

ANALYTIC TRADECRAFT

INTELLIGENCE · LAW ENFORCEMENT · CRIME ANALYSIS · INVESTIGATION

STEALING FROM THE SPOOKS

A Monograph on Structured Analytic Techniques for Law Enforcement Crime Analysis, Adapting the Tradecraft of the Intelligence Community to Criminal Investigation, Pattern Analysis, and Charging Review

Prepared for the Analysts, Investigators, and Prosecutors of
the Law Enforcement Community

by

C. Constantin Poindexter

MA IN INTELLIGENCE, JD, GRADUATE CERTIFICATE IN COUNTERINTELLIGENCE,
NICCS OSINT CERTIFICATION, CCI

FORMER U.S. INTELLIGENCE COMMUNITY OPERATOR
FORMER CERTIFIED LAW ENFORCEMENT OFFICER (NC DOJ)

First Edition · November 2026

San Juan, Puerto Rico

Copyright 2026 C. Constantin Poindexter. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the author, except for brief quotations in reviews or scholarly works with attribution. No copyright is claimed in works of the United States Government summarized or cited here.

This publication is offered for the professional education of crime analysts, investigators, supervisors, and prosecutors. It is not legal advice, it creates no attorney client relationship, and it is no substitute for agency policy or for the advice of the prosecuting authority in a particular case. Rules of discovery, disclosure, and evidence vary by jurisdiction and change over time. Verify every legal authority against current official sources before relying on it.

The views expressed are the author's own and do not represent the position of any agency of the United States Government. Everything here is drawn from unclassified, publicly available sources. The case scenarios, registers, logs, and matrices that are not attributed to a source are hypothetical illustrations composed for teaching. They describe no real investigation.

Table of Contents

A Note on Sources and Credit 7

Preface 8

PART I. Foundations 9

Chapter 1. The Problem Is Not Data. The Problem Is Your Brain. 10

1.1 The diagnosis 10

1.2 Tunnel vision is a mind-set with a badge 10

1.3 The biases, translated 11

1.4 Why knowing about bias is not enough 11

Chapter 2. Why Policing Should Steal This 12

2.1 The Intelligence Community paid retail for these lessons 12

2.2 Same failure mode, different uniform 12

2.3 Three differences that raise the stakes 13

2.4 What the techniques are, and what they are not 13

PART II. Diagnostic Techniques: Making the Argument Visible 15

Chapter 3. Key Assumptions Check 16

3.1 What the primer says 16

3.2 The primer's case study: the Washington sniper 16

3.3 What the case teaches beyond the primer 17

3.4 The application to crime analysis 17

3.5 A worked register 17

3.6 How to run it 18

3.7 Where it goes wrong 18

Chapter 4. Quality of Information Check 19

4.1 What the primer says 19

4.2 The application to policing 19

4.3 Recalled reporting is the Brady problem seen from the analyst's chair 20

4.4 A worked source log 21

4.5 How to run it 21

4.6 Where it goes wrong 22

Chapter 5. Indicators or Signposts of Change 22

5.1 What the primer says 22

5.2 The application to crime analysis 22

5.3 A worked list 23

5.4 Other uses 23

5.5 How to run it 23

5.6 Where it goes wrong 24

Chapter 6. Analysis of Competing Hypotheses 24

6.1 What the primer says 24

6.2 Diagnosticity 25

6.3 The application to investigation 25
6.4 A worked matrix 25
6.5 The matrix as a record 27
6.6 How to run it 27
6.7 Where it goes wrong 27

PART III. Contrarian Techniques: Institutionalized Disagreement 28

Chapter 7. Devil's Advocacy 29
7.1 What the primer says 29
7.2 The application: a standing devil's advocate 29
7.3 How to run it 29
7.4 Label it 30
7.5 Where it goes wrong 30

Chapter 8. Team A/Team B 31
8.1 What the primer says 31
8.2 The application 31
8.3 How to run it in a week 32
8.4 Where it goes wrong 32

Chapter 9. High-Impact/Low-Probability Analysis 32
9.1 What the primer says 32
9.2 The application 33
9.3 A worked pathway 33
9.4 How to run it, and where it goes wrong 34

Chapter 10. "What If?" Analysis 34
10.1 What the primer says 34
10.2 The application 35
10.3 How to run it 35
10.4 How it differs from its neighbors 35

PART IV. Imaginative Techniques: Getting Outside the Building, the Box, or Whatever the Hell You Want to Call It 36

Chapter 11. Brainstorming 37
11.1 What the primer says 37
11.2 The application 37
11.3 How to run it 37
11.4 Where it goes wrong 38

Chapter 12. Outside-In Thinking 38
12.1 What the primer says 38
12.2 The application 39
12.3 How to run it 39
12.4 Where it goes wrong 39

Chapter 13. Red Team Analysis 40
13.1 What the primer says 40

13.2 The application 40
13.3 How to run it 41
13.4 Cautions 41

Chapter 14. Alternative Futures Analysis 42
14.1 What the primer says 42
14.2 The application 42
14.3 How to run it 43
14.4 Where it goes wrong 43

PART V. Putting It to Work 45

Chapter 15. Sequencing the Techniques Across the Life of a Case 46
15.1 The primer's timeline 46
15.2 The same timeline on a major case 46
15.3 If you only have an hour 47

Chapter 16. Discovery, Disclosure, and the Witness Stand 47
16.1 Assume the defense will read it 48
16.2 That is a feature 48
16.3 Writing analytic products for a courtroom reader 48
16.4 The warrant affidavit 49
16.5 The analyst as a witness 49
16.6 Settle the protocol with the prosecutor first 50

Chapter 17. Limits and Honest Cautions 50
17.1 The techniques guarantee nothing 50
17.2 The evidence base is thinner than the enthusiasm 50
17.3 A matrix is not evidence 50
17.4 Process theater 50
17.5 Contrarianism can paralyze 51
17.6 Culture eats technique 51

Chapter 18. Standing It Up in a Department 51
18.1 A one page directive 51
18.2 Who does what 52
18.3 Training 52
18.4 The first ninety days 52
18.5 Measuring whether it works 53
18.6 Small agencies 53

Conclusion 53

Appendix A. The Twelve Techniques at a Glance 54

Appendix B. Worksheets 55
B.1 Assumptions register 55
B.2 Source log 56
B.3 Competing hypotheses matrix 57
B.4 Indicator list 58
B.5 Devil's advocate memorandum 59

Appendix C. A Supervisor's Checklist Before Charging 60

References 61

Books, articles, and reports 61

Cases 62

Statutes and rules 62

About the Author 63

A Note on Sources and Credit

This monograph stands on someone else's foundation. The reader is entitled to know exactly where the borrowed stone ends and my own construction begins.

What belongs to the primer. The twelve structured analytic techniques, their grouping into diagnostic, contrarian, and imaginative families, the method steps for each, and the suggested timeline for using them all come from *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*, prepared by the US Government and published in March 2009. So do several of the illustrations discussed here: the Key Assumptions Check applied to the 2002 Washington sniper shootings, the competing hypotheses matrix on the 1995 Tokyo subway attack, the 1941 State Department odds on war with Japan, and the 1990 estimate on Yugoslavia. Wherever I report what the primer says, I cite it by page as (US Government 2009).

What belongs to Richards Heuer. The primer in turn credits Richards J. Heuer, Jr., whose *The Psychology of Intelligence Analysis* (1999) supplied the cognitive diagnosis and the Analysis of Competing Hypotheses. The insight that analysts fail because of how minds process information, and not for want of information, is Heuer's. I claim none of it.

What is mine. The argument that this body of tradecraft belongs in police work, and everything built to prove it. That includes the translation of each technique into the vocabulary and workflow of criminal investigation and crime analysis; the policing scenarios, assumptions registers, source logs, indicator lists, and matrices; the mapping of the primer's timeline onto the life of a major case; the treatment of discovery, disclosure, and cross examination; the cautions; and the program for standing the discipline up inside a department. Where I lean on the wrongful conviction, forensic science, and intelligence studies literature to support those arguments, the sources are cited in the text and collected in the References.

An earlier and much shorter version of this argument appeared on my blog in September 2026 under the same title.

Preface

Police departments do not have a data problem. They have body cameras, license plate readers, gunshot detection, cell site records, and records management systems holding decades of reports. They have analysts who can map all of it before lunch. What they have, and what no procurement cycle will ever fix, is a thinking problem. The same problem put the United States Intelligence Community on the wrong side of Pearl Harbor, the Yalu River, and Iraq's weapons programs.

The Intelligence Community responded to its humiliations by writing down how its analysts ought to think, and then by drilling it. The most compact statement of that discipline is a forty page unclassified primer published in 2009. It was written for people who track missile programs and terrorist cells. It reads as though it were written for a detective sergeant staring at a whiteboard covered in string.

This monograph takes that primer apart, technique by technique, and rebuilds it for law enforcement. It is written for four readers:

- **The crime analyst**, tactical, strategic, or intelligence, who already senses that the squad's theory is running ahead of its evidence and needs a professional way to say so.
- **The investigator**, who wants cases that hold up in week three, at the preliminary hearing, and on appeal.
- **The supervisor**, who signs off on charging recommendations and would like to know what was assumed before the settlement conference instead of after it.
- **The prosecutor and the conviction integrity reviewer**, who inherit whatever the investigation did or did not think about.

Part I sets out the diagnosis and the case for borrowing. Parts II, III, and IV take the twelve techniques in the primer's own order. Every chapter follows the same plan: what the primer says, how the technique translates to police work, how to run it with the people and hours a real unit has, and where it goes wrong. Part V puts the techniques in sequence across the life of a case, deals squarely with discovery and the witness stand, states the limits, and offers a program for adoption. The appendices hold a quick reference, blank worksheets, and a supervisor's checklist.

A word on tone. I have not sanded the edges off the prose. The subject is how competent, well meaning investigators convict the wrong man and miss the right one. It does not deserve to be discussed in the passive voice.

PART I

Foundations

Chapter 1. The Problem Is Not Data. The Problem Is Your Brain.

1.1 The diagnosis

In March 2009 the US Government published a slim, unclassified volume titled *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*. Its central diagnosis, borrowed from Richards Heuer, is blunt. Analysts do not fail for lack of information. They fail because human beings process information through mental models that decide, before conscious thought kicks in, which facts get noticed and which get quietly binned (US Government 2009, 1; Heuer 1999).

The primer lists the risks of a settled mind-set with clinical economy. Analysts perceive what they expect to perceive. A mind-set, once formed, resists change. New information gets absorbed into the existing model, sometimes wrongly. Information that conflicts with the model is dismissed or ignored (US Government 2009, 1).

The primer's most damning observation is that experience makes this worse, not better. Seasoned analysts may be more vulnerable precisely because their expertise and their past successes taught them to trust the model (US Government 2009, 1). The veteran is not immune. The veteran is the high risk population.

1.2 Tunnel vision is a mind-set with a badge

Anyone who has worked a homicide unit will recognize that description. It is a clinical portrait of tunnel vision.

The wrongful conviction literature has been saying the same thing in its own vocabulary for a quarter century. Findley and Scott (2006) describe tunnel vision as a bundle of ordinary heuristics and institutional pressures that lead investigators to settle on a suspect, then select and filter evidence to build the case while discounting whatever points elsewhere. They stress that it is the product of normal cognition and not of malice. That is exactly Heuer's point transplanted into a squad room. Rossmo (2009) catalogs the same pattern across failed investigations: premature judgment, confirmation bias, groupthink, and a refusal to revisit the first theory.

The body count is public. The National Registry of Exonerations has documented more than three thousand exonerations in the United States since 1989. The files are a graveyard of cases in which investigators locked onto a suspect in the first seventy-two hours and then spent months unconsciously bending every new fact to fit.

The disease is not confined to detectives. In 2004 the FBI Laboratory identified a latent fingerprint from the Madrid train bombings as belonging to Brandon Mayfield, an Oregon lawyer who had not left the country. Multiple examiners concurred. The Spanish National Police disagreed and were right. The Inspector General later found that the examiners reasoned backward from Mayfield's known print to the latent, that verification was not independent of the first conclusion, and that the Laboratory was slow to reconsider when Madrid objected (Office of the Inspector General 2006). These were the best fingerprint examiners in the world, and their mind-set beat their eyes.

1.3 The biases, translated

The primer condenses Heuer's catalog of perceptual and cognitive biases into a single page (US Government 2009, 2). The left and center columns below paraphrase that page. The right column is my translation into the language of a case file.

Bias named in the primer	What the primer says	What it looks like in a case file
Expectations	We perceive what we expect, and need more and clearer information to recognize the unexpected	The canvass is looking for a white van, so nobody logs the blue sedan
Resistance	Perceptions resist change even when new evidence arrives	The alibi that checks out in week three gets explained away instead of believed
Ambiguities	Early exposure to a blurred stimulus interferes with accurate perception even after better information is available	The grainy first frame everyone "recognized" still looks like the suspect after the enhanced frame says otherwise
Consistency	A small, consistent body of data inspires more confidence than a large, messy one	Three statements that agree, because the witnesses talked to each other, feel stronger than thirty untidy data points
Missing information	It is hard to judge the effect of evidence that is absent, even when the gap is known	Nobody asks why there is not one phone contact between the supposed coconspirators
Discredited evidence	The perception outlives the evidence that created it	The informant recants and the theory he built stays on the whiteboard
Availability	Probability estimates follow whatever is easiest to recall	Last year's big case becomes the template for this one
Anchoring	Estimates move only incrementally from where they started	The first name on the board remains the yardstick for every later suspect
Overconfidence	Certainty is overstated, especially by experts	"Twenty years on the job" is offered as a confidence interval
Rationality	Events are read as orderly and intended, and accident and error are discounted	Every shooting gets a motive, so the stray round and the mistaken identity are ruled out too early
Attribution	Others act from fixed character, we act from circumstance	The suspect asked for a lawyer because he is guilty, and the detective cut a corner because the unit was short handed

1.4 Why knowing about bias is not enough

The usual institutional response to all of this is a two hour block of training on cognitive bias. It does not work, and Heuer explained why a generation ago. Cognitive biases behave like optical illusions. Knowing that the two lines are the same length does not make them look the same (Heuer 1999). Kahneman (2011) reached the same conclusion after a career spent studying the problem.

The laboratory evidence is unkind to expertise. Dror, Charlton, and Péron (2006) handed experienced fingerprint examiners pairs of prints that each examiner had personally declared a match years earlier, and told them the prints were the notorious erroneous Mayfield identification. Most of them reversed their own prior conclusion. The prints had not changed, only the context around them. Kassin, Dror, and Kukucka (2013) call the phenomenon forensic confirmation bias and document it well beyond fingerprints.

If awareness does not help, what does? Heuer's answer, and the primer's, is to stop relying on the inside of anyone's head. Get the reasoning out on paper where other people can attack it. Make the assumptions explicit. Force the alternatives onto the table. Decide in advance what evidence would change your mind (US Government 2009, 2). The primer packages that discipline as twelve techniques, and the rest of this monograph is about using them.

Chapter 2. Why Policing Should Steal This

2.1 The Intelligence Community paid retail for these lessons

The primer includes a page that every police executive should tape to the office wall. It lists strategic assumptions that nobody challenged, each paired with the alternative that turned out to matter. Japan would avoid war because it understood American superiority. China would not cross the Yalu. Moscow would not put offensive missiles in Cuba. The Arab states would not attack in 1973 because they knew they could not win. Saddam Hussein stonewalled the inspectors because he was hiding weapons (US Government 2009, 3).

The last of those forced the reckoning. The Senate Select Committee on Intelligence (2004) and the presidential commission on weapons of mass destruction (2005) found analysts leaning on thin and ambiguous sourcing, inheriting assumptions from earlier assessments without testing them, and failing to explain how little they actually knew. Congress then ordered alternative analysis into the system by statute (Intelligence Reform and Terrorism Prevention Act 2004, § 1017). The Director of National Intelligence followed with binding analytic standards. Analysts must describe the quality of their sources, express uncertainty, separate assumption from judgment, and consider alternatives (Office of the Director of National Intelligence 2015).

None of that was adopted out of intellectual curiosity. It was adopted because the community got burned, publicly and catastrophically, by its own mind-sets.

2.2 Same failure mode, different uniform

The structural parallels between an intelligence problem and a criminal investigation are close to exact.

- Both work from incomplete and ambiguous information under time pressure.
- Both face people who conceal, lie, and sometimes actively deceive.

- Both are run by hierarchical organizations in which the senior person's theory tends to become everyone's theory.
- Both produce judgments on which someone else, a policymaker or a prosecutor, will act.
- Both have a long record of confident error traced afterward to assumptions nobody wrote down.

Policing has already imported the vocabulary. Intelligence led policing is two decades old (Ratcliffe 2016). Fusion centers exist. The profession's own guidance speaks of source evaluation and hypothesis testing (Carter 2009; Global Justice Information Sharing Initiative and IALEIA 2012). What is usually missing is the drill, meaning the routine, written, reviewable practice of the techniques on live cases. A department that owns the vocabulary and skips the drill is running investigations with the analytic rigor of a bar argument.

The primer makes the case for transfer implicitly. Its showcase example for the Key Assumptions Check is not a foreign intelligence problem at all. It is the 2002 Washington sniper investigation (US Government 2009, 8).

2.3 Three differences that raise the stakes

The transplant is not perfectly clean. Three differences matter, and each one makes the techniques more valuable in policing, not less.

The product gets cross examined. An intelligence estimate is never tested by an adversary with subpoena power. An investigative theory is. The case will be attacked by a lawyer whose only job is to find the unexamined assumption. It is better found in the squad room.

The file gets disclosed. Intelligence analysts work behind classification. Police analysts work in front of disclosure obligations. Chapter 16 argues that this is a feature and explains how to write for it.

The error has a name and a prison number. A wrong estimate embarrasses a government. A wrong charging decision takes a particular human being's liberty and leaves the actual offender at large to do it again.

2.4 What the techniques are, and what they are not

The primer sorts its techniques into three families by purpose. Diagnostic techniques make arguments, assumptions, and gaps visible. Contrarian techniques challenge the current thinking head on. Imaginative techniques generate new insights and alternative outcomes (US Government 2009, 5).

The primer is honest about the limits, and I intend to be as well. Using the techniques guarantees neither precision nor accuracy. What they buy is sophistication, credibility, and usefulness to the decision maker (US Government 2009, 5). They do not manufacture evidence, and a matrix is not probable cause.

Because the primer speaks the dialect of Langley, a short glossary will save confusion in the chapters that follow.

The primer says	A police reader should hear
Analytic line	The theory of the case, or the working explanation of a crime pattern
Policymaker	The charging prosecutor, the unit commander, the chief
Collector	The detective, the patrol officer, the lab, the informant handler
Finished intelligence	The case summary, the warrant affidavit, the charging memorandum, the crime bulletin
Denial and deception	Alibis, staged scenes, false confessions, informants with an agenda
Warning	The threat assessment and the early warning bulletin

PART II

Diagnostic Techniques: Making the Argument Visible

The four diagnostic techniques do not tell an investigator what happened. They show the investigator what the current theory is standing on. That is a humbler service and a more useful one.

Chapter 3. Key Assumptions Check

> *List and review the working assumptions on which the fundamental judgments rest (US Government 2009, 7).*

3.1 What the primer says

The primer defines a key assumption as any hypothesis the analyst has accepted as true and on which the assessment is built. Such assumptions are held, often unconsciously, and are therefore seldom examined and almost never challenged (US Government 2009, 7).

The method has four steps (US Government 2009, 9):

1. Write down the current analytic line where everyone can see it.
2. Articulate every premise, stated and unstated, that must be accepted for that line to hold.
3. Challenge each premise. Ask why it must be true and whether it holds under all conditions.
4. Cut the list to the assumptions that truly must be true, and consider what conditions or information would defeat each one.

The primer suggests questions to drive the challenge. How confident are we in the assumption, and what explains that confidence? What would undermine it? Was it true once and less so now? If it proves wrong, does the analytic line change? (US Government 2009, 9).

Two features deserve emphasis. The check is cheap. The primer puts it at an hour or two at the start of a project, repeated before judgments are finalized (US Government 2009, 7). And its purpose is not to throw assumptions out. It is to make them explicit and to identify in advance what would force a rethink (US Government 2009, 7).

3.2 The primer's case study: the Washington sniper

The primer's illustration is a police case. During the sniper shootings in the Washington area in the fall of 2002, a working theory emerged quickly. The shooter was a lone white male with military training, driving a white van (US Government 2009, 8).

The primer breaks that sentence into its five component assumptions and grades each one. Male was highly likely on precedent. Acting alone was highly likely on precedent. White was likely but less certain, so excluding nonwhite suspects carried real risk. Military training was possible, but no reason to exclude people without it. The white van rested on an eyewitness account in a region with more than 70,000 registered white vans, at a time when witnesses were describing other vehicles as well (US Government 2009, 8).

The primer's conclusion is that officials who ran this exercise could have avoided narrowing the suspect pool to a group that did not contain the perpetrators. They would have been more receptive to tips, including reports of a particular Chevrolet leaving a scene. And they would have been primed to notice evidence against the assumption that the shooter worked alone (US Government 2009, 8).

3.3 What the case teaches beyond the primer

The outcome is public record. The shooters were John Allen Muhammad and Lee Boyd Malvo, two Black males, one of them seventeen years old, working as a team out of a blue Chevrolet Caprice. Press accounts after the arrests reported that officers had come across the Caprice and run its tags more than once during the spree. It was not a white van, so it went on its way.

I draw three lessons that the primer leaves implicit.

Precedent is not evidence about this offender. The assumption the primer itself graded as highly likely on precedent, a lone shooter, was false. Base rates tell you where to start looking. They do not tell you whom to stop looking at.

A half right assumption is the most dangerous kind. Muhammad was an Army veteran. The military training assumption was right about him and wrong about Malvo. An assumption that pays off part of the time earns loyalty it has not deserved, and the squad stops distinguishing between "this narrows the search" and "this excludes everyone else."

The tip that breaks the case arrives looking like noise. The Caprice was in the data. Nobody had written down that the investigation was assuming a van, so nobody recognized the Caprice as a contradiction of anything. You cannot notice the violation of an assumption you never admitted making.

3.4 The application to crime analysis

The translation to routine work is direct. A serial burglary pattern assumes the offender is local, works alone, and is fencing the goods instead of hoarding them. A gang shooting assumes retaliation for the last gang shooting. A missing person case assumes the spouse.

These assumptions are usually right, which is exactly why they are dangerous. Nobody writes them down, so nobody abandons them when the evidence quietly stops supporting them.

My recommendation is concrete. The crime analyst should hand every major case team a one page assumptions register before the first canvass is finished, and reopen it at every case review. It costs an hour. It has saved careers.

3.5 A worked register

The following register is a hypothetical illustration. Fourteen daytime residential burglaries have hit two adjoining beats in six weeks, all through rear sliding doors, all taking jewelry and small electronics.

Assumption	Why we believe it	Confidence	What would make us drop it
One offender or crew committed all fourteen	Same entry point, same hours, same property taken	Likely	A matching burglary while our best suspect is in custody, or two distinct shoe impressions across scenes
The offender lives or works nearby	Tight geographic cluster and past experience with local offenders	Likely, not certain	Stolen property surfacing two counties away, or one out of area plate at several scenes
The offender moves on foot	No vehicle reported by any neighbor	Possible. This rests on absence of evidence only	A single doorbell camera showing a drop off
The property is being fenced locally	That is how the last three series ended	Possible	No pawn or resale hits after thirty days
The offender is an adult	Precedent	Possible	Events that track the school calendar and stop on holidays

Notice what the register does. The third and fifth rows expose assumptions resting on nothing but habit. The fourth column converts each assumption into a tripwire that a patrol officer or a records clerk can actually trip.

3.6 How to run it

1. The analyst writes the working theory as a single sentence on the board. If the team cannot agree on the sentence, that disagreement is the first finding.
2. Each member silently lists what must be true for the sentence to hold. Do it silently so the senior detective's list does not become everyone's list.
3. Merge the lists. Split compound assumptions into single claims, as the primer does with the sniper theory.
4. Grade each claim as highly likely, likely, or possible, and write down the basis. "Experience" is a basis. Say so honestly.
5. For each claim, write the specific observation that would defeat it.
6. Mark the load bearing claims, the ones whose failure would collapse the theory. Those drive collection.
7. Date the register, put it in the file, and set the next review.

3.7 Where it goes wrong

- **Written once, never reopened.** A register that is not revisited is a souvenir.
- **Only the safe assumptions get listed.** The assumption nobody wants to say aloud, that the cooperating witness is truthful or that the lead detective's first read was right, is the one that belongs at the top.

- **Fact and assumption get confused.** "The victim was killed between ten and midnight" is an assumption until the medical examiner and the phone records say it is not.
- **Rank gets an exemption.** If the lieutenant's assumption cannot be listed and graded like everyone else's, the exercise is theater.

Chapter 4. Quality of Information Check

> *Evaluate the completeness and soundness of the available information sources (US Government 2009, 10).*

4.1 What the primer says

Confidence in a judgment, the primer says, should rest on how accurate and reliable the underlying information is. Having many sources is no substitute for having good information that has been examined. Without periodic checks, important judgments become anchored to weak information, and the caveats once attached to it are forgotten over time (US Government 2009, 10).

The method is a systematic, recurring review of every source feeding the analytic line. The primer's list (US Government 2009, 11) asks the analyst to:

- Review all sources for accuracy.
- Identify the sources that are most critical or most compelling.
- Check for sufficient and strong corroboration of critical reporting.
- Reexamine information previously dismissed, in light of new facts.
- Make sure any recalled reporting is flagged, and review the analysis that relied on it.
- Check that ambiguous information was interpreted and caveated properly.
- Assign a level of confidence to each source for future use.

For human sources the primer calls for close review of the source's background, access, and motivation. For technical sources it warns of errors in processing, translation, or interpretation that otherwise go unnoticed (US Government 2009, 10). Its cautionary tale is Iraq, where the postmortems found reliance on a single ambiguous source and a failure to grasp the limits of technical collection (US Government 2009, 11; Commission on the Intelligence Capabilities of the United States 2005).

4.2 The application to policing

Intelligence agencies learned this lesson the hard way in the run up to Iraq. Police departments learn the same lesson, one jailhouse informant at a time.

Translate the primer's source review into policing and you have a checklist that would embarrass a great many affidavits.

The informant. What does the confidential informant get for this? How does the informant claim to know it: saw it, heard it from the suspect, or heard it from somebody's cousin? Has this informant ever

been wrong, and did anybody record it when that happened? The law has long treated veracity and basis of knowledge as central to weighing an informant's tip (Illinois v. Gates 1983). The research on what happens when nobody weighs them is grim reading (Natapoff 2009).

The eyewitness. Was the identification made under conditions the science says produce reliable results? Or was it a photo array shown by the lead detective who already had a favorite? The National Research Council (2014) recommends blind administration, standardized instructions, and a recorded statement of the witness's confidence at the first identification. Confidence inflates afterward. An analyst reviewing source quality asks which of those safeguards were actually used.

The forensic result. A laboratory report is a source, and it has access and motivation problems of its own. What was the examiner told about the case before the comparison? Has the method's error rate ever been measured? The National Research Council (2009) found that much of forensic pattern comparison lacked that foundation. Mayfield showed what contextual information does to a comparison.

The digital record. Technical collection in policing has limits that investigators routinely forget. Historical cell site records place a handset in a sector, not on a porch. A license plate reader misreads characters. A surveillance recorder's clock may be off by minutes or by an hour. Acoustic gunshot detection reports a location estimate, not an eyewitness account. A facial recognition candidate is a lead and nothing more. Every one of these gets written into reports as if it were a fact.

The statement. A confession is a source too. The analyst should ask what the suspect knew that had not already been disclosed during the interview, and whether those details check out independently.

A simple grading convention helps. Intelligence services have long rated the reliability of the source and the credibility of the information on separate scales, since a reliable source can pass along bad information and a rogue can tell the truth. Criminal intelligence files use the same two axis logic. Extend it from the intelligence file to the case file.

4.3 Recalled reporting is the Brady problem seen from the analyst's chair

The primer adds a point that should make every prosecutor sit up. Recalled reporting must be flagged, and the analysis built on it must be reexamined to see whether that reporting was essential to the judgment (US Government 2009, 11).

In the criminal justice context this is the disclosure problem viewed from the analyst's chair. When a source is discredited, the prosecution's obligations under *Brady v. Maryland* (1963) and *Giglio v. United States* (1972) come into play. That duty reaches favorable information known to the police, whether or not the prosecutor has heard about it (*Kyles v. Whitley* 1995).

But disclosure is only half the question. The other half is analytic. Was the entire investigative theory load bearing on that source? Which later steps, the second warrant, the identification, the cooperating codefendant's deal, grew out of what that source said? And does anyone have the guts to say so out loud?

A unit that has kept a source log can answer in an afternoon. A unit that has not will answer under oath.

4.4 A worked source log

A hypothetical illustration, from a shooting investigation three weeks old.

Source	How the source knows	Motive and conditions	Track record	Corroboration	Load bearing?
Confidential informant	Says the suspect admitted it at a party. Secondhand as to the event	Pending drug charge. Expects consideration	Two prior tips, one accurate, one never checked	None yet	Yes. Named the suspect
Eyewitness across the street	Saw the shooter for seconds at night at roughly forty yards	Cooperative, no known stake	No history	Clothing description matches video	Yes. Picked the suspect from an array run by the lead detective, not blind
Corner store video	Direct recording	Recorder clock not yet verified	Not applicable	Consistent with the 911 time if the clock is right	Partly. Sets the timeline
Cell site records	Carrier business records	Sector coverage only	Not applicable	Consistent with half the neighborhood being present	No. Does not discriminate
Shell casings	Lab comparison pending	Examiner was told the suspect's name	Not applicable	None yet	Unknown

Read the last column down. The theory rests on one compensated informant with secondhand knowledge and one identification made under poor conditions by a nonblind administrator. Everything else is consistent with the theory and with a great many other theories. That is the state of the case, and it is better to learn it from a table than from a defense expert.

4.5 How to run it

1. Open the log when the case opens. One row per source, human or technical.
2. Record access, motive, conditions, and track record at intake, while the facts are fresh and before the source has become important.
3. Mark which sources are load bearing. A case with one load bearing source has a single point of failure, and the collection plan should say so.
4. Review the log at every case review and whenever a source changes status.
5. When a source is discredited, trace forward. List every investigative step and every judgment that relied on it, and tell the prosecutor the same day.

4.6 Where it goes wrong

- **Counting sources instead of weighing them.** Five witnesses who all heard it from the same person are one source.
- **Circular corroboration.** The informant is believed because the eyewitness agrees, and the eyewitness is believed because the informant agrees. Neither was tested alone.
- **Deference to technology.** A printout carries more authority than it has earned.
- **Caveats that evaporate.** "Possibly the suspect's vehicle" in the first report becomes "the suspect's vehicle" by the fourth. The primer names this drift specifically (US Government 2009, 10).

Chapter 5. Indicators or Signposts of Change

> *Periodically review a list of observable events or trends to track developments, spot emerging trends, and warn of unanticipated change (US Government 2009, 12).*

5.1 What the primer says

An indicators list is a set of observable events one would expect to see if a postulated situation is developing. Building one takes a few hours to a few days. It serves on its own for tracking a situation over time, and it supports nearly every other technique in the primer by telling the analyst what to watch (US Government 2009, 12).

The process is the same either way (US Government 2009, 12):

1. Identify a set of competing hypotheses or scenarios.
2. Build a separate list of the activities, statements, or events expected under each.
3. Review and update the lists on a regular schedule to see which indicators are changing.
4. Judge which hypothesis or scenario is emerging from the pattern of indicators observed.

The primer adds two refinements worth keeping. First, build two lists for each scenario: indicators that it is developing, and indicators that it is not. Second, when views are sharply divided, an agreed list depersonalizes the argument by moving attention to objective criteria (US Government 2009, 12).

The primer's illustration is a matrix for tracking political instability in a foreign country. It follows indicators of government capacity, regime legitimacy, opposition activity, economic factors, and environmental stress across successive quarters. It grades each from negligible to serious concern and adds a list of trigger mechanisms that could set off a sudden shift (US Government 2009, 13).

5.2 The application to crime analysis

Crime analysts already track indicators. They just call it a hot spot map. The primer's contribution is to formalize the logic, and above all to tie each indicator to a hypothesis.

Swap the rows of the primer's instability matrix and you have a gang conflict early warning matrix. No single indicator predicts a shooting. But a disciplined, periodically reviewed list settles the argument between the gang unit sergeant who insists things are quiet and the analyst who thinks the neighborhood is about to catch fire. Once both sides agree on the criteria, the data does the arguing.

5.3 A worked list

A hypothetical illustration, following the primer's advice to keep one list for the scenario emerging and one for the scenario receding.

Category	Signs the conflict is heating up	Signs it is cooling
Custody	A known shooter or shot caller is released	Key players are in custody or have left the area
Online	Taunts, mockery of the dead, scorekeeping posts	Accounts go quiet, or talk of a truce appears
Markets	Disputes over sales locations, sudden price changes	Stable territory and prices
Gunfire	Shots fired with no victim on boundary blocks	Detections and calls fall back to baseline
Weapons	More recoveries, stolen gun reports, ballistic links between incidents	Recoveries flat, no new links
Calendar triggers	A funeral, an anniversary of a killing, a court date, a release date	The date passes without incident
Community	Outreach workers and school staff report fear, children kept home	Mediation under way and reported by the people doing it

The calendar row is the policing equivalent of the primer's trigger mechanisms. Triggers do not cause the conflict. They decide which week it arrives.

5.4 Other uses

Indicators are not only for strategic warning. They are the natural output of every other technique in this monograph.

- From a Key Assumptions Check: the tripwires in the right hand column of the register are indicators.
- From a competing hypotheses matrix: what would we expect to observe next if the second hypothesis is the true one?
- From a High-Impact/Low-Probability or "What If?" exercise: the observables on each pathway.
- In a series investigation: signs that the offender has changed method, moved territory, or stopped.
- In a fugitive case: signs of preparation to run, such as liquidating property or new travel documents.

5.5 How to run it

1. Start from hypotheses, never from whatever data is lying around. Ask what you would expect to see, then go find out whether you can see it.

2. Make every indicator observable by a named collector. “Tension is rising” is not an indicator. “Three or more shots fired calls without a victim on the boundary blocks in seven days” is.
3. Agree on the list before anyone looks at the current readings. That agreement is what depersonalizes the dispute.
4. Fix a review schedule, weekly for a live conflict and monthly for a slow problem, and keep the old versions.
5. Publish the list with the product. The primer notes that including indicators lets the decision maker track developments independently (US Government 2009, 12).

5.6 Where it goes wrong

- **Indicators that measure the police.** Arrests and field interviews rise when a unit is deployed. That measures deployment, not offender behavior. Build the list from what the other side does.
- **Nobody reviews it.** A list that is not read on schedule is a decoration.
- **Indicator inflation.** Forty indicators guarantee that something is always blinking. Keep the list to the few that discriminate between scenarios.
- **Moving the goalposts.** When the indicators say the favored theory is wrong, the temptation is to rewrite the indicators. Change them only with a written reason.

Chapter 6. Analysis of Competing Hypotheses

> *Identify the alternative explanations and evaluate all the evidence in a way that disconfirms hypotheses instead of confirming one (US Government 2009, 14).*

6.1 What the primer says

Analysis of Competing Hypotheses, or ACH, is Richards Heuer’s invention (Heuer 1999), and it is the primer’s heavyweight. The primer recommends it where there is a large body of data to absorb, where the issue is controversial, and where analysts want a clear record of what theories they considered and how they reached a judgment. It works best with a small team whose members challenge each other’s reading of the evidence, and the matrix can often be built in a day or less (US Government 2009, 14).

ACH exists to defeat three habits (US Government 2009, 14). Analysts are unduly swayed by a first impression. They seldom generate a full set of explanations at the outset. And they rely on evidence that supports their preferred hypothesis without noticing that it is equally consistent with the others.

The steps, condensed from the primer (US Government 2009, 14, 15):

1. Brainstorm, with people of differing perspectives, to identify every reasonable hypothesis.
2. List all significant evidence and arguments.
3. Build a matrix with hypotheses across the top and evidence down the side. Mark each cell consistent, inconsistent, or not applicable.

4. Refine the matrix. Add hypotheses and revisit the evidence as needed.
5. Focus on disproving hypotheses. Tally the inconsistencies to see which explanations are weakest.
6. Test how sensitive the result is to a few critical items. What if they are wrong, misleading, or planted?
7. Ask what evidence one would expect to see for each hypothesis and is not seeing. Consider denial and deception.
8. Report all the conclusions, including the weaker hypotheses that should still be monitored.
9. Identify indicators to watch going forward.

6.2 Diagnosticity

The primer's example scores four explanations of the group behind the 1995 Tokyo subway sarin attack against four items of evidence. One item, that the group had a blind leader, is consistent with every hypothesis (US Government 2009, 15).

That is the whole lesson in one row. Evidence consistent with everything discriminates among nothing. The primer calls the property diagnostic value. An item that fits all the hypotheses is unimportant to choosing among them, however vivid it may be (US Government 2009, 15).

6.3 The application to investigation

ACH is the technique law enforcement most needs and least uses.

A suspect with no alibi, a motive, and proximity to the scene sounds like a strong case. Run those three facts against the six other people who also had no alibi, a motive, and proximity, and they discriminate among no one. Detectives collect evidence that is consistent with their suspect. ACH forces them to ask which evidence is inconsistent with everyone else.

That inversion breaks most investigators' instincts, and it is the entire point. A case is not built by piling up facts that fit. It is built by eliminating the explanations that do not.

I add two rules for police use that the primer does not state.

Always include the null hypotheses. Every homicide matrix gets a column for an offender not yet known to the investigation. Every death investigation gets columns for accident, suicide, and natural causes until the evidence removes them. Every arson matrix gets a column for accidental origin. The column you refuse to draw is the one the defense will draw for you.

Hypotheses are explanations, not people. "The husband did it" is a poor column heading. "Killed by an intimate partner during an argument" is a better one. It keeps the matrix about what happened and lets several individuals be tested against the same explanation.

6.4 A worked matrix

A hypothetical illustration. A fire guts a struggling restaurant at 2:30 in the morning. The squad likes the owner for it, on the strength of his finances and his insurance. Four hypotheses are on the table. C means consistent, I means inconsistent, and N means neutral or not applicable.

Evidence	H1: Owner set it for the insurance	H2: Fired employee set it for revenge	H3: Accidental electrical fire	H4: Burglar set it to cover a break in
Business is three months behind on rent	C	C	C	C
Accelerant pattern in the rear storeroom	C	C	I	C
Rear door forced from the outside	I	C	N	C
Coverage increased sixty days before the fire	C	N	N	N
Cash drawer and safe emptied	N	C	I	C
Alarm disarmed with a valid code at 2:10	C	C	N	I
Former employee posted threats two weeks earlier	N	C	N	N
Owner's phone was at home all night	N	N	N	N
Inconsistencies	**1**	**0**	**2**	**1**

Read it the way the primer instructs, by inconsistencies and not by confirmations.

- **The squad's two favorite facts do the least work.** The unpaid rent is consistent with every hypothesis. The increased coverage is consistent with the owner and neutral toward everyone else. It can support. It cannot eliminate.
- **The owner is not the least contradicted hypothesis.** The fired employee is. Nothing in hand is inconsistent with that explanation.
- **The phone record is not an alibi and not an accusation.** A phone's location is not a person's location, and the owner could have hired the job out. It scores neutral across the board.
- **Two items decide the case, and neither has been collected properly.** If the door was forced from inside to stage a break in, the owner hypothesis has no inconsistencies left. If the alarm panel log shows whose code was used, it will damage either the owner hypothesis or the employee hypothesis badly.

So the matrix did not solve the arson. It told the squad that its confidence was resting on evidence with no diagnostic value. And it produced a two item collection plan: a tool mark examination of the door and a download of the alarm panel's user log. Those are investigative leads, and the analysis produced them in an afternoon.

Then ask the primer's absent evidence question. If the owner did it, we would expect valuables or records to have been removed before the fire. Were they? If the former employee did it, we would expect his phone or vehicle near the scene. Has anyone looked? What should be there and is not is evidence too.

6.5 The matrix as a record

The primer notes that ACH suits controversial issues where analysts want a clear record of what they considered (US Government 2009, 14). In policing, that record is worth real money.

A cold case unit or a conviction integrity review that can produce a dated matrix of considered and rejected hypotheses is in an infinitely stronger position, in court and in the press, than one that can only say "we always knew it was him." The matrix answers the question every defense lawyer asks and every juror wonders about: did you look at anybody else?

6.6 How to run it

1. Generate hypotheses with a structured brainstorm (Chapter 11), including the nulls. Do it before the evidence review, not after.
2. List evidence and its absence. Take source quality from the log (Chapter 4), because a C from a compromised source is not worth a C from a good one.
3. Score across each row, not down each column. Ask of one item at a time how it bears on every hypothesis. Scoring down a column is how the favorite gets an easy ride.
4. Strike or gray out the rows with no diagnostic value. Count how much of the case just disappeared.
5. Run the sensitivity test. Identify the two or three items on which the outcome turns, and ask what the case looks like if each is wrong or staged.
6. Write the result as a ranking with reasons, not as a verdict. Name the hypotheses still alive and what would kill each.
7. Date it, version it, and revisit it when new evidence arrives.

6.7 Where it goes wrong

- **Garbage evidence in.** ACH is only as good as the items on the left. Run the Quality of Information Check first.
- **Arithmetic mistaken for judgment.** The tally shows where to think harder. One solid inconsistency, a verified alibi or an exclusion by DNA, outweighs any number of soft consistencies.
- **A hypothesis set that is too small.** A matrix with two columns, the suspect and "someone else," is confirmation bias with gridlines.
- **Reverse engineering.** Filling in the matrix after the arrest to justify it is fraud on the method, and it will read that way on cross examination.
- **Overselling.** Experimental work has not shown that ACH reliably makes analysts more accurate (Dhami, Belton, and Mandel 2019). Chapter 17 takes that up. Its strongest claim is transparency, and transparency is what a criminal case needs.

PART III

Contrarian Techniques: Institutionalized Disagreement

Diagnostic techniques expose the structure of an argument. Contrarian techniques attack it on purpose. The four in this part exist because no group can be trusted to argue against its own conclusion voluntarily, and a paramilitary one least of all.

Chapter 7. Devil's Advocacy

> *Challenge a single, strongly held view or consensus by building the best possible case for an alternative explanation (US Government 2009, 17).*

7.1 What the primer says

Devil's Advocacy is for the questions one cannot afford to get wrong. It works best against an analytic consensus or a key assumption on a critically important issue. An analyst with private doubts can take up the role, or a manager can designate someone, and the primer's adjective for that person is "courageous." When a group has worked an issue for a long time, the primer says, it is wise to assume a strong mind-set exists that deserves this scrutiny (US Government 2009, 17).

The advocate's method (US Government 2009, 17, 18):

1. Outline the mainline judgment, its key assumptions, and the evidence supporting it.
2. Select the assumptions, stated or not, that look most open to challenge.
3. Review the information for questionable validity, possible deception, and major gaps.
4. Highlight the evidence that supports an alternative hypothesis or contradicts the current thinking.
5. Present the findings to the group.
6. If the review uncovers major flaws, consider a separate contrarian paper.
7. Label every product clearly as a Devil's Advocate effort.

The exercise has three legitimate outcomes. The current line is sound. The current line is still the strongest but needs more work in places. Or serious flaws in logic or evidence mean the line must be changed or at least caveated more heavily (US Government 2009, 17). The first outcome is not a failure. A theory that has survived a real attack is worth more than one that was never tested.

7.2 The application: a standing devil's advocate

Every major case unit should have a standing devil's advocate who is not the lead investigator and does not report to the lead investigator.

Before charging, this person's job is to write the defense's closing argument. If the case survives, it is stronger. If it does not, you just saved the county a seven figure settlement, and you may have saved an innocent person several years.

The assignment is specific, and it is not "poke holes." The advocate builds the best affirmative case for a different explanation, using the same file the squad has.

7.3 How to run it

1. **Pick the right person.** Experienced enough to be taken seriously, outside the case team, and outside the lead's chain. Rotate the duty so nobody becomes the unit crank.

2. **Give full access.** The advocate reads the whole file, including the assumptions register and the source log. An advocate working from a briefing is reviewing the squad's summary of itself.
3. **Set the deliverable.** Two pages. The three weakest assumptions. The weakest load bearing source. The best alternative explanation and the evidence consistent with it. The evidence that ought to exist if the theory is right and is missing.
4. **Present before the charging recommendation goes up.** After charging, the organization is defending a decision, not making one.
5. **Require a written response.** The lead answers each point: resolved, resolved by further work, or acknowledged and accepted as a risk. The supervisor signs.
6. **Protect the advocate.** If doing this job honestly costs someone an assignment, nobody will do it honestly again.

7.4 Label it

The primer warns that an unlabeled contrarian product can confuse the reader about the official view (US Government 2009, 18). In a criminal case that warning applies with special force. A devil's advocate memo in a case file must be marked on every page as a deliberate contrarian exercise. Otherwise a defense attorney will wave it around in front of a jury as the department's "real" view.

Labeling does not keep the memo out of the defense's hands, and it should not. Chapter 16 addresses disclosure. Labeling ensures the memo is understood for what it is: proof that the department tried to break its own case before it asked a jury to believe it.

7.5 Where it goes wrong

- **Ritual advocacy.** A token objection, politely overruled, so that a box can be checked. The cure is the written response requirement.
- **The weak advocate.** A supervisor who wants the case to pass assigns the job to the newest detective.
- **Advocacy after the fact.** A challenge mounted after the press conference is not a review.
- **The advocate falls in love.** The advocate's alternative is a stress test, not a new orthodoxy. It must face the same scrutiny as the theory it challenges.

Chapter 8. Team A/Team B

> *Use separate analytic teams to contrast two or more strongly held views or competing hypotheses (US Government 2009, 19).*

8.1 What the primer says

Devil's Advocacy challenges one dominant view. Team A/Team B is for the situation in which two views, perhaps equally strong, are already in the building. The primer notes that analysts sometimes confuse the two (US Government 2009, 19).

A full exercise costs real time, so the primer reserves it for a longstanding issue, a critical decision with far reaching implications, or a dispute that has obstructed cooperation across agencies (US Government 2009, 19).

It runs in two phases (US Government 2009, 21). In the analysis phase, the competing hypotheses are identified and teams are formed to build the best case for each. Each team reviews all the pertinent information and identifies the missing information that would buttress its position. Each argument is then structured with explicit assumptions, key evidence, and logic. In the debate phase, each team presents, challenges the other, and rebuts. An independent jury of peers listens, questions, and recommends next steps for research and collection.

The value, according to the primer, runs in two directions. Inside the organization, the exercise helps opposing experts see merit in the other view and reduces friction. For the decision maker, well argued conflicting views often teach more than a single assessment that papers over the differences or sinks to the lowest common denominator (US Government 2009, 19).

8.2 The application

The primer recommends the technique for a dispute that has obstructed cooperation across agencies. That describes roughly every joint task force ever assembled.

Consider an overdose spike. The narcotics squad believes it reflects a supply shift by a trafficking organization. The homicide unit believes a local crew is cutting product with fentanyl to stretch margins. The two theories call for different operations, different partners, and different public warnings. Left alone, each unit will run its own play and blame the other when it fails.

Other natural candidates:

- One offender or two in a linked series.
- Arson or accident, where the fire investigator and the detective disagree.
- An internal theft ring or an external one.
- Whether a run of shootings is one conflict or several unrelated ones.

The primer's practical tip is superb. Where positions are well established, put analysts on the team arguing the position they do not hold (US Government 2009, 19). Nothing exposes your own mind-set faster than being forced to argue against it.

8.3 How to run it in a week

1. **Day one.** The commander states the question in one sentence and names the teams, crossing them where possible. Both teams get the same file.
2. **Days two through four.** Each team writes a brief of no more than five pages: assumptions, key evidence, logic, and the missing information that would strengthen its case.
3. **Day five.** Thirty minutes each to present, fifteen each to challenge and rebut. The jury is a supervisor from an uninvolved unit, an analyst, and a prosecutor.
4. **The output is not a winner.** It is a short list of the facts in genuine dispute and a collection plan to resolve them. The primer is explicit that the jury's job is to recommend next steps for research and collection (US Government 2009, 21).

8.4 Where it goes wrong

- **The jury votes by rank.** If the outcome is whatever the senior team leader wanted, save the week.
- **A turf fight with slides.** Without crossed teams and an explicit rule that the product is a collection plan, the exercise hardens the split it was meant to resolve.
- **No follow through.** The collection plan gets filed and each unit goes back to its own theory.
- **It is really Devil's Advocacy.** If only one view has institutional weight, call it what it is and use Chapter 7.

Chapter 9. High-Impact/Low-Probability Analysis

> *Highlight a seemingly unlikely event that would have major consequences if it happened (US Government 2009, 22).*

9.1 What the primer says

The primer illustrates this technique with a State Department assessment dated 27 November 1941. Its author offered odds of five to one that the United States and Japan would not be at war by 15 December (US Government 2009, 23). Pearl Harbor was ten days later.

The technique is designed for exactly that failure. It applies when analysts and decision makers are convinced an event is unlikely and have not given much thought to the consequences of being wrong (US Government 2009, 22). The primer lists the fall of the Shah, the collapse of the Soviet Union, and the reunification of Germany as events that were once considered improbable.

The method (US Government 2009, 22):

1. Define the high impact outcome clearly. Its consequences are what justify the effort.
2. Devise one or more plausible pathways to it, as precisely as possible.
3. Insert triggers or changes in momentum where appropriate.
4. Brainstorm with people of broad experience to find plausible but unpredictable triggers.
5. For each pathway, identify indicators that events are beginning to play out that way.
6. Identify the factors that would deflect a bad outcome or encourage a good one.

Note what the technique does not do. It does not claim the event is likely. It claims the event is too costly to leave unexamined.

9.2 The application

For a police department the list writes itself. A coordinated ambush of officers. A mass casualty attack at the county fair. A courthouse shooting. The targeted killing of a judge, a prosecutor, or a witness. A catastrophic failure of the evidence room or the crime lab that taints hundreds of cases. A cyberattack that takes dispatch down on a Friday night.

Every one of those is unlikely in any given year. Every one of them has happened to somebody.

It is the difference between thinking about the unthinkable on a Tuesday afternoon with coffee and thinking about it for the first time on the radio.

9.3 A worked pathway

A hypothetical illustration. The outcome to examine is the killing of the key civilian witness before trial in a gang homicide prosecution. The unit considers it unlikely because it has not happened here.

Pathway	Possible triggers	Indicators	Deflectors
The defendant directs associates from custody	The witness's name appears in discovery, or a trial date is set	Oblique references to the witness in recorded jail calls, new visitors, messages passed through third parties	Protective orders on discovery, prompt review of jail communications, relocation
The witness's identity circulates in the neighborhood	Discovery pages or a courtroom photo posted online	The witness's statement appears on social media, or the witness's family reports being approached	Limits on dissemination of discovery, monitoring of open sources, a named point of contact for the family
A chance encounter escalates	The witness returns to the neighborhood for a family event	The witness stops answering the prosecutor's calls, or reports being followed	Relocation that actually holds, an early deposition to preserve testimony where the rules allow

None of this requires believing the witness will be harmed. It requires an afternoon, and it leaves behind a list of things somebody is now responsible for watching.

9.4 How to run it, and where it goes wrong

Run it annually for the department's standing nightmares, and at the start of any case or operation with a catastrophic downside. Use a structured brainstorm with at least one outsider. Hand the indicators to a named owner with a review schedule (Chapter 5).

The failure modes are three. **Doing it once** and filing it. **Confusing it with prediction**, so that the product gets dismissed the first year nothing happens. And **crying wolf**, issuing so many improbable warnings that the one that matters is ignored. The primer's own example of a warning that did not land is the President's Daily Brief item of 6 August 2001 on al-Qa'ida's interest in attacks inside the United States (US Government 2009, 23). A warning that changes nobody's behavior has not done its job.

Chapter 10. "What If?" Analysis

> *Assume an event has occurred, with negative or positive impact, and explain how it might have come about (US Government 2009, 24).*

10.1 What the primer says

"What If?" analysis is a close cousin of the previous technique. The difference is one of emphasis. It dwells less on consequences and moves straight to explaining how the event could come about. By shifting the question from whether something could happen to how, the analyst suspends judgment about likelihood and concentrates on mechanism (US Government 2009, 24).

The primer calls the technique particularly important when a judgment rests on limited information or unproven assumptions (US Government 2009, 24). That describes most judgments.

The method (US Government 2009, 24):

1. State the conventional line, then assume the contrary event has happened.
2. Select triggering events that make the scenario plausible.
3. Develop a chain of argument, based on logic as much as evidence, for how it came about.
4. Think backward from the event in concrete terms. Specify what must have occurred at each stage.
5. Identify one or more plausible pathways.
6. Generate indicators for each pathway.
7. Consider the scope of the consequences.
8. Monitor the indicators periodically.

The primer's example is the October 1990 National Intelligence Estimate on Yugoslavia. It judged that the country muddling through was very unlikely, and then set out concretely what muddling through would look like if it happened (US Government 2009, 25).

10.2 The application

The technique converts cleanly into three questions a case team should be made to answer in writing.

What if the informant has been playing the squad for a year? Think backward. What would he have had to know, and from whom? Which of his tips were verifiable only through him? Who benefited from the arrests his information produced? What would we expect to find in his phone?

What if the suspect in custody is innocent? Then someone else did it, and the evidence against the suspect has another explanation. Take each item in turn. How did his fingerprint get there innocently? Why would the witness be mistaken? Who else fits the description? What must have happened for all of that to be true, and what trace would it have left?

What if this conviction is vacated in ten years? Write the press release now. What does it say went wrong? A misidentification, an informant who was paid, a lab result that was overstated, a lead that was never run. This is Klein's premortem (Klein 2007) applied to a prosecution. People are far better at explaining a failure they have been told has already happened than at predicting one in the abstract.

10.3 How to run it

Forty-five minutes, at the point where the team is most confident. State the conventional line. Assume its opposite. Work backward on a whiteboard, stage by stage, writing what must have happened. Convert each stage into an observable. Assign someone to check the three cheapest observables before the next review.

10.4 How it differs from its neighbors

Technique	Starting point	Product
Devil's Advocacy	The current theory is wrong. Argue the alternative from the existing file	A contrarian case and a list of weaknesses
High-Impact/Low-Probability	An unlikely catastrophe deserves attention because of its cost	Pathways, indicators, and deflectors
"What If?"	The unlikely thing has already happened. Explain how	A backward chain of events and the traces each would leave

PART IV

Imaginative Techniques: Getting Outside the Building, the Box, or Whatever the Hell You Want to Call It

The diagnostic techniques examine the theory you have. The contrarian techniques attack it. The imaginative techniques go looking for the theories, forces, and futures nobody in the room has thought of yet.

Chapter 11. Brainstorming

> *An unconstrained group process designed to generate new ideas and concepts (US Government 2009, 27).*

11.1 What the primer says

The primer's brainstorming is not a bull session. Paradoxically, it says, brainstorming must be a very structured process to be productive (US Government 2009, 27).

The structure has two phases (US Government 2009, 29). In the divergent phase, the group is given a single focal question. Members write their responses silently on sticky notes, and all the notes go on the wall with equal standing. When the flow of ideas pauses, the group has reached the end of its conventional thinking, and the new ideas tend to arrive after that. The collection stage ends after two or three such pauses. In the convergent phase, the group rearranges the notes into clusters without talking, names each cluster, looks hard at the orphans, and votes on which areas deserve the most attention.

The rules are few (US Government 2009, 27). Never censor an idea, however unconventional. Find out what prompted it, because it may point to an unstated assumption. Allow enough time to exhaust the conventional wisdom first. And involve at least one outsider, someone who does not share the group's background or mind-set but knows something about the topic.

The primer also reproduces five points from an experienced practitioner (US Government 2009, 28). Leave rank at the door. Make sure there is no official line to protect. Ban killer phrases such as "that could not happen." Keep the session under ninety minutes. Record the ideas where everyone can see them. The same practitioner observes that the most creative ideas often come from relatively junior people and from seniors who are not experts on the issue.

11.2 The application

In a paramilitary organization, a lieutenant's theory becomes the squad's theory by default. Nobody decides that. It just happens, because rank speaks first and everyone else calibrates. Leaving rank at the door is therefore a structural correction, not a nicety. The silent sticky note is the mechanism that makes it real: an idea on the wall has no stripes on its sleeve.

Invite the patrol officer who works the beat. Invite the civilian analyst. Invite the crime scene technician, who looks at the same scene with different eyes. On a cold case, invite a defense attorney and watch the room squirm.

11.3 How to run it

1. **Write a focal question that does not contain the answer.** "Who wanted this victim dead, and why?" is a question. "How do we prove the boyfriend did it?" is a conclusion with a question mark.
2. **Seat eight to twelve people**, at least one of them from outside the unit.
3. **Divergent phase, silent.** Everyone writes. All notes go up. The facilitator is not the lead investigator.

4. **Wait out the pauses.** The first twenty minutes produce the theories everyone walked in with. Stopping there is the most common mistake.
5. **Convergent phase, silent.** Cluster, name the clusters, and examine the notes that fit nowhere.
6. **Vote, then photograph the wall.** The clusters become the hypothesis set for the competing hypotheses matrix in Chapter 6.

Good focal questions for crime analysis follow the same rule. What explains the rise in vehicle thefts in the fourth sector since March? What are all the ways this property could be leaving the county? Who benefits from this fire?

11.4 Where it goes wrong

- **The boss talks first.** After that, the session is a poll on the boss's idea.
- **Killer phrases.** "We already looked at that" ends more lines of inquiry than any defense motion.
- **No convergent phase.** A wall of notes with no clustering and no vote is a memory, not a product.
- **No record.** The idea that was laughed at in week one is the one somebody needs in month six.

Chapter 12. Outside-In Thinking

> *Identify the full range of basic forces, factors, and trends that would indirectly shape an issue (US Government 2009, 30).*

12.1 What the primer says

Most analysts, the primer observes, think from the inside out. They start with the familiar factors in their own lane and work toward the wider world. Outside-in thinking reverses the direction. It begins with the external changes that could, over time, profoundly affect the analyst's own issue (US Government 2009, 30).

The steps (US Government 2009, 30):

1. Describe the problem in generic terms.
2. List the key social, technological, economic, environmental, and political forces that could bear on it and over which one has little influence.
3. List the factors over which an actor can exert some influence.
4. Assess how each force could affect the problem.
5. Determine, from the available evidence, whether those forces actually do.

The primer recommends the technique at the conceptual stage of a project. Its promise is modest and correct: a small effort early reduces the risk of missing important variables, and of discovering too late that the data was never coded for them (US Government 2009, 30).

12.2 The application

Crime analysts spend their days inside: the calls for service, the arrest data, the known offenders. Those are the factors the department produces and controls. The forces that actually move crime mostly originate somewhere else.

Eviction filings. A plant closure. A change in state sentencing law. A new encrypted messaging application. A heat wave. The school calendar. An upstream shift in fentanyl precursor supply. A change in what scrap dealers will pay.

Criminology has a theory for why this matters. Crime requires a motivated offender, a suitable target, and the absence of a capable guardian converging in space and time (Cohen and Felson 1979). The department influences guardianship. The outside world moves all three.

The catalytic converter is the cleanest recent example. When thefts exploded across the United States in the early 2020s, the cause was not a new kind of thief. It was the price of the precious metals inside the part and the ease of selling it. Analysts who were watching commodity prices and scrap regulation understood the problem months before analysts who were watching only theft reports.

12.3 How to run it

One hour, at the start of any strategic assessment or problem solving project.

1. State the problem generically. Not "thefts from vehicles in the downtown garage," but "theft of portable property from unattended vehicles."
2. Take the five categories in turn and list forces under each. Bring someone from outside policing: a city planner, a school administrator, a public health analyst, a pawn industry regulator.
3. Sort the forces into those the department can influence and those it cannot.
4. For each force, ask what data would show whether it is operating here. Most of that data belongs to another agency. Go and ask for it.
5. Add the confirmed forces to the indicators list (Chapter 5).

12.4 Where it goes wrong

- **A list without a test.** The fifth step is the one that matters. A force that cannot be shown to operate locally is a hypothesis.
- **Everything is poverty.** Root cause explanations that are true everywhere explain nothing about why here and why now.
- **Nobody outside is asked.** An outside-in session staffed entirely from inside is a contradiction in terms.

Chapter 13. Red Team Analysis

> *Model the behavior of an individual or group by trying to replicate how an adversary would think about an issue (US Government 2009, 31).*

13.1 What the primer says

The target of this technique is mirror imaging: imputing to the other side one's own motives, values, and understanding of the situation. Traditional analysis, the primer warns, tends to assume the adversary will behave rationally as the analyst defines rational. History shows otherwise (US Government 2009, 31).

Red Team analysis places the analyst deliberately in the adversary's cultural, organizational, and personal setting. The primer insists on staffing. The team needs people with deep knowledge of the operating environment and of the target's personality and style of thinking, and ideally people who have experienced the culture or worked in a similar environment (US Government 2009, 31).

Team members then (US Government 2009, 31):

1. Put themselves in the adversary's circumstances and react to stimuli as the target would.
2. Develop first person questions the adversary would ask. How would I perceive this information? What are my personal concerns? To whom would I look for an opinion?
3. Draft papers in which the adversary makes decisions, proposes recommendations, or lays out courses of action.

The product is distinctive. It is often written in the first person, as a memo to or from the adversary. It avoids caveats. It does not try to chart every possible course of action, but offers a prediction grounded in the target's particular experiences (US Government 2009, 33).

The primer is candid that this is hard and that analysts can never fully escape their own experience. The technique can at least keep them from falling into mirror imaging unconsciously (US Government 2009, 33).

13.2 The application

For crime analysis, this means assembling people who actually understand the operating environment and having them plan the crime.

Where would I sell forty stolen catalytic converters? How would I move product if the corner I worked just got a camera? What would my crew expect me to do after my cousin got shot? Whom would I call first if I thought the police were looking at me?

The uses are practical.

- **Predicting the response to enforcement.** Before the camera goes up or the takedown is executed, a red team writes the memo from the other side. Where does the activity move? Who fills the vacuum?

- **Fugitive work.** A fugitive runs to the people and places he trusts, not to the ones the squad would choose.
- **Fraud and financial crime.** Ask someone who has worked inside the control system how they would beat it.
- **Interview strategy.** What does this subject fear more than prison? What does he think the detectives already know?
- **Testing a theory of motive.** If the theory requires the suspect to have acted against his own interests as he understood them, the theory needs work.

A department that has never once tried to think like the people it is chasing is not doing analysis. It is doing bookkeeping.

13.3 How to run it

1. **Staff it with knowledge, not rank.** Veteran undercover officers, gang unit detectives, probation and parole officers, street outreach workers, a fraud examiner from the private sector. Where it can be done lawfully and safely, a cooperating former offender knows things no officer does.
2. **Give the team the adversary's information, not the department's.** The red team should know what the target plausibly knows and nothing more.
3. **Demand a first person product.** One page. "I am the person running this crew, and here is what I do next."
4. **Separate it from the regular analysis.** The primer notes that the team must distance itself from the normal analytic process and work as though living in the target's world (US Government 2009, 33).
5. **Convert the memo into indicators.** If the red team says the activity moves two blocks east, somebody watches two blocks east.

13.4 Cautions

- **Red teaming is not profiling by demographics.** The primer asks for knowledge of a specific target's culture, organization, and personal history. Assigning behavior to a person because of race, ethnicity, or neighborhood is the opposite of the technique. It is mirror imaging's lazier cousin, and in police work it invites an equal protection claim.
- **Label the product.** A first person memo written in the voice of a drug trafficker, found unlabeled in a case file, is a discovery problem and a headline.
- **Do not mistake it for evidence.** A red team product is a hypothesis generator. It tells investigators where to look. It does not tell a court what happened.

Chapter 14. Alternative Futures Analysis

> *Systematically explore multiple ways a situation can develop when there is high complexity and uncertainty (US Government 2009, 34).*

14.1 What the primer says

This technique is for the situation too complex, or the outcome too uncertain, to trust a single forecast. The primer contrasts it sharply with the contrarian techniques. Those challenge high confidence. This one accepts uncertainty and uses it to describe several futures the decision maker should prepare for (US Government 2009, 34).

The common method (US Government 2009, 36), which the primer describes as the most common approach in both the public and private sectors, and which owes much to Schwartz (1991):

1. Develop the focal issue by interviewing experts and officials.
2. Convene a group, internal and external, to brainstorm the forces and factors that could affect it.
3. Select by consensus the two most critical and most uncertain forces.
4. Turn each into an axis with defined endpoints.
5. Cross the axes into a matrix. The four quadrants are four alternative worlds.
6. Write a vivid story for each world and how it could come about.
7. Develop indicators for each.

Participants then ask how current strategies would fare in each of the four worlds, and whether some alternative would hold up better across all of them (US Government 2009, 36). The primer adds that involving the decision makers in the exercise is the most effective way to communicate its results, and that most participants find the process as valuable as any written product (US Government 2009, 34).

14.2 The application

This is the technique for strategic planners, command staff, and the budget office. It does not solve cases. It tests whether a five year strategy survives contact with a future other than the one assumed in the grant application.

A department could cross population growth against court capacity, or recruitment against attrition. The illustration below crosses narcotics supply against enforcement funding. The quadrant names and descriptions are mine.



Figure 1. *Four worlds a five year drug strategy has to survive. Illustrative scenarios built on two uncertain forces: narcotics supply and enforcement funding.*

The useful question is not which world will arrive. It is which current investments make sense in all four. A treatment diversion partnership, a competent analytic unit, and a working relationship with the public health department earn their keep in every quadrant. A strategy built entirely on overtime funded street enforcement works in one.

14.3 How to run it

Half a day, with the people who will make the decisions in the room.

1. Agree on the focal issue and the time horizon. Three to five years is realistic for a department.
2. Brainstorm the driving forces, using the outside-in categories from Chapter 12.
3. Rank the forces twice: by impact, and by uncertainty. The two that score high on both become the axes. A force that is important but predictable, such as an aging population, belongs in every scenario and on no axis.
4. Name the four worlds and write a paragraph on each. Names matter, because people remember them.
5. Test each current strategy and each major budget line against all four.
6. Write indicators for each world and assign them to the analytic unit.

14.4 Where it goes wrong

- **Picking the favorite.** The group falls in love with one quadrant and plans for it. That is single outcome forecasting with extra steps.
- **Axes that are not independent.** If one force drives the other, the matrix has two real quadrants, not four.

- **Best case, worst case, and two fillers.** If two quadrants are obviously implausible, the axes were chosen badly.
- **No indicators.** Without them, nobody will know which world is arriving until it has.

PART V

Putting It to Work

Chapter 15. Sequencing the Techniques Across the Life of a Case

15.1 The primer's timeline

The primer closes with guidance on when to use which technique over the course of an analytic project (US Government 2009, 38, 39).

- **Starting out.** Brainstorming and an assumptions check, so that important factors are not missed or taken for granted. Outside-in thinking to set the problem in its wider context. A High-Impact/Low-Probability look to sensitize the team early to dramatic events that could upend the line.
- **Throughout.** Indicators and ACH, revisited as new information is absorbed. The primer singles out ACH as a guard against premature closure.
- **As hypotheses form.** A contrarian technique to challenge the developing line. Red Team analysis where the assessment depends on strong judgments about an adversary's behavior. A review of information gaps.
- **A final check.** A last review of key assumptions as a sanity check on the logic. A brainstorm to confirm that no plausible hypothesis was left unaddressed. Devil's Advocacy if a firm consensus has gone unquestioned. A list of indicators for tracking whether the judgments hold.

15.2 The same timeline on a major case

Map that onto a major case and the fit is nearly exact. The mapping below is mine.

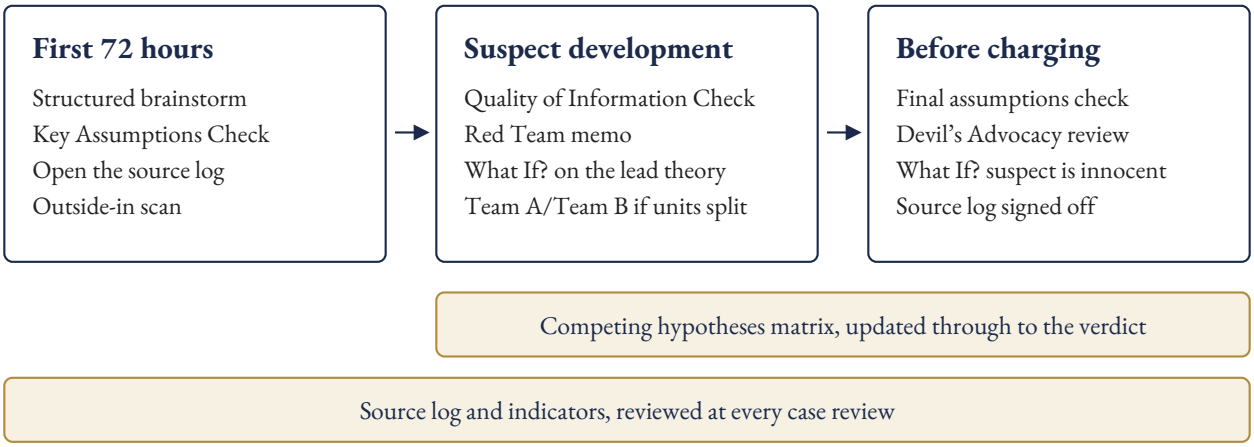


Figure 2. *Each phase of a case has its techniques, and the records run alongside. The primer's timeline mapped onto a major case.*

The first seventy-two hours. This is when the mind-set forms, so this is when the cheap techniques pay the most. Run a structured brainstorm for hypotheses, including the nulls. Open the assumptions register. Open the source log while every source is still just a source. For pattern and strategic work, add the outside-in scan.

Suspect development. A name is on the board and the gravitational pull has begun. Build the competing hypotheses matrix now and keep it current. Run the Quality of Information Check on the sources that

have become load bearing. Write a Red Team memo where the theory depends on what the suspect would or would not do. Run a "What If?" on the lead theory at the moment of greatest confidence. If two units disagree, settle it with Team A/Team B instead of in the parking lot.

Before charging. This is the final check. Reopen the assumptions register and grade it honestly against what is now known. Commission the Devil's Advocacy review. Run the innocence "What If?" Sign off the source log. Freeze a version of the matrix.

From charge to verdict. The work does not stop at arraignment. New evidence arrives. Sources change status. The indicators and the source log keep running, and anything that moves gets to the prosecutor at once.

15.3 If you only have an hour

No unit will run twelve techniques on a stolen bicycle. The primer itself says the analyst should pick the tool that fits the task (US Government 2009, 5). My triage follows.

Situation	Minimum discipline	Time
Any case assigned to a detective	The working theory in one sentence and three assumptions under it	Ten minutes
Any case relying on an informant or a single eyewitness	A source log entry with access, motive, and corroboration	Twenty minutes
Felony with a named suspect and a contested identification	Assumptions register and a competing hypotheses matrix with the nulls	Two hours
Homicide, officer involved shooting, or any case likely to draw scrutiny	The full sequence, with a labeled Devil's Advocacy review before charging	Days, spread across the case
Crime pattern or strategic assessment	Outside-in scan, indicators list, and a stated set of competing explanations	Half a day

If a department adopts only three things from this monograph, they should be the assumptions register, the source log, and the devil's advocate before charging. They are the cheapest, and they catch the most.

Chapter 16. Discovery, Disclosure, and the Witness Stand

The objection I hear most often from investigators is a legal one. "If we write down our doubts, the defense gets them." This chapter answers it. Nothing here is legal advice for a particular case, and every unit should settle its own protocol with its prosecuting authority.

16.1 Assume the defense will read it

The constitutional floor is familiar. The prosecution must disclose evidence favorable to the accused and material to guilt or punishment (*Brady v. Maryland* 1963). That includes evidence bearing on the credibility of government witnesses (*Giglio v. United States* 1972). The duty reaches favorable information known to the police even when the prosecutor is unaware of it (*Kyles v. Whitley* 1995).

Above that floor the rules vary. In federal practice, internal government reports and memoranda prepared in connection with the investigation are generally outside defense discovery (Fed. R. Crim. P. 16(a)(2)), and witness statements are produced on the schedule the Jencks Act sets (18 U.S.C. § 3500). Many states require far broader disclosure. Work product protection exists and has limits. None of those shields protects favorable information.

The safe working rule is therefore simple. Write every analytic product as though the defense will read it. If it contains anything favorable to the accused, they are entitled to that content whatever the document is called.

16.2 That is a feature

Consider what the techniques produce. An assumptions register shows what the investigation assumed and when it checked. A source log shows that the informant's motive was recorded and weighed. A matrix shows that other explanations were considered and why they were set aside. A devil's advocate memo shows that the department attacked its own case and the case survived.

An investigation that can show its assumptions, its considered alternatives, and its source review is an investigation that survives cross examination. The one that cannot is relying on the jury never asking how the sausage got made.

There is a second benefit, and prosecutors will see it at once. A matrix row marked inconsistent with the charged theory is, by definition, a candidate for disclosure. The technique surfaces that material in the squad room, on the government's own schedule. The alternative is that somebody finds it in the file ten years later, in a habeas proceeding, with the question of why it was never turned over.

The fear behind the objection is that honest doubt on paper loses cases. The record of wrongful convictions suggests the opposite. The cases that fall apart are those in which the doubt existed, went unrecorded, and came out anyway.

16.3 Writing analytic products for a courtroom reader

- **Label every product** with its type, author, date, and version. Mark contrarian and red team products as such on every page.
- **Separate fact, assumption, and judgment.** The Intelligence Community's standards require analysts to distinguish underlying information from their own assumptions and judgments (Office of the Director of National Intelligence 2015). Do the same, in separate sections if necessary.
- **State confidence and its basis.** "Likely, based on two independent sources with direct access" can be defended on the stand. "We believe" cannot.

- **Use probability words consistently.** The table below reproduces the scale in the Intelligence Community's analytic standards. It is for analytic products. In a warrant affidavit or a charging document the legal standard governs, and nobody should write a percentage next to probable cause.
- **Avoid words that claim more than the method delivers.** "Match" and "consistent with" have misled juries for decades (National Research Council 2009).
- **Keep the versions.** A superseded matrix is a record of how the thinking changed. A deleted one looks like concealment and may violate retention rules.

Term	Probability range
Almost no chance	1 to 5 percent
Very unlikely	5 to 20 percent
Unlikely	20 to 45 percent
Roughly even chance	45 to 55 percent
Likely	55 to 80 percent
Very likely	80 to 95 percent
Almost certain	95 to 99 percent

16.4 The warrant affidavit

An affiant who includes a false statement in a warrant affidavit knowingly, or with reckless disregard for the truth, puts the warrant at risk if that statement was necessary to probable cause (*Franks v. Delaware* 1978). Lower courts have applied similar reasoning to material omissions.

The Quality of Information Check is the affiant's protection. A source log that records what was known about the informant's reliability, basis of knowledge, and motive on the day the affidavit was sworn answers the question of what the affiant knew and whether anything was held back. The caveat that evaporated between the first report and the affidavit is exactly what a hearing on the warrant is designed to find.

16.5 The analyst as a witness

When an analyst testifies, the method is on trial along with the conclusion. Expert testimony must rest on reliable principles and methods, reliably applied to the facts (Fed. R. Evid. 702; *Daubert v. Merrell Dow Pharmaceuticals* 1993).

Two cautions follow. First, a documented, repeatable procedure is far easier to defend than "training and experience." Second, do not oversell. A competing hypotheses matrix is a record of reasoning. It is not a validated scientific instrument, and Chapter 17 explains why nobody should testify as if it were. Offered honestly, as the way the unit made sure it considered the alternatives, it is hard to attack. Offered as proof, it deserves to be.

16.6 Settle the protocol with the prosecutor first

Before the first register is opened, the unit and the prosecuting authority should agree in writing on four points: which products are created and when, where they are kept, how they are labeled, and who is responsible for reviewing them for disclosure. Prosecutors dislike surprises more than they dislike paper.

Chapter 17. Limits and Honest Cautions

A monograph that asks investigators to list their assumptions should list its own weaknesses. There are six.

17.1 The techniques guarantee nothing

The primer says so itself. Applying the techniques is no guarantee of analytic precision or accuracy. What they improve is the sophistication, credibility, and usefulness of the assessment (US Government 2009, 5). Anyone selling them as an error proof method has not read the source.

17.2 The evidence base is thinner than the enthusiasm

The Intelligence Community adopted structured techniques largely on the strength of their logic and of Heuer's authority, not on controlled trials. A RAND study found little systematic evaluation of whether the techniques actually improve analysis and urged the community to start measuring (Artner, Girven, and Bruce 2016).

The academic critique is sharper. Chang and colleagues (2018) argue that many biases cut both ways, so that a technique built to cure overconfidence can produce underconfidence. They also argue that breaking a judgment into many small subjective ratings can add noise instead of removing it. An experiment with trained analysts did not find that those using ACH judged better than those who did not (Dhami, Belton, and Mandel 2019).

I take those findings seriously, and I draw a specific conclusion from them. The strongest case for these techniques in policing is not that they make any one detective more accurate. It is that they make the reasoning visible, reviewable, and correctable by somebody else. Accuracy in a criminal case comes from adversarial testing, and adversarial testing needs something written to test. A theory that lives only in the lead investigator's head can be reviewed by no one.

17.3 A matrix is not evidence

The techniques organize thinking about evidence. They do not create any. A hypothesis that survives every test in this monograph is still only a hypothesis until admissible evidence proves it. An ACH matrix is not probable cause, an indicator list is not reasonable suspicion, and a red team memo is not a confession.

17.4 Process theater

Any discipline can be performed without being practiced. Registers filled in after the arrest. Devil's advocates chosen for their docility. Matrices with two columns. An agency can adopt every form in the

appendix and change nothing about how it thinks. The test is whether a theory has ever changed because of the exercise. If none has, the unit is doing paperwork.

17.5 Contrarianism can paralyze

There is a failure on the other side as well. A unit that challenges everything decides nothing. The contrarian techniques are stress tests with a beginning and an end, and the primer gives each a legitimate outcome in which the original judgment stands (US Government 2009, 17). At some point the supervisor must decide, on the record, with the doubts noted. That is what the supervisor is for.

17.6 Culture eats technique

None of this survives a command climate in which dissent is punished. The primer's choice of the word "courageous" for the devil's advocate is an admission that the role carries risk (US Government 2009, 17). If the analyst who says "we have not excluded the roommate" is transferred to the property room, the forms are worthless. Leadership has to want the bad news.

Chapter 18. Standing It Up in a Department

18.1 A one page directive

Policy should be short enough to be read. A workable directive says four things.

1. Every major case, as the agency defines it, has an assumptions register and a source log opened within seventy-two hours and reviewed at each case review.
2. Every major case with a named suspect has a competing hypotheses matrix that includes the applicable null hypotheses.
3. No charging recommendation in a homicide or other designated case goes forward without a labeled Devil's Advocacy review and a written response.
4. Any change in the status of a load bearing source is reported to the prosecutor the same day.

18.2 Who does what

Role	Responsibility
Crime or intelligence analyst	Owns the method. Opens and maintains the register, the log, and the matrix. Facilitates the brainstorm
Lead investigator	Owns the facts. Supplies and corrects the entries. Responds in writing to the devil's advocate
Devil's advocate	From outside the case team and outside the lead's chain. Delivers the two page challenge
Supervisor	Reviews the products at each case review. Decides, signs, and protects the dissenters
Prosecutor liaison	Agrees on the protocol in advance. Receives source status changes. Reviews products for disclosure

The analyst as owner of the method is deliberate. In most agencies the civilian analyst is the person least invested in the lead detective's theory and least able to challenge it. A written directive gives the analyst standing.

18.3 Training

One day is enough to start. Spend the morning on the diagnosis and the four diagnostic techniques. Spend the afternoon running them on one of the agency's own closed cases, preferably one that went wrong. Nothing persuades a room of detectives like watching a register expose the assumption that sank a case they remember.

The primer is free and short. Issue it. For depth, Heuer (1999) and Heuer and Pherson (2010) are the standard texts.

18.4 The first ninety days

1. **Days 1 to 15.** The chief or the investigations commander issues the one page directive and names an owner. The owner meets the prosecuting authority and agrees on the protocol in Chapter 16.
2. **Days 16 to 30.** One day of training for one unit. Start with the unit that carries the most risk, usually homicide.
3. **Days 31 to 60.** Run the register, the log, and the matrix on every new major case in that unit. The analyst facilitates. Expect grumbling.
4. **Days 61 to 75.** Conduct the first formal Devil's Advocacy review on a live case approaching a charging decision.
5. **Days 76 to 90.** Review what happened. How many theories changed? How many load bearing sources turned out to be single points of failure? What did it cost in hours? Adjust the directive and extend it to the next unit.

18.5 Measuring whether it works

Clearance rate will not tell you. Better measures are the number of major cases with a current register and log, the number of cases in which a theory or a suspect changed after a structured review, the number of source status changes reported to the prosecutor, and the results of suppression and disclosure litigation over time.

The most valuable measure is the review of failures and near misses. The sentinel event approach, borrowed from medicine and aviation, treats a wrongful arrest or a collapsed prosecution as a system failure to be studied by all the stakeholders without blame (National Institute of Justice 2014). The products described in this monograph are the raw material for such a review. Without them, a review of a failed case is an argument about what people remember thinking.

18.6 Small agencies

A department with nine sworn officers and no analyst can still do this. The assumptions register takes one officer and one sheet of paper. The devil's advocate can be borrowed from the neighboring agency, the county prosecutor's investigator, or the regional fusion center, and the favor returned. An outsider is what the technique calls for in any event.

Conclusion

Intelligence analysts adopted this discipline because they got burned, publicly and catastrophically, by their own mind-sets. Policing has the same failure mode and, in wrongful convictions and unsolved cases, the same body count.

The remedy is not more data, more software, or another camera. It is the unglamorous practice of writing down what you are assuming, weighing where your information came from, forcing the alternatives onto the table, and paying someone to tell you that you are wrong before a defense lawyer does it for free.

The framework is public, it is free, and it is forty pages long. There is no excuse left for not using it.

Intelligence, counterintelligence, and their directorates of analysis invented this wheel. I write about them often and put what I can into the wild, in the hope that fellow Intelligence Community and law enforcement analytic cadres will not have to reinvent it.

Appendix A. The Twelve Techniques at a Glance

The techniques and their families are the primer's (US Government 2009). The questions, timing, and products are my adaptation for police use.

Technique	Family	The question it answers	Best moment in a case	What it leaves in the file
Key Assumptions Check	Diagnostic	What must be true for our theory to hold?	First 72 hours, and again before charging	Assumptions register
Quality of Information Check	Diagnostic	How good is what we know, and what is it resting on?	Continuous, and whenever a source changes	Source log
Indicators or Signposts of Change	Diagnostic	What would we see if this were developing?	Continuous	Indicator list with owners and review dates
Analysis of Competing Hypotheses	Diagnostic	Which explanations can we eliminate?	From the first named suspect to verdict	Dated, versioned matrix
Devil's Advocacy	Contrarian	What is the best case that we are wrong?	Before the charging recommendation	Labeled memo and written response
Team A/Team B	Contrarian	Which of two entrenched views does the evidence favor?	When units or agencies are split	Two briefs and a collection plan
High-Impact/Low-Probability Analysis	Contrarian	What if the thing we consider unlikely happens?	Annually, and at the start of high risk cases	Pathways, indicators, deflectors
"What If?" Analysis	Contrarian	Suppose it happened. How?	At the point of greatest confidence	Backward chain and observables
Brainstorming	Imaginative	What are all the possibilities?	At the start, and before final review	Clustered hypothesis set
Outside-In Thinking	Imaginative	What outside forces are shaping this problem?	Start of pattern and strategic work	Force list with data sources
Red Team Analysis	Imaginative	How does this look from the other side?	When the theory depends on what the target will do	Labeled first person memo
Alternative Futures Analysis	Imaginative	Which futures must our strategy survive?	Strategic planning and budget cycles	Four scenarios with indicators

Appendix B. Worksheets

These are blank formats for agency use. Adapt the columns to local practice and agree on them with the prosecuting authority first.

B.1 Assumptions register

Case number, working theory in one sentence, date opened, date of this review, and reviewer go at the head of the sheet.

Assumption	Basis	Confidence (highly likely, likely, possible)	What would defeat it	Load bearing?	Status at this review

B.2 Source log

Source	Type	Access: how does the source know?	Motive and conditions	Track record	Corroboration	Load bearing?	Status and date

B.3 Competing hypotheses matrix

Score each cell C, I, or N. Score across each row before moving to the next. Include the applicable null hypotheses.

Evidence, or expected evidence that is absent	Source quality	H1	H2	H3	H4: null	Diagnostic?
Inconsistencies						

B.4 Indicator list

Scenario or hypothesis	Indicator, stated as something observable	Collector	Review interval	Reading at last review

B.5 Devil's advocate memorandum

Head every page: DEVIL'S ADVOCACY REVIEW. A DELIBERATE CONTRARIAN EXERCISE. NOT THE ASSESSMENT OF THE INVESTIGATING UNIT.

1. The theory under review, in one sentence, as the case team states it.
2. The three assumptions most open to challenge, and why.
3. The weakest load bearing source, and what is known about its access and motive.
4. The best alternative explanation, and the evidence in the file consistent with it.
5. The evidence that should exist if the theory is correct and has not been found.
6. The three inquiries that would most quickly confirm or defeat the alternative.
7. The case team's written response to each point, and the supervisor's decision and signature.

Appendix C. A Supervisor's Checklist Before Charging

- ☐ The theory of the case is written as a single sentence that the whole team accepts.
- ☐ The assumptions register is current, and every load bearing assumption has been checked against the evidence, not against experience.
- ☐ Every load bearing source has a log entry showing access, motive, track record, and independent corroboration.
- ☐ No judgment rests on a single uncorroborated source without that fact being stated to the prosecutor.
- ☐ Each identification was reviewed for how it was administered and what the witness's confidence was at the first identification.
- ☐ Each forensic result was reviewed for what the examiner was told beforehand.
- ☐ The competing hypotheses matrix includes the null hypotheses, and each rejected hypothesis was rejected on a stated inconsistency.
- ☐ The evidence that should exist and does not has been listed and explained.
- ☐ A devil's advocate from outside the team has reviewed the full file, and the lead has answered in writing.
- ☐ The team has answered the question: if this person is innocent, how did this evidence come to exist?
- ☐ Everything inconsistent with the charged theory has been given to the prosecutor.
- ☐ Contrarian and red team products are labeled on every page.
- ☐ The supervisor has recorded the remaining doubts and the reason for going forward.

References

Books, articles, and reports

Artner, Stephen, Richard S. Girven, and James B. Bruce. 2016. *Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community*. Santa Monica, CA: RAND Corporation.

Carter, David L. 2009. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*. 2nd ed. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Chang, Welton, Elissabeth Berdini, David R. Mandel, and Philip E. Tetlock. 2018. "Restructuring Structured Analytic Techniques in Intelligence." *Intelligence and National Security* 33 (3): 337-356.

Cohen, Lawrence E., and Marcus Felson. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44 (4): 588-608.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. 2005. *Report to the President of the United States*. Washington, DC.

Dhami, Mandeep K., Ian K. Belton, and David R. Mandel. 2019. "The 'Analysis of Competing Hypotheses' in Intelligence Analysis." *Applied Cognitive Psychology* 33 (6): 1080-1090.

Dror, Itiel E., David Charlton, and Ailsa E. Péron. 2006. "Contextual Information Renders Experts Vulnerable to Making Erroneous Identifications." *Forensic Science International* 156 (1): 74-78.

Findley, Keith A., and Michael S. Scott. 2006. "The Multiple Dimensions of Tunnel Vision in Criminal Cases." *Wisconsin Law Review* 2006 (2): 291-397.

Global Justice Information Sharing Initiative and International Association of Law Enforcement Intelligence Analysts (IALEIA). 2012. *Law Enforcement Analytic Standards*. 2nd ed. Washington, DC: U.S. Department of Justice.

Heuer, Richards J., Jr. 1999. *The Psychology of Intelligence Analysis*. Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence.

Heuer, Richards J., Jr., and Randolph H. Pherson. 2010. *Structured Analytic Techniques for Intelligence Analysis*. Washington, DC: CQ Press.

Kahneman, Daniel. 2011. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

Kassin, Saul M., Itiel E. Dror, and Jeff Kukucka. 2013. "The Forensic Confirmation Bias: Problems, Perspectives, and Proposed Solutions." *Journal of Applied Research in Memory and Cognition* 2 (1): 42-52.

Klein, Gary. 2007. "Performing a Project Premortem." *Harvard Business Review* 85 (9): 18-19.

Natapoff, Alexandra. 2009. *Snitching: Criminal Informants and the Erosion of American Justice*. New York: New York University Press.

National Institute of Justice. 2014. *Mending Justice: Sentinel Event Reviews*. Washington, DC: U.S. Department of Justice.

National Registry of Exonerations. A joint project of the University of California Irvine Newkirk Center for Science and Society, the University of Michigan Law School, and the Michigan State University College of Law.

National Research Council. 2009. *Strengthening Forensic Science in the United States: A Path Forward*. Washington, DC: National Academies Press.

National Research Council. 2014. *Identifying the Culprit: Assessing Eyewitness Identification*. Washington, DC: National Academies Press.

Office of the Director of National Intelligence. 2015. *Intelligence Community Directive 203: Analytic Standards*. Washington, DC.

Office of the Inspector General, U.S. Department of Justice. 2006. *A Review of the FBI's Handling of the Brandon Mayfield Case*. Washington, DC.

Ratcliffe, Jerry H. 2016. *Intelligence-Led Policing*. 2nd ed. London: Routledge.

Rossmo, D. Kim. 2009. *Criminal Investigative Failures*. Boca Raton, FL: CRC Press.

Schwartz, Peter. 1991. *The Art of the Long View: Planning for the Future in an Uncertain World*. New York: Doubleday.

Senate Select Committee on Intelligence. 2004. *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*. S. Rep. No. 108-301. Washington, DC.

US Government. 2009. *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*. March 2009. https://www.cia.gov/resources/csi/static/Tradecraft-Primer-apr09.pdf

Cases

Brady v. Maryland, 373 U.S. 83 (1963).

Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

Franks v. Delaware, 438 U.S. 154 (1978).

Giglio v. United States, 405 U.S. 150 (1972).

Illinois v. Gates, 462 U.S. 213 (1983).

Kyles v. Whitley, 514 U.S. 419 (1995).

Statutes and rules

Federal Rules of Criminal Procedure, Rule 16.

Federal Rules of Evidence, Rule 702.

Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1017, 118 Stat. 3638.

Jencks Act, 18 U.S.C. § 3500.

About the Author

C. Constantin Poindexter holds a Master of Arts in Intelligence, a Juris Doctor, and a Graduate Certificate in Counterintelligence, together with the NICCS OSINT Certification and the CCI credential. He is a former operator in the U.S. Intelligence Community and a former certified law enforcement officer (North Carolina Department of Justice). He writes on intelligence, counterintelligence, national security, and analytic tradecraft, in English and Spanish, at constantinpoindexter.com/blog.

This publication is provided for professional education and does not constitute legal advice. Copyright 2026 C. Constantin Poindexter. All rights reserved.