

## THINKING LIKE AN INTELLIGENCE ANALYST

(Below is an excerpt from Dr. Tom O'Connor's class on Intelligence Analysis.  
Dr. O'Connor teaches at North Carolina Wesleyan College).

<http://faculty.ncwc.edu/toconnor/427/427lect04.htm>

So-called "mission-specific" schools of thought have evolved with respect to intelligence analysis, and these are usually named after the people who developed them, for example, the Kees, Helms, and Kent schools of thought (Ford 1993). What they all have in common, however, is the notion that thinking analytically is a skill like carpentry or driving a car. It can be taught, it can be learned, and it can improve with practice. Analysts learn by doing, and the best analysts have often learned from their mistakes. Mistakes in intelligence work are called "intelligence failures" or "strategic surprises" (Betts 1978, 1982; Ben-Zvi 1979). Mistakes are often disastrous – people die. It is important, therefore, to constantly work at improving the mind, never accepting old habits of thinking. The single most important cause of mistake is *cognitive bias*, a technical term for predictable mental errors caused by simplified information processing strategies. Since cognitive bias is inevitable, intelligence failures are inevitable.

Intelligence analysts must know themselves. They must understand their own lenses that they use to process, filter, channel, or focus information. These lenses are known by many names – mental models, mind-sets, or analytical assumptions. It is never a satisfactory excuse to say: "If we just had more information." Analysts already have more information than they can digest. It is never an excuse to say: "If we only had more useful information, more reliable HUMINT from knowledgeable insiders." More information isn't going to help in sorting through ambiguous and conflicting information. To understand China, for example, you need more than information on China. You need to have a perspective of your own, one that helps you get the production out on time and keeps things going between the watershed events that become chapter headings in the history books.

The disadvantage of bringing your own perspective to the information is that you become a specialist. You may become the last to see what is really happening when world events take a new and unexpected turn. During the reunification of Germany, for example, many German specialists had to be prodded by their generalist supervisors to accept the significance of dramatic new changes.

Intelligent analysts tend to treat what they *expect* to perceive as more important than what they *want* to perceive. They don't engage in wishful thinking; they think reflectively. They have analyzed their own background, not in a soul-searching sense of trying to find what they really want, but in terms of looking at how past experiences, education and training, cultural and organizational norms have influenced them to pay particular attention to some things and not to others.

Intelligence analysis doesn't involve an open mind. There's no such thing as an open mind, no matter how you define it. Preconceptions are inevitable. Intelligence analysts obtain objectivity by making basic assumptions and reasoning as explicitly as possible. Validity is obtained by the two-fold process of self-examination (regarding the assumptions made) and making your work challengeable by other analysts (reasoning explicitly).

A fresh perspective is sometimes needed. Often, an analyst assigned to work on a topic or country for the first time generates insights that have been overlooked by experienced analysts who have worked on the same problem for 10 years.

Analysts commonly try to shift back and forth from one perspective to another. They try to perceive things from an adversary's interpretation as well as from the United State's point of view.

The circumstances under which intelligence analysis is produced involves highly ambiguous situations, information that is processed incrementally, and pressure for early judgment, if not instant diagnosis. Customer demand for interpretive analysis is greatest within two or three days after an event occurs. Once the analysis is committed in writing, both the analyst and the organization have a vested interest in maintaining the original assessment.

Concepts and schemata (plural for schema) stored in memory also exercise a powerful influence on perception. With memory, there are usually only three ways in which information may be learned: by rote (repetition), by assimilation (comprehension), and by using a mnemonic device (e.g. HOMES for remembering the first letter of each of the Great Lakes). Rote and mnemonic techniques work best with information that doesn't already fit a conceptual structure or schema already in memory. Without an appropriate category for something in place, a person is unlikely to perceive it.

The idea of "working memory" refers to the phenomenon of constraint on the number of pieces of complex information people can keep in their heads all at once. People are not ordinarily made to grasp complexity or for multitasking: about seven – plus or minus two – is the limit on the number of things a person can keep in their head all at once. The practical implications come into play when we try to think in terms of pros and cons. Few people can consider more than three arguments in favor of something plus three arguments against something, plus at the same time consider and overview or how all the arguments balance each other.

Judgment is what analysts use to fill gaps in their knowledge. It entails going beyond the available information and is the principal means of coping with uncertainty. It always involves an analytical leap, from the known to the unknown. While the optimal goal of intelligence collection is complete knowledge, this goal is seldom reached in practice. Almost by definition, intelligence involves considerable uncertainty and tolerance for ambiguity.

The most common technique of intelligence analysis is "situational logic," sometimes called the "area studies" approach. This involves generating different hypotheses on the basis of considering concrete elements of the current situation. Broad, global generalizations are avoided. Even though everybody knows this to be untrue, every situation is treated as one-of-a-kind, to be understood in terms of its own unique logic. A single country is looked at, although on multiple interrelated issues.

Next, the analyst seeks to identify the logical antecedents and consequences of the situation. This is called building a "scenario," and the analyst may work backwards to explain the origins of the current situation or forward to estimate the future outcome. Situational logic is cause-and-effect logic, based on the assumption of rational, purposive behavior. The analyst identifies the goals being pursued by the foreign actor and explains why the foreign actor believes certain

means will achieve certain goals. One of the major risks with this approach is projecting American values onto foreign actors.

Another operating mode of intelligence analysis is "applying theory," sometimes called the "social science" approach. Theory is not a term used much in the Intelligence Community, but "applying theory" involves drawing conclusions from generalizations based on the study of many examples of something. Theory enables the analyst to see beyond transient developments, to recognize which trends are superficial and which are significant. For example, suppose some event happens in Turkey. The analyst applies what they know about developing countries in precarious strategic positions to predict how Turkey will react militarily and politically. Multiple countries are looked at in terms of a single, overriding issue.

Sometimes situational logic and applying theory contradict one another. Consider Saudi Arabia, for example. A theoretical approach would apply the axiom that economic development and massive infusion of foreign ideas lead to political instability. It would suggest that the days of the Saudi monarchy are numbered, although analysts using a situational logic approach would conclude that no such threat exists to the Saudi royal family.

A third approach is comparison, where the analyst seeks to understand current events by comparing them with historical precedents in the same country or with similar events in other countries. It differs from theory in that conclusions are drawn from a small number of cases, whereas theory is generated from examining a large number of cases. This approach is quite useful when faced with an ambiguous and novel situation because it looks at how the country handled similar situations in the past or how similar countries handled similar situations. Historical precedent is influential, but one must be careful in arguing from analogies with the past.

Intelligence analysts "analyze rather than analogize." They tend to be good historians, with knowledge of a large number of historical precedents. They don't just jump on the first analogy that comes along. Instead, they pause to look at the differences and similarities in the precedent, and always ask in what ways it might be misleading. The most productive use of the comparative approach involves suggesting hypotheses and highlighting differences, not drawing firm conclusions.

Analysis begins when the process of absorbing information stops. Analysts insert themselves into the process of selecting, sorting, and organizing information. They bring their own conscious or subconscious assumptions and preconceptions to the analysis. Different analysts have different analytical habits and preferences for particular analytical strategies. Analysts trained in area studies tend to prefer situational logic. Analysts with a social science background are more likely to favor theoretical or comparative techniques. On the whole, the Intelligence Community is far stronger in situational logic than in theory. Academics, on the other hand, rely extensively on theory and generalize too much.

The concept of "diagnosticity of evidence" refers to the extent to which any piece of information helps to determine the likelihood of alternative hypotheses. Information has diagnostic value if it makes at least some of the alternative hypotheses inconsistent. For example, a high temperature has value in telling a doctor that a patient is sick, but it has little diagnostic value because it supports so many possible hypotheses about the cause of a patient's illness. Scientific method is based on the procedure of rejecting hypotheses. Therefore, most of the best intelligence work involves the analysis of disconfirming evidence. For instance,

in a situation where it can readily be seen that the sequence of events is 1-2-3, a good intelligence analyst would check to see if the sequence 2-1-3 also fits the pattern, theory, or logic.

The point at which an intelligence analyst stops, and realizes that they have enough information is when they feel they have the minimum information necessary to make an informed judgment. Generally, that is the point at which additional information will not improve the accuracy of an estimate. It's a matter of confidence, not overconfidence, in one's judgment. Actually, it's a combination of amount of information, accuracy, and analyst confidence.

Mathematical modeling has been done on the processes by which analysts weigh and combine information on relevant variables (Slovic & Lichtenstein 1971). Invariably, these studies have shown that statistical models, built on regression analysis, are far superior to conceptual models built on an analyst trying to describe in words what they do. However, once you have constructed a mathematical model, the accuracy of the analytical judgment will be determined mostly by the accuracy and completeness of the data. This is called "data-driven" analysis, and it's entirely appropriate for some uses, but not for others. An example of appropriate use is in military intelligence, for example, estimating combat readiness. In this case, the rules and procedures for estimating combat readiness are relatively well established, so a mathematical model would help arrive at accurate judgments depending upon how accurate the source of the data is.

"Conceptually-driven" analysis, on the other hand, doesn't rely upon any agreed-upon schema. Analysts are left to their own devices. Other analysts examining the same data may reach different conclusions. The daily routine of an intelligence analyst is driven by incoming wire service news, embassy cables, clandestine- and open-source information. Interpretation will be ongoing and based on an implicit model in the analyst's head about how and why events normally transpire in the country for which the analyst is responsible. Accuracy of judgment depends almost exclusively on accuracy of the mental model, not the data.

Mental models are neither good nor bad, but unavoidable. When information is lacking, analysts often have no choice but to lean heavily on mental models. They must remain open to new ideas, however, and avoid mental blocks and ruts. To accomplish this, creativity exercises are sometimes useful. Sometimes, agencies implement Peer Review, where at least one of the reviewers is not from the branch that produced the report or is required to play the Devil's Advocate. Mirror-imaging, or thinking "if I were a Russian intelligence officer," is also useful but dangerous. People in other cultures do not think the way we do. Another creativity technique is the "crystal ball" where you imagine some perfect intelligence source (such as a crystal ball) has told you a certain assumption is wrong. If you can develop a plausible alternative scenario, it suggests your original estimation is open to some question. Gaming simulation also serves the purpose of creativity.

Analysts should keep a record of unexpected events and think hard about what they might mean, not disregard them or explain them away. They should pay careful attention to any unexpected developments that might signal an impending event. Any such tactical indicators that are inconsistent with strategic assumptions should trigger a higher level of intelligent alert.

## **COMMON CREATIVITY PRINCIPLES APPLIED TO INTELLIGENCE**

*Deferred Judgment.* This is the principle that the idea-generation phase of analysis should be separated from the idea-evaluation phase, with all judgments deferred until all possible ideas have been thought out.

*Quantity Leads to Quality.* This principle reflects the assumption that the first ideas that come to mind are the least useful. It's not the quantity of information, but the quantity of thinking.

*Cross-Fertilization of Ideas.* This is the principle of combining ideas to form more and even better ideas. As a general rule, people generate more creative ideas when teamed up with others. A diverse group is obviously preferable to a homogeneous one.

*Sense of Security.* Of all the organization factors that affect productivity, none is more important than a sense of security – in one's job, in one's responsibilities, and in freedom from close supervision.

*Competitive Analysis.* This is the deliberate fostering of separate analysis centers (decentralization) so that, while each has full access to the same information, a comparison can be made between their two separate assessments.

*Devil's Advocate.* This is the Rumsfeld Commission notion of having a B team which plays the role of devil's advocate, and always offers a competitive point of view to an assessment in circulation.

Other than creativity, the analyst needs to know how to break problems down into their component parts, assess each part individually, and then put the parts back together. In many ways, this is the essence of analysis – the difference between thinking about a problem and really analyzing it. You wouldn't want to do this for your everyday decisions, but advanced techniques may be appropriate for complex intelligence problems. One such technique is the *eight-step ACH (Analysis of Competing Hypotheses) developed by Richards Heuer (1999):*

1. Brainstorm the possible hypotheses with other analysts. Consider the hypotheses you don't want to waste time on to simply be unproven hypotheses. Always consider the possibility that an opponent is trying to deceive you. Keep the number of hypotheses manageable; seven is a good number.
2. Make a list of significant evidence for and against each hypothesis. Include your own assumptions or logical inferences about another person's or country's intentions, goals, and standard procedures. Note the absence as well as presence of evidence. Ask yourself the question: If this hypothesis is true, what should I expect to be seeing or not seeing? What you are not seeing may represent the need for greater data collection.
3. Prepare a matrix with hypotheses across the top and evidence down the side. Analyze the "diagnosticity" of the evidence by marking which items are most helpful in judging the relative likelihood of alternative hypotheses. Use your own marking system, pluses, minuses, or whatever.
4. Delete evidence and arguments that have no diagnostic value. Save these items in a separate list as a record of information you considered. You are establishing an audit trail for your work. If others disagree with your assessment, they can be provided with this separate list.

5. Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove hypotheses rather than prove them. Look at the minuses in your matrix. Hypotheses with the most minuses are the ones you should start with. You should be spending more time than you thought you should on these least likely hypotheses. The one that is most likely is usually the one with the least evidence against it, not the one with the most evidence for it.
6. Analyze how sensitive your conclusion is to a few critical pieces of evidence. Consider the consequences for your analysis if that critical piece of evidence were wrong, misleading, or subject to a different interpretation. Put yourself in the shoes of a foreign deception planner to evaluate motive, opportunity, means, costs and benefits of deception as they might appear to the foreign country.
7. Report your conclusions by discussing the relative likelihood of all the alternative hypotheses. If you say that a certain hypothesis is the most likely one to be true, you are saying that there is anywhere from a 55-percent to 85-percent chance that future events will prove it correct. That leaves anywhere from 15-45 percent possibility that any decision made on your judgment will turn out to be a wrong decision. You should discuss these possibilities in your narrative report.
8. Identify things in your report that the policymaker should look for that would alter your appraisal of the situation. In other words, specify in advance what it would take for you to change your mind.

## **CERTAINTY AND UNCERTAINTY**

The information environment that intelligence analysts work in is somewhat unique. Information comes from a diverse set of sources: newspapers and wire services, observations by Embassy officers, reports from controlled agents and casual informants, information exchanges with foreign governments, photo reconnaissance, and communications intelligence. The analyst only has limited control over this environment. Information on some important topics is sporadic or nonexistent. Most human-source information is second hand at best.

Intelligence analysts work with secondhand information. Analysts should give little weight to anecdotes and personal case histories unless they are known to be typical. In cases of missing information, analysts should factor this into their calculations by adjusting confidence in their judgment accordingly. In some cases, "fault trees" are used, which are schematic drawings showing all the things that might go wrong with any endeavor.

Analysts should never place too much reliance on small samples. When working with a small but consistent body of evidence, analysts need to consider how representative that evidence is of the total body of potentially available information. They should avoid "best guess" strategies.

The approach can be compared to the work of a historian, and historians use certain criteria to attribute causality. The historian tries to make a coherent whole out of the events studied, looking for dominant concepts or leading ideas which illuminate the facts. The historian then traces the connections between the ideas themselves, and then constructs a narrative of the events, showing how they make the main ideas intelligible (Carr 1961). Historians commonly observe only a single case, but they don't avoid causality. They sometimes make best guesses because of a need to impose order on their environment. The intelligence analyst cannot afford this luxury. Random events often look patterned, and people sometimes appear to follow patterns even though the reward structures that drive their behavior are random (Skinner 1948).

Judgments about correlation are fundamental to intelligence analysis. For example, assumptions about worsening economic conditions are correlated to increased political support for opposition parties. Correlation is not causation, however, it's better than speculation.

The act of analysis itself influences the imaginative process. The act of constructing a scenario for a future event makes that event more readily imaginable. Analysts need to know when they are taking leaps into uncertainty. There are two ways to express uncertainty: one is to make a "subjective probability assessment"; the other is to use statistics. Verbal expressions of uncertainty – such as "possible," "probable," "unlikely," "may," and "could" – are forms of subjective probability assessment. When expressing numbers, like 1-99 percent probability, one is using the language of statistics. To calculate mathematically the probability of a scenario, the proper procedure is to multiply the probabilities of each event. Thus, for a scenario with three events, each with 70% certainty to the analyst, the probability of the scenario would be  $.70 \times .70 \times .70$ , or about 34%. Adding further variables tends to lower the probability of the scenario. CIA estimates are rarely stated in terms of quantitative probabilities, but by themselves, verbal expressions of probability are empty shells. The reader or listener fills them with meaning through the context in which they are used.

Intelligence analysts can improve their performance by evaluating their past estimates in light of hindsight. Oversight will do this anyway. There is a tendency to believe analysts should have foreseen events that were, in fact, unforeseeable on the basis of information available at the time. It should always be recognized that conclusions are driven by how the evidence is interpreted rather than by the evidence itself. Especially critical are assumptions about what is in another country's national interest and how things are usually done in that country. Assumptions are fine as long as they are made explicit in the analysis.

The organization in the CIA responsible for making estimates is the National Intelligence Council. There, your work will be evaluated and refined by senior analysts (often not from the CIA) who are called NIOs (National Intelligence Officers). Nothing goes to the Director of Central Intelligence unless through one of them.

From 1950-1973, the CIA operated the Office of National Estimates (ONE), a special group for developing National Intelligence Estimates (NIEs). NIEs are the reports presented by the Director of Central Intelligence to the National Security Council. One of the civilian members of ONE was Professor Sherman Kent, Yale Professor. His method of balancing mathematics with verbal probability is sometimes referred to as the "Kent" or "Yale" method:

100% -- certainly  
93% give or take 6% -- almost certainly  
75% give or take about 12% -- probably  
50% give or take about 10% -- chances about even  
30% give or take about 10% -- probably not  
7% give or take about 5% -- almost certainly not  
0% -- impossible

The job of an intelligence analyst is to protect US interests by providing useful, high-quality analysis to policymakers, lawmakers, warfighters, law enforcement officers, negotiators, and other officials. These individuals indicate what they expect to gain from a request for analysis – specialized information, cause-and-effect analysis, cost-benefit assessment of tactical alternatives, etc. Sometimes the initiative comes from the intelligence side of the relationship,

and it is here that people who monitor agencies (such as Congressional Oversight committees) usually become involved.

While the requesters of intelligence reports are free to ask for anything, an intelligence analyst working in the CIA, for example, would be expected to have proficiencies and skills in the following areas:

- Opportunities and dangers for US interests, especially unexpected developments that may require a US reaction
- Motives, objectives, strengths, and vulnerabilities of adversaries, allies, and other actors
- Direct and indirect sources of US leverage on foreign players and issues
- Tactical alternatives for advancing stated US policy goals

Skillful intelligence analysts support the policymaking process without engaging in policymaking per se. They target the policymakers' specific interests in a substantive issue, knowing full well that the policymaker doesn't want a "story" or general background information. The goal of intelligence reports is to be "value-added." The responsibility and risk of choosing what actions to take remains with the policymaker.

Policymakers often have an interest in long-shot threats and opportunities. The skillful intelligence analyst doesn't concentrate on when the event they are interested in will come about, but provides a tough-minded assessment of the how and why other events would have to take place first.

Rarely will policymakers wait for intelligence analysis. Reports or briefings must be delivered in timely fashion. Analysts will always make sure, however, that their assessments address the operational concerns of hands-on policy officials. They may use the "so-what" test – does what they have to say address what policymakers need to know to get their jobs done; or they may use the "action-support" test – does what they have to say provide actionable information or insight.

Intelligence analysts need access and credibility with key policymakers. They increase their access by making it clear to officials what's in it for them if they read an intelligence report. They increase their credibility by producing sound assessments that can be relied on. Analysts must convey their distinctive expertise on an issue by having a sophisticated analysis that shows depth of research, while at the same time is short enough to fit in the prescribed space.

In the intelligence report, analysts should take care to distinguish from direct evidence (satellite imagery, electronic intercepts) and testimonial evidence (embassy reporting, clandestine reports). On complex matters (such as attitudes and plans of foreign leaders), analysts should declare their level of confidence in the assessment.

Assessments should emphasize well-documented events in terms of trends, patterns, and precedents that underscore dangers or opportunities for US interests. Whenever possible, the calculus or logic leading from the factual basis to the actionable finding should be spelled out (e.g., rules used to establish degrees of risk).

When analysts face uncertainty, or deal with incomplete information, they should always clearly state the assumptions that allow them to go beyond the hard evidence into matters that require estimation or interpretation.

## DRIVERS AND LINCHPINS

With estimative or "outlook" assessments, analysts should always spell out the "drivers" that will have the greatest impact on subsequent developments. "Drivers" are key variables and unknown factors that analysts judge most likely to determine the outcome of a complex situation. At times, the economy is the key uncertain factor; at times the loyalty of the security forces; at times the leadership skills of a president or dictator. At times, all three are judged as carrying equal weight as "drivers."

The analyst's working assumptions about the drivers are referred to as "linchpin" assumptions because they are the premises that hold the argument together and warrant the validity of the conclusion. The following are some examples of statements containing drivers and linchpins:

- "The loyalty of the military is the key factor in determining Egyptian stability in the short term. The military probably will continue supporting the government. Therefore, the government is unlikely to be seriously threatened by opposition forces over the next few years."
- "Castro's skill in handling recurrent anti-regime incidents will largely determine the regime's staying power over the next several months. He probably will continue to diffuse anti-regime pressures with a mix of carrots and sticks. Thus, a serious threat to regime stability is unlikely."

Linchpin assumptions are the most debatable and subject to error. Therefore, analysts should defend "linchpins" more carefully than "drivers." For instance, in the Egyptian example, the analyst should offer convincing evidence for the "linchpin" that "the military probably will continue supporting the government." In general, both drivers and linchpins should be precisely stated and well defended.

When the US stake is high, or plausible alternative outcomes are in the range of, say, 20 percent or greater, the outlook section of an intelligence report should contain enough information to enable policymakers to do contingency planning. This means that each potentially important alternative outcome should provide an analysis of drivers and linchpins or plausible reversals of drivers and linchpins. All important factors, expected or unexpected (e.g., crop failures, natural disasters), should be analyzed as events that might or might not trigger a major shift in direction of the main pattern of subsequent events. These additional factors should have their relative importance ranked, but analysts should avoid phrases that compound uncertainty with confusion, like in "real possibility", or "good chance." As a rule, analysts use constructions that tie the outcome to the driver and linchpin assumptions, rather than make flat predictions. Here's an example of an intelligence statement containing uncertainty:

- Castro is unlikely to be forced out of office over the next six months unless his security forces mishandle disturbances and trigger prolonged violent riots. On balance, there is a less than one-in-five chance of this happening.

Notice the switch in focus from *whether* something will happen to *how* it would happen. In the above example, the analyst might rely on evidence of security force morale, lapses in salary or training, rivalries between elite, paramilitary security forces and regular forces, to justify the prediction that security forces getting out of control would be a factor. In general, the intelligence

information (unless classified) will contain lists of key individuals and group players in the Cuban security forces with such tendencies, complaints, or rivalries.

Also in the Cuban example, there's a linchpin assumption that violent riots would lead to revolution, or forcing Castro out of office. This is an example of a "scenario", and the analyst needs to think backwards and generate one or more plausible "how-it-could-happen" scenarios by postulating who would have to do what, when, how, and why.

The following definitions have some standardized usage in intelligence work:

- Fact – Verified information; something known to exist or to have happened
- Information – The content of reports, research, and reflection on an intelligence issue that helps to evaluate the likelihood that something is factual and thereby reduces uncertainty
- Direct information – Information relating to an intelligence issue the details of which can be considered factual because of the nature of the source (imagery, intercepts, observations)
- Indirect information – Information relating to an intelligence issue the details of which may or may not be factual because of some doubt about the source's reliability, the source's lack of direct access, or the complex (non-concrete) character of the contents (hearsay from clandestine sources, foreign government reports and local media accounts)
- Sourcing – Depiction of the manner in which information was obtained, in order to assist in evaluating the likelihood that the content is factual
- Data – Organized information that provides context for evaluating the likelihood of factualness

The following example will demonstrate all these terms:

"We believe country X has begun a major crackdown on the "Extremist Movement" which the government holds responsible for the campaign of terrorism over the past two years. The Army has been ordered to support the police in cleaning out Extremist strongholds (direct information), according to special intelligence (sourcing). The President of X reportedly is using last week's attack on a shopping center in a working-class neighborhood to justify calling upon the Army to close down the terrorist campaign (*indirect information*).according to a reliable clandestine source (*sourcing*). The pro-government press reports (*sourcing*) the *Extremists* cannot match Army firepower and are taking high casualties (*indirect information*). A US Embassy observer reports (*sourcing*) seeing Army trucks deliver more than 100 prisoners, some badly wounded, to the Central Prison (*direct information*). According to country X police officials (*sourcing*),these were part of the 1,000 *Extremists* rounded up so far in the crackdown (*indirect information*). CIA's "Country X Terrorism Chronology" indicates this is the first time the Army has been used against the *Extremists* since the terrorism campaign began in 1993 (*data*)."

Intelligence analysts would report contradictory or inconsistent information as:

- According to special intelligence, President X has canceled his planned trip to country Y. Imagery indicates no signs of the airport security procedures that usually are undertaken for a Presidential flight. The media in both countries, however, continue to report plans for the scheduled peace talks between the two countries.

- We have no direct information on President X's involvement in narcotics trade, despite persistent charges in the media by his political opponents that his reelection campaign is being financed with funds he obtained from his engagement in trafficking.

This is how intelligence analysts would source information:

- US Embassy officers observed sparse crowds at several political rallies.
- In the opinion of a US Embassy official, political support for President X has increased in recent weeks.
- According to special intelligence, President X is telling confidants he will fire Prime Minister Y next week.
- President X is reported to be ready to fire Prime Minister Y, according to a reliable clandestine source

This is how a complex, high-stake intelligence issue would be reported:

- We believe country X is preparing to invade country Y. The deployment of military forces of country X along the border of country Y is consistent both with routine annual military exercises and with preparations for an invasion. Special intelligence, however, indicates two key generals have been called back from an important arms purchase mission abroad. A reliable clandestine source reports that two generals who oppose an invasion have been placed under house arrest. US Embassy officers report extensive civil defense drills and the closing of the national airport to civilian flights. According to a CIA database, these actions have not been undertaken in previous military exercises.

This is how the mindsets or attitudes of foreign leaders would be reported:

- Multiple reliable clandestine sources report President X is optimistic about economic prospects.
- President X probably is optimistic about economic prospects. Multiple reliable clandestine sources report his recent upbeat statements. Moreover, recently released IMF statistics indicate a marked improvement in exports and worker productivity.

When it comes to treaties, law, and binding agreements, the intelligence analyst should avoid flat statements about who is or is not breaking a contract. That is the job of the policymaker. Here's how such an instance would be reported:

- The following information relates to the recent behavior of country X regarding its pledge, under the US economic assistance agreement, to cease support of anti-government guerrilla forces in country Y:
  - The President of country X told the US Ambassador that all official assistance had been terminated, although small-scale shipments of weapons by private groups that sympathize with the guerrillas' cause might still be taking place.
  - According to a reliable clandestine source, a senior assistant to the President of X has ordered the military to hide small shipments of weapons for the guerrillas in trucks engaged in normal cross-border trade.

-- Special intelligence indicates that a military mission from country X is to await further orders before purchasing abroad communications equipment requested by the guerrillas.

Intelligence analysts often include footnotes, references, maps, imagery, or other graphics to enhance the credibility of their reports.

Here's some examples of strongly-made assessments by intelligence analysts:

- The latest information shows country "X's" expenditures on weapons-related technology *increased sharply* in 1995 after several years of little or no growth.
- DI data demonstrate that incidents of human rights violations in country "Y," as reported by international monitors and reliable clandestine sources, are *decreasing for the first time* since the military government took power in 1989.
- The DI database shows that terrorist incidents in country "Z" *are taking on a pattern* of attempting to intimidate the foreign business community.
- Examination of DI chronologies of the seven national elections since the restoration of civilian government in country "A" indicates that recent government use of armed thugs to break up opposition political rallies is *without precedent*.

The *cause-and-effect* relationship between Premier "B's" political difficulties and his calling for military exercises to turn public attention to the "foreign threat" is by now well established.

But note how the legal word "evidence" is used sparingly:

- Information from special intelligence and clandestine reporting indicates that Justice Minister X has been involved in the narcotics trade.
- Special intelligence and clandestine reporting indicate that Justice Minister X has been involved in the narcotics trade.

## **DENIAL AND DECEPTION**

In the case of deception, here's how it would be reported. Deception is defined as the manipulation of information by a foreign government, group, or individual to get US intelligence analysts to reach an erroneous conclusion. The only defense an intelligence analyst has is the strength of their all-source information.

- President X assured the US Ambassador on Tuesday that all missile sites in his country had been dismantled, but imagery from last week shows no dismantling activity at the 29 missile sites listed in CIA's database.
- We have no direct information to support reports by a clandestine source with access to Colonel X that anti-government military forces loyal to him are about to undertake a military coup. No other clandestine sources with military contacts are reporting advanced coup planning or unusual movements of troops. Opposition political groups abroad report that they are unaware of any serious coup activity, according to multiple reliable clandestine sources. The government, therefore, could be running a deception operation involving Colonel X, to smoke out "disloyal" officers.

Deception operations can be divided into two subsets: "Denial" – measures taken to protect secrets through concealment, camouflage, and other activities that degrade collection systems; and "Disinformation" – operations to feed analysts false or partly false information through the use of double agents and manipulation of diplomatic and media as well as intelligence channels.

Here are some warning signs that a deception operation might be active:

1. The foreign entity has the MEANS to undertake sophisticated deception operations.
2. The foreign entity has the OPPORTUNITY to counter a collection system or platform by knowledge of the periodicity of collection vehicles
3. The foreign entity has the MOTIVE to deceive by seeing a high payoff from distorting US analysis
4. Suspicious gaps in collection, or changes in the usual range and volume of information flow
5. Contradictions to carefully researched patterns in and adversary's priorities & practices
6. Suspicious confirmations from new streams of information from clandestine sources

### **INTELLIGENCE FAILURE AND SURPRISE**

An intelligence failure can be defined as *any misunderstanding of a situation that leads a government or its military forces to take actions that are inappropriate and counterproductive to its own interests* (Schulsky & Schmitt 2002: 63). It is a mistake to think that any human endeavor, including intelligence, will be error-free. Enemies may be underestimated or overestimated, and events that should be predictable go unforeseen. Because intelligence work is the product of a team effort, there are certain peculiarities common to the bureaucratic environment that help explain failure. Arguably, the worst kind of failure is surprise attack. [For more on the subject of intelligence failure, see the [Lecture on History and Lessons of Intelligence Failure](#)]

Reasons for intelligence failure can be classified in a number of ways:

1. Overestimation -- this is perhaps the most common reason for failure, and one which, if uncorrected, can lead to the continuation of error for a long time. Examples include the long Cold War period in which the U.S. consistently overestimated the "missile gap" between the U.S. and Soviet Union. Critics of the Iraq invasion say this was the main kind of error that happened in the estimation of Saddam Hussein's warfare capability.
2. Underestimation -- this occurs when intelligence or political leadership seems unwilling to be receptive to warnings, or completely misreads the enemy's intentions. A classic example is Stalin in 1941, who didn't want to hear about the possibility of Hitler invading Russia, even though the British and Americans tried to tip him off.
3. Subordination of Intelligence to Policy -- this happens when judgments are made to produce results that superiors want to hear instead of what the evidence indicates. It is the most widely discussed and analyzed type of intelligence failure, although some discussions talk about a related error, bias.
4. Lack of communication -- the lack of a centralized office often creates this problem, but it more typically results from when you have different officials from different agencies who have

different rules on who and how they communicate, or few analysts who work on-the-fly for different agencies and don't have full-time intelligence responsibilities.

5. Unavailability of Information -- regulations and bureaucratic jealousies are sometimes the cause of this, but the most common problem involves restrictions on the circulation of sensitive information. When there is virtually no intelligence at all, this is called something else, ignorance.

6. Received Opinion -- this is also called "conventional wisdom" and consists of assertions and opinions that are generally regarded in a favorable light, but have never been sufficiently investigated.

7. Mirror-Imaging -- this is technically defined as "the judging of unfamiliar situations on the basis of familiar ones," but most often involves assessing a threat by analogy to what you (your government or a similar government) would do in a similar position.

8. Over-confidence -- this occurs when one side is so confident of its ability that it projects its reasoning onto the other side and believes that since it would not do something itself, neither will the other side. The classic case is the Yom Kippur war of October 1973.

9. Complacency -- this happens when you know the enemy might do something, though you are not sure what or when, and yet you do nothing anyway. The classic example is the British who did nothing in the weeks leading up to the Falkland War of 1982.

10. Failure to connect the dots -- this occurs when the connections between bits of intelligence are not put together to make a coherent whole. It is most easily observed in hindsight.

## **ADVANCED INTELLIGENCE ANALYSIS**

Analysis is the separation of a whole into its parts to allow an examination and interpretation of the information. Analysis typically involves certain methods and techniques, some of which are statistical, others which are not, which reveal patterns and trends that often reveal the probability of conclusions. Analysis is the "working" of collected intelligence to explore contexts and anticipated events in their fullest political, military, economic, diplomatic and cultural implications. Intelligence analysis has been an integral part of the work of intelligence agencies for many years, and some advanced techniques have emerged. The CIA, for example, has the Advanced Analytic Tools office in the Directorate of Science and Technology where some of its top analysts are employed. Modern Scientific and Technical Intelligence Analysis (commonly abbreviated S&T) first began in 1981 with the British Security Service's (MI5) switch from reliance on agents to reliance on more technical and electronic forms of surveillance (wiretaps, computer taps, and bugs). There are four (4) main analytical tools used in advanced analysis.

(1) *Psychological profiling* -- first used around 1986 to map out the minds of foreign leaders. Under the direction of CIA Chief Profiler, Jerrold Post, the technique of profiling used was much more clinical and psychodynamic than FBI methods. Since then, the CIA has evolved its profiling capabilities to center around the psycholinguistic analysis of oral and written rhetoric by foreign leaders, and some modern techniques even include gait analysis, or what you can tell from how a person walks. Dr. Post is Director of the Political Psychology Program at George Washington University, founding Director of the CIA Center for the Analysis of Personality and Political Behavior, and co-author of *Political Paranoia: The Psycho-politics of Hatred*. One of

the more well-known profiles Dr. Post has put together is on Yasir Arafat and available at the [ICT](#) website.

(2) *Estimative intelligence* -- involves national estimates about the strength, size, and capabilities of another nation's military and/or counterintelligence threat. All sources, even open sources, are often used for data collection, but analysis in this area tends to be driven by the need for justifying military or technical superiority, and there are similarities between an intelligence analyst and an economic analyst in this respect, but the hard part is sociological estimation of the "mood" of a nation. Estimative intelligence is all about judging the probable outcomes of something - you do one thing, and others do something else. An extensive bibliography on estimative intelligence is available at the [Muskingum College](#) website.

(3) *Warning intelligence* -- involves threat assessment, the analysis of surprise, intelligence failures, and other indicators of catastrophe. It's the use of hindsight to improve foresight, and the ultimate product is a set of Indicators and Warnings (I & W) to detect indicators of potential threats while sufficient time exists to counter those same threats. The intelligence mechanism, however, always functions better after a crisis than before. Much of military science is related to this type of intelligence in that famous military battles are studied (e.g., Barbarossa, Pearl Harbor, Dieppe, Arnhem, Battle of the Bulge, Tet Offensive), although some of these battles are not strictly cases of warning problems as much as they are an order-of-battle analysis problem (e.g., Arnhem). Pearl Harbor, the Chinese surprise offensive in the Korean War, and the Yom Kippur War constitute the classic case studies in warning problems. The US tries to centralize the warning function by naming at least one officer to be National Intelligence Officer (NIO) for Warning. The National Warning System that the NIO is responsible for concentrates on threats judged to be about six months away. In the business community, warning intelligence is called competitive intelligence, and used to anticipate market shifts as well as corporate allies and enemies. There's also the area of Emergency Preparedness which uses a type of warning intelligence to prepare for disasters, and much of Homeland Security preparation is of this kind. A basic paper on the history of post-mortem, warning intelligence can be found at the [Sherman Kent Center](#).

(4) *Fusion intelligence* -- involves joint or collaborative efforts to develop multi-intelligence products of a global, regional, or national nature. Real-time data sharing and combined work on analytic processes are hallmarks of this activity, and frequently involve public-private partnerships. Within government intelligence agencies, fusion intelligence is sometimes handicapped by the "one-nation rule" or custom in which analytic products are only shared with one nation (say between the UK and US or Israel and US) and are not passed on to a third nation to avoid problems of hearsay. In the Homeland Security context, fusion intelligence tends to be the same as efforts to achieve better interoperability of communications, and is sometimes referred to as unified command. This kind of intelligence is highly important in the post-9/11 era where moving targets (subnational, global terrorists) are involved. Law enforcement agencies seem to have embraced the fusion concept quite strongly. An example of a fusion center can be found at the [Coast Guard](#) site.

Advanced intelligence (like the above) is usually hard to come by. Far more common is the collection of vast amounts of ordinary information. Analysts should know what to collect intelligence on, but the consumers of intelligence often don't know what they want. Therefore, collection for the sake of collection seems to be the driving force. At one time the DIA collected 200 different things about a foreign entity, and the CIA had 83 standard collection categories for intelligence on each country (Laqueur 1985). That was before the CIA method of KIQ (Key

Intelligence Questions) was introduced, and coordination of tasking became common within the Intelligence Community. The following two categories have typically played a large role in intelligence affairs as the key things to look at.

(1) *Economic intelligence* -- This consists of the things that economists collect data on, such as population demographics, labor statistics, crop statistics, manufacturing production rates, import-export rates, natural resources, and public opinion.

(2) *Science & Technology intelligence* -- this consists of the better-kept secrets of a foreign entity, including their research into technology development and/or their plans for the uses of such technology, such as weapons or space exploration. There is a tendency in this category to use the worst-case scenario approach.

## **A GLOSSARY OF INTELLIGENCE PRODUCTS**

**ACTIVITY FLOW CHART** -- this is a chart that shows exact occurrences and dates; e.g., "Mr. A sells one kilo of cocaine to Mr. B for \$25,000." They include boxes and symbols connected by direct and dotted lines. They are best used for money transactions.

**ASSESSMENTS** -- These are written reports that summarize the results of investigative research. They normally include charts, tables, graphs, and maps mixed in with words.

**ASSOCIATION CHART** -- These are charts that provide a brief biographical sketch on each of the people or entities involved, its hierarchy, its strong and weak points, the strength of relationships in the group, and possible members who could be used as agents in the group.

**BANK RECORD ANALYSIS** -- These are charts showing a chronology of bank deposits, withdrawals, checks written, balances, and other financial information on a monthly, quarterly, or yearly basis.

**BAR CHARTS** -- These are graphic depictions of some activity along another factor like time, money, etc., and are generally reserved for things that can be quantified.

**BRIEFINGS** -- These are notes used by an oral presenter containing the fact pattern, answers to a series of questions that might arise (FAQ), an overview of the assessment, and any charts, tables, or other graphics that support summary statements concerning conclusions or hypotheses.

**BULLETINS** -- These are short warning reports, similar to wanted posters or Be on the Lookout announcements.

**CASE ANALYSIS** -- These are essentially references to files and other sources of information on a case along with a summary of the final products and maybe a sample table, chart, or other figure used to support conclusions and recommendations.

**CHARTS** -- These present an analytical overview of data, showing an activity or relationship in the simplest manner. They often contain a legend.

**CHRONOLOGICAL TABLE** -- also known as a timeline, these depict the specific time frames of activities.

**COLLECTION PLAN** -- These are group- or activity-specific lists of things to be done to prove or disprove hypotheses. Unknown persons or locations that need to be investigated are pointed out. The focus is usually on geographic territory.

**COMMODITY FLOW CHARTS** -- These are depictions of the flow of goods or currency among persons or entities to determine the meaning of an activity.

**COMPOSITE TABLE** -- These are collections of incident data or person data to determine the most common factors within the incidents.

**CONCLUSIONS** -- These are hypotheses, trends, forecasts, or predictions.

**CONTENT ANALYSIS** -- These are reports on the most commonly reoccurring words in communication or on documents.

**DEMOGRAPHIC ANALYSIS** -- These are tables containing factors such as age, race, gender, level of education, economic resources, security interests, and income of a place or group.

**DESCRIPTIVE ANALYSIS** -- These are evaluations of an event, activity, group, or person. They are found in all kinds of reports.

**EVENT FLOW ANALYSIS** -- These are charts providing a visual depiction of a series of important occurrences. A summation of each event is put in a box which is connected by arrows to other boxes summarizing other events.

**FACT PATTERN** -- These are paragraphs, much like legal briefs, that summarize the salient information that a policymaker needs to make a decision as to whether or not something happened.

**FORECAST** -- These are narrative paragraphs which indicate the bases used for making the forecast, several predictions based on different bases, and the reasoning behind the choice about the most certain prediction.

**FREQUENCY DISTRIBUTION** -- These are tables of numbers indicating the number of times something occurs, with percentage weights often added to represent the heaviest amount of specific activities.

**GEOGRAPHIC DISTRIBUTION ANALYSIS** -- These are maps showing the location of certain areas and distribution routes to and between the areas.

**INDICATOR ANALYSIS** -- These are profile checklists which mark whether or not someone or something manifests a set of important indicators which would predict a present or future activity.

**INFERENCE DEVELOPMENT** -- These are narrative statements which draw conclusions based on deductive or inductive reasoning. All analytical products contain inferences, but in some reports, the logic is spelled out.

**MAPS** -- These are often included in a report to show important geographic or locational information relating to territory or turf covered by an activity.

**MARKET ANALYSIS** -- These are narrative statements, gleaned from information about demographics, that indicate the existence or nonexistence of a market for some good, service, or activity.

**MATRIX** -- These are triangular or rectangular charts that allow the viewer to read across a row and down a column to see connections or relationships between individuals, entities, or organizations. They mostly contain numerical information.

**NET WORTH ANALYSIS** -- These are tables showing the financial affairs of an individual or entity, listing assets, liabilities, and expenses.

**PIE CHART** -- These are circular charts where the pieces of the pie have some meaningful representation and add up to 100%.

**PREMONITORY** -- These are notes, similar to briefings, in which the feasibility or viability of short-range action is contemplated. They usually have four parts: a description of activities someone or something is engaged in; what their strengths and weaknesses are; what recommendations can be made; and what the probability of success for some action might be.

**PROBABILITY ANALYSIS** -- These are sentences expressing confidence in something occurring. Anything over 80% is most likely to occur; from 60-80% somewhat likely to occur; from 40-60% an even chance of occurring; from 20-40% somewhat unlikely; and below 20% very unlikely.

**PROFILE** -- These are paragraphs in which indicators of behavior or activity are used to create models that can be used to identify the characteristics of persons or entities that may or may not be involved in some activity.

**RECOMMENDATIONS** -- These are statements about the precise time and place of some activity that would be of concern to policymakers along with some suggested action that could be taken beforehand to deter or alter the course of events.

**SOURCE & APPLICATION OF FUNDS** -- These are tables, similar to net worth analysis, showing what a person or entity has legally available to them, and what they are spending on, to determine any discrepancy.

**STATISTICAL ANALYSIS** -- These are tables of numbers showing whether or not any relationship between the numbers are statistically significant.

**STRATEGIC ANALYSIS** -- These are notes, similar to premonitories, in which the feasibility or viability of long-range action is contemplated. They include a collection plan for gathering intelligence, description of the activities someone or something might engage in, preliminary

recommendations that can be made, and an assessment plan for evaluating any recommended action.

**SUMMARY** -- These are sentences summarizing the whole analytical product. They are often part of all reports.

**SURVEY** -- These are lists of questions that need to be answered in order to provide more information for analysis.

**TABLES** -- These present a comparative overview of data, showing an activity or relationship compared to other variables. They often contain a legend.

**TELEPHONE RECORD ANALYSIS** -- These are lists on the date span of calls, hours & patterns of use, and numbers called from telephone or other communications intercepts.

**THREAT ASSESSMENT** -- These are narrative statements about the propensity of a group or entity to engage in some activity, usually a violent activity. They usually describe the data on which the possibility of the threat is based, the projected time frame of the threat, the possible targets of the threat, a vulnerability assessment for the targets, and recommendations for countermeasures.

**TIME SERIES ANALYSIS** -- These are computerized statistical printouts showing lagged or nonlagged correlations between events or relationships.

**TREND ANALYSIS** -- These are non-computerized extrapolations of a direction or tendency based upon the numbers or rates from prior time periods.

**VISUAL INVESTIGATIVE ANALYSIS** -- These are charts showing boxes in which the future necessary steps that need to be taken by somebody or something are outlined in order to complete their plans or objectives.

**VULNERABILITY ASSESSMENT** -- These are narrative statements about the softness or weakness of a target to some possible activity or action.

**WARNINGS** -- These are forecasts or predictive statements about a potential future occurrence which may threaten a group or individual. They are typically part of threat and vulnerability assessments.

## **INTERNET RESOURCES**

[A Compendium of Analysis Notes and Bibliography](#)

[Air War College Gateway to Intelligence](#)

[BBC Article on Intelligence Failure](#)

[The Sherman Kent Center](#)

[AFIO \(Association of Former Intelligence Officers\)](#)

[CIA Kid's Page](#)

[DIA-JMIC](#)

[Dr. Rob Johnson's Taxonomy of Intelligence Analysis Variables](#)

[Interpol](#)

[Mercyhurst College Institute for Intelligence Studies](#)

[Richard Heuer's book Psychology of Intelligence Analysis](#)

[Stratfor - a commercial intelligence analysis agency](#)  
[The NID and Intelligence Analysis Process \(pdf\)](#)

#### PRINTED REFERENCES

- Alexseev, M. (1997). *Without Warning: Threat Assessment and Intelligence*. NY: St. Martin's.
- Allison, Graham. (1971). *Essence of Decision: Explaining the Cuban Missile Crisis*. NY: Little, Brown.
- Ben-Zvi, Abraham. (1979). "The Study of Surprise Attacks" *Brit. J. of International Studies*, Vol. 5.
- Betts, Richard. (1978). "Why Intelligence Failures are Inevitable" *World Politics*, Vol 31, No. 1.
- Betts, R. (1982). *Surprise Attack: Lessons for Defense Planning*. Washington DC: Brookings Institute.
- Carl, Leo. (1990). *International Dictionary of Intelligence*. NY: Maven Books.
- Carr, E. H. (1961). *What is History?* NY: Macmillan.
- Chan, S. (1979). "The Intelligence of Stupidity: Understanding Failures" *Am. Pol. Sci. Rev.* 73:633-50.
- Clark, R. (2003). *Intelligence Analysis: A Target-Centric Approach*. Washington D.C.: CQ Press.
- Clauser, J. & S. Weir. (1976). *Intelligence Research Methodology*. US Defense Intelligence School.
- Davis, Jack (1992). "The Kent-Kendall Debate of 1949." *Studies in Intelligence* Vol. 36 No. 5 (1992), 91-103.
- Davis, Jack. (1997). *A Compendium of Analytic Tradecraft Notes*. Directorate of Intelligence: CIA Center for the Study of Intelligence.
- Dulles, Allen. (1965). *The Craft of Intelligence*. NY: Signet Books.
- Ford, Harold. (1993). *Estimative Intelligence*. Lanham, MD: Rowman & Littlefield.
- Garst, R. & Gross, M. (2005). "On Becoming an Intelligence Analyst." Pp. 39-45 in D. Cliff, *Learning with Professionals: Selected Works from the JMIC*. Washington DC: JMIC.
- Grabo, Cynthia. (2002). *Analysis for Strategic Warning*. Washington DC: DIA-Joint Military Intelligence College.
- Heuer, R. (1978). *Quantitative Approaches to Political Intelligence*. Boulder, CO: Westview.
- Heuer, Richard. (1999). *Psychology of Intelligence Analysis*. Langley, CA: CIA Center for Study of Intelligence.
- Hummel, Wm. & K. Huntress. (1956). *The Analysis of Propaganda*. NY: Dryden Press.
- Jervis, Robert. (1977). *Perception and Misperception in International Politics*. Princeton NJ: Princeton U. Press
- Johnson, Edgar. (1974). Effects of Data Source Reliability on Inference. Technical Paper #251 US Army Research Institute for the Behavioral and Social Sciences.
- Johnson, Rob. (2005). *Analytic Culture in the US Intelligence Community*. Washington DC: Center for the Study of Intelligence.
- Kahn, David. (1995). "Toward a Theory of Intelligence" *Military History Quarterly* 7(2): 92-97.
- Keller, B. (1992). *Avoiding Surprise at War*. Ft. Leavenworth: Army Command & Gen. Staff College.
- Kendall, Willmore. (1949). "The Function of Intelligence" review of *Strategic Intelligence for American World Policy*, by Sherman Kent, in *World Politics*, Vol. 1, No. 4 (July 1949): 91-103.
- Laqueur, Walter. (1985). *A World of Secrets: The Uses and Limits of Intelligence*. NY: Basic.
- Laqueur, W. (1985). *A World of Secrets: The Uses and Limits of Intelligence*. NY: Basic.
- Lowenthal, M. (2006). *Intelligence: From Secrets to Policy*, 3e. Washington DC: CQ Press.
- May, Ernest. (1973). *Lessons of the Past: Uses & Misuses of History in Foreign Policy*. NY: Oxford U. Press
- Miller, George. (1956). "The Magical Number Seven—Plus or Minus Two: Some Limits on our Capacity for Processing Information" *Psychological Review* Vol. 63, No. 2

- Nisbett, Richard & Lee Ross. (1980). *Human Inference*. NJ: Prentice Hall.
- O'Toole, George. (1990). "Kahn's Law: A Universal Principle of Intelligence" *International Journal of Intelligence and Counterintelligence* 4(1):39-46.
- Peterson, M. (1994). *Applications in Criminal Analysis*. Westport, CT: Praeger.
- Shulsky, Abram. (1999). (2<sup>nd</sup> ed) *Silent Warfare: Understanding the World of Intelligence*. Dulles, VA: Brassey's.
- Schum, D. (1987). *Evidence & Inference for the Intelligence Analyst*. NY: Univ. Press of America.
- Skinner, B. F. (1948). "Superstition in the Pigeon" *Journal of Experimental Psychology* 38: 168-72.
- Slovic, Paul & Sarah Lichtenstein. (1971). "Comparison of Bayesian and Regression Approaches to the Study of Information Processing in Judgment" *Organizational Behavior & Human Performance* 6.
- Treverton, G. (2001). *Reshaping National Intelligence in an Age of Information*. NY: Cambridge Univ. Press.
- Troy, T. (1991). "The Correct Definition of Intelligence" *International Journal of Intelligence and Counterintelligence* 5(4):433-54.
- U.S. Central Intelligence Agency. (1994). *Consumer's Guide to Intelligence*. Washington, DC: CIA Center for Study of Intelligence.
- Westerfield, H. Bradford. (1995). *Inside CIA's Private World*. New Haven: Yale Univ. Press.