting toward the planners' views because they supply its information and

control its careers. Rotating membership and reporting to the sponsor's superior help. Finally, the exercise can degrade into ritual when nobody has to answer its findings. The written response requirement guards against that, because it forces the sponsor to treat the work as a decision input rather than a formality.

- 1Red team
- 2Red teaming handbook
- 3Introduction to red team thinking workbook
- 4Five red team insights for leaders and practitioners
- 5Breaking the cycle of strategic failure: why national security needs empowered red teams now

Summary

Red teaming works when an organization accepts that its own planners cannot see every flaw in what they build. The value comes from independence, a clear mandate, and a sponsor who answers findings in writing. Without those conditions the exercise becomes a ritual that produces nothing but a slide. With them, leaders gain an honest view of how a competitor, a regulator, or a skeptical customer would read the plan, along with time to adjust. Use the technique on the few decisions that cost most to reverse, keep the group small, and judge it by whether the plan changed or the decision to proceed became better documented.