1981-06

Strategic Deception and Counterdeception, a Cognitive Process Approach

Heuer, Richards J. Jr.

Wiley

Strategic Deception and Counterdeception

A Cognitive Process Approach

RICHARDS J. HEUER, Jr.
Naval Postgraduate School

Research in experimental psychology is applied to an analysis of problems of strategic military deception and counterdeception. In conducting deception, the deceiver has a clear advantage; empirical evidence confirms assumptions drawn from cognitive psychology that deception seldom fails when it exploits a target's preconceptions. The target's tendency to assimilate discrepant information to existing mental sets generally negates the risks to deception posed by security leaks and uncontrolled channels of information. Cognitive biases in the assessment of probabilities, evaluation of evidence, and attribution of causality are described and related to questions of deception and counterdeception. Approaches to enhancing an organization's ability to detect deception are examined. Improved intelligence collection and heightened alertness to deception are often insufficient. Cognitive aids to facilitate analysis are recommended, as is the formation of a counterdeception staff as a focal point for deception analysis.

Strategic deception aims to manipulate elite perceptions in order to gain competitive advantage. It is usually achieved by passage of information to national or military decision makers either directly or via a nation's intelligence services. Channels for passing such information include public or private statements by government officials, leaks to journalists, double agents, and spoofing of technical intelligence collection sensors.

AUTHOR'S NOTE: The research on which this article was based was funded by the Interdisciplinary Research Project on Deception, Naval Postgraduate School, Monterey, Calif. The views are those of the author and should not be interpreted as representing the official policies, express or implied, of the U.S. Government. Material from this article will also be published in Donald C. Daniel and Katherine L. Herbig, editors, *Strategic Military Deception: Perspectives on Its Study and Use,* Pergamon Press, forthcoming.

INTERNATIONAL STUDIES QUARTERLY, Vol. 25 No. 2, June 1981 294-327

The chances for successful deception are increased by knowledge about the cognitive processes of the target decision makers or intelligence analysts. Similarly, the chances of detecting deception are enhanced by designing a counterdeception program that takes into account known limitations in one's information processing capabilities. This study examines cognitive processes relating to strategic deception and counterdeception. One has the choice of determining the cognitive propensities and predilections of individual decision makers and analytical organizations, or of examining those factors that most people seem to have in common. The study takes the latter approach. It concludes by considering means of improving an organization's ability to detect deception. Several cognitive aids to analysis are recommended, and circumstances are defined in which it may be advisable to form a counterdeception staff to focus on this problem.

Over 20 years ago, Herbert Simon (1957) advanced the concept of "bounded" or limited rationality. Because of limits in our mental capacity, he argued, the human mind cannot cope directly with the complexity of the world. Rather, we construct in our mind a simplified model of reality and then work with this mental model. We behave rationally within the confines of our mental model, but this model is generally not well adapted to the requirements of the real world.

Much psychological research on perception, memory, attention span, and reasoning capacity documents the limitations in our "mental machinery" referred to by Simon. This work has been applied to the study of international political behavior by De Rivera (1968), George and Smoke (1974), Jervis (1976), and many others. A psychological perspective underlies the writings on intelligence and strategic surprise by Wasserman (1960), De Weerd (1962), Knorr (1964), Shlaim (1976), and Handel (1976). In this article, we apply recent research findings more specifically to the problems of conducting and detecting strategic deception.

Recent psychological research stimulated by the seminal work of Tversky and Kahneman (1974) and Jones and Nisbett (1971),

and recently summarized by Nisbett and Ross (1980) and Hogarth (1980), identifies various cognitive heuristics and biases that influence human information processing. This research appears to be broadly applicable to all forms of judgment under uncertainty, including foreign policy analysis, although many IR scholars seem unfamiliar with it. Several researchers have recently started to apply this body of literature to problems of intelligence analysis (Chan, 1979; Stech, 1980; Heuer, 1978, 1979, 1980a). Selected aspects of this literature are related to the problems of deception and counterdeception.

Evidence cited in this study is drawn largely from experimental psychology. There are always potential problems in generalizing from such laboratory findings to real world applications. In some instances, historical examples are cited to illustrate the plausible application of the laboratory evidence to problems of intelligence analysis. The number of historical examples is limited, however, both by space constraints and by the difficulty of demonstrating that any specific historical instance of misjudgment was caused principally by the cited cognitive tendencies.[1]

Perception and Deception

Circumstances under which human perception is most commonly distorted have significant implications for understanding the nature and limitations of intelligence analysis. They correspond with the circumstances under which intelligence analysis is generally conducted. Intelligence analysts deal with highly ambiguous situations on the basis of information that is processed incrementally under pressure for early judgment. This is a recipe for inaccurate perception that has clear implications for assessing

1. To check my own judgment concerning the face validity and applicability of the laboratory findings in an intelligence context, I have discussed these findings in training courses for experienced intelligence analysts. These discussions reveal broad consensus that the laboratory experiments referred to in this article document processes that do, in fact, influence the outcome of intelligence analysis. I have also successfully replicated several experiments with groups of intelligence analysts; these were small, informal, classroom demonstrations that are not reported here.

both the opportunities available to those planning deception and the difficulties faced by those seeking to detect such strategems.

Intelligence analysis tries to illuminate the unknown. Almost by definition, it is concerned with hazy, uncertain, ambiguous situations. Yet we know that the greater the ambiguity of the stimuli, the greater the impact of expectations and pre-existing images on the perception of those stimuli. Thus, despite maximum striving for objectivity, the intelligence analyst's own preconceptions are likely to exert a greater impact on the analytical product than in other fields where the analyst is working with less ambiguous and less discordant information.

Moreover, the intelligence analyst is among the first to view new problems at an early stage when the evidence is fuzzy and even the problem itself may be ill-defined. The analyst then follows a problem as additional increments of evidence are received and the picture gradually clarifies. Yet we know (Bruner and Potter, 1964) that initial exposure to blurred stimuli interferes with accurate perception even after more and better information becomes available.

Perceptions are quick to form but then resist change. Once we have formed an impression about an object, event, or situation, we are biased toward continuing to perceive it in the same way. This suggests that because the intelligence analyst starts observing a potential problem situation at its early and most unclear stage, he or she is at a disadvantage when compared with others (for example, policy makers) whose first exposure may come at a later stage, with more and better information.

The receipt of information in small increments over time also facilitates assimilation of this information into the analyst's existing views. No one item of information may be sufficient to prompt a change of view. The cumulative message inherent in many pieces of information is not examined as a whole. This problem of incremental analysis was noted in the U.S. intelligence community's still-classified postmortem analysis of community performance prior to the 1973 Arab-Israeli War.[2] Analysts,

2. The U.S. intelligence community consists of the Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, Federal Bureau of Investigation,

according to their own accounts, had been proceeding on the basis of each day's report, hastily comparing it with material received the previous day. They produced, in an "assembly line fashion," reports that may have reflected perceptive intuition but were not based on systematic consideration of an accumulated body of integrated evidence.

As time passes and more information is received, a fresh look at all the evidence might suggest a different explanation. Yet there is rarely time or interest for this, and the early judgment adversely affects the formation of future perceptions in any event. Once an analyst thinks he or she knows what is happening, a change of view is unlikely. The new information received incrementally fits easily into the analyst's existing image. This perceptual bias is reinforced by organizational pressures favoring consistent interpretation, for once the analyst is committed in writing, both the analyst and the organization have a vested interest in maintaining the original diagnosis.

Finally, the intelligence analyst operates in an environment that exerts strong pressures for premature judgment. Decision makers' needs for interpretive analysis are greatest within, at most, two or three days after an event occurs. The system often requires the analyst to make an almost instant diagnosis before sufficient hard information makes a well-grounded judgment possible. This diagnosis can only be based upon the analyst's preconceptions concerning how and why events normally transpire in a given society.

With respect to deception, one overwhelming conclusion stands out: It is far easier to lead a target astray by reinforcing the target's existing beliefs, thus causing the target to ignore the contrary evidence of one's true intent, than to persuade a target to change his or her mind.

Military operations, in particular, possess a certain logic. Terrain, weather, supplies, and the relative balance of forces often suggest optimal tactics or strategy. If the preferred alternative is equally obvious to the opponent, however, its advantages will be

---

and intelligence components of the Departments of State, Treasury and Energy and of the U.S. Army, Navy, and Air Force.

offset by the other side's counterpreparations. Thus, planners of military operations often use deception to conceal their true intent, and in so doing are faced with two basic alternatives. They can plan to attack in a place, time, and manner most expected by the opponent, while seeking, through deception, to achieve surprise by changing the opponent's expectations. Or they can reinforce the other side's expectations while planning a surprise attack in a different place, time, or manner.

People's tendencies to perceive the expected, and to assimilate new information to existing images, make it far easier to reinforce a target's existing beliefs than to change them. Deceptions that follow this principle seldom fail, for the odds are then strongly in favor of the deceiver. The human capacity to rationalize contradictory evidence is easily sufficient to outweigh the pernicious effects of security leaks and uncontrolled channels of information that planners of deception might otherwise fear might compromise their efforts. Perhaps the most extreme of many possible examples is the case described by Masterman (1972), in which British intelligence tried to discredit one of the German agents they had "turned" in order to enhance the credibility of other German agents they had also brought under control. The British effort was unsuccessful; no matter how blatant the actions the agent took under British direction, the Germans refused to believe he was no longer loyal.

Deceptions that require persuading a target of something different from what he or she already is inclined to believe are difficult because of the target's tendency to integrate any new information into those already existing beliefs. This kind of deception is sometimes required by the nature of the operational situation, however, in which case the chances for success can be influenced by the sequence in which information is fed to the target. The deception should be initiated with strong and obvious evidence that forces the desired conclusion to be at least seriously considered by the target intelligence analysts and decision makers. This should then be followed in quick succession by additional supporting evidence that leads the target to a reasoned conclusion in favor of the desired alternative.

The opposite tactic, which seems incorrect from a psychological point of view, would be to save the more dramatic evidence until after the stage has been set by transmitting a number of supporting messages. The expectation is that the target initially attributes little importance to the supporting messages, but once the key is received the other pieces will fall into place forming a coherent and persuasive picture. The weakness of this tactic is that the target may have failed to notice, forgotten or misinterpreted the earlier evidence, for information that does not fit neatly into an existing hypothesis tends to be ignored or misperceived. Intelligence analysts and decision makers are commonly confronted with a large amount of discordant information. They have only a limited capacity to sort and store this information in their memory in a manner that makes it possible to recall it for the evaluation of hypotheses currently under consideration.

The target of a deception is likely to have a different agenda of concerns, different predispositions, and a different information base than the planners of deception. Normally this will lead to a different interpretation of messages. If the deception planners have sufficient understanding of the target's situation and thinking, messages may be planned to take advantage of the particular context in which they will be received; but in practice the target may miss many clues the deceiver provides, and may assign considerable weight to factors the deceiver regards as trivial or to information of which the deceiver is unaware. To the extent that the deception signals reinforce the target's expectations, there is a large margin for error and these miscalculations have little impact. If the goal is to change the target's mind, however, they may be critical.

Planning and implementing a deception typically involves a major investment of time, energy, and ego. When people make such an investment in preparing a message, they tend to overestimate how clear this message will be to the receiver. This results from the importance of context in perceiving and interpreting a signal; when a message is placed in a different context, it assumes a different meaning. The message developed by the

deception planners is understood by them in the context of the endless meetings in which alternatives were weighed and details worked out. They are so familiar with their own thinking that they risk overlooking the degree to which the message is clear to them only because they know what to look for.

Cognitive Biases and Deception

The term bias, as used here, refers to any form of mental error that is not random, but is consistently and predictably in the same direction. Cognitive biases are those that result from regularities in the way the human mind processes information, independent of any intellectual or emotional predisposition toward a certain judgment. They may be distinguished from biases induced by self-interest, organizational role, ideology, or cultural norms. They are, therefore, one of the most pervasive forms of bias. Much of the research on this topic is relatively recent in origin. In this section, we discuss biases that affect the estimation of probabilities, the evaluation of evidence, and the attribution of causality; and we relate these biases to problems of deception and counterdeception.

BIASES IN ESTIMATING PROBABILITIES

Estimating probabilities is important because we live in a probabilistic world. Social, political, military, and economic developments are not rigidly determined but occur or fail to occur with some degree of probability. The intelligence analyst is constantly assessing probabilities with respect to the intentions of foreign leaders, the capability of military forces, the future consequences of current events, and the credibility of sources.

Typically, these probability judgments are expressed in imprecise terms such as possibly, probably, or very likely—terms that unfortunately have different meanings to different people (Decisions and Designs, 1977: 68). Yet the issue here is not whether communication of intelligence judgments can or should

be improved by replacing these verbal qualifiers with numerical ranges of probability. It is whether the estimates themselves are influenced by systematic biases that affect their accuracy. Experimental research findings suggest that this is in fact the case.

Availability Bias

One of the simplified rules of thumb people use in making probability estimates is the availability rule. In this sense availability refers to imaginability or retrievability. Two of the cues used to judge the probability of an event are (1) the ease with which we can imagine relevant instances of the event, and (2) the number or frequency of such events we can easily remember (Tversky and Kahneman, 1973).

Normally, this availability works quite well. If one thing actually occurs more frequently and therefore is more probable than another, we probably *will* be able to recall more instances of it. Events that *are* likely to occur generally *are* easier to imagine than unlikely events. We are constantly making inferences based on these assumptions. We estimate the probability of successful deception by recalling historical examples of deception under similar circumstances. We estimate the probability that a politician will lose an election by imagining ways in which he may lose popular support. However, we are often led astray because the ease of recollection is influenced by many factors, such as emotional saliency, vividness, and how recently we have been exposed to these events, all of which may be unrelated to the correct probability. For example, Soviet assessment of the likelihood that Germany may once again become a military threat to Soviet interests seems clearly biased by the ready availability of vivid memories of World War II.

United States estimates of the likelihood of Sino-Soviet reconciliation may also be influenced by availability bias. This is because it is so easy to imagine such a development and what impact it would have on U.S. policy. In fact, our memory of having been taken by surprise by the Sino-Soviet split causes many people to be *preoccupied* by the possibility of reconciliation.

Analysts working full time on this question are presumably considering the operative causal factors, not making quick and easy inferences on the basis of imaginability. But the policymaker or generalist who lacks time or information to go into details must unconsciously take shortcuts, and the obvious shortcut is to use the availability rule of thumb for making inferences about probability.

Anchoring Bias

Another strategy that people seem to use intuitively and unconsciously to simplify the task of mentally processing complex information is called anchoring. Some natural starting point is used as a first approximation to the desired judgment. This starting point is then adjusted, based on the results of additional information or analysis. Typically, however, the starting point serves as an anchor or drag that reduces the amount of adjustment, so that the final estimate remains closer to the starting point than it ought to be (Tversky and Kahneman, 1972).

Decision makers and intelligence analysts deal with dynamic situations. They must continually review their estimates in response to changes in the situation or the receipt of previously unavailable information. Ideally, a direct correlation should exist between changes in the situation and/or new information and changes in the estimate, but such is frequently not the case. Much evidence suggests that people do not change their judgments enough (Edwards, 1968). Once an estimate is made, thinking becomes anchored and moves only within a narrow range around that spot.

Implications for Deception

Availability bias may make a person believe that strategic deception is more common that it really is, and thus cause one to be more disposed to perceive it. Successful cases of deception may be far more salient, and consequently more available for recall in memory, than cases in which deception was not employed under

comparable circumstances. Deception attracts both the popular imagination and the attention of historians, while the absence of deception in strategic operations does not. When faced with a situation in which deception may or may not be employed, one's estimate of the probability of deception may be influenced by this easy retrievability of past instances of it. An analyst's appreciation of the frequency of deception may, of course, be offset by the feeling that "it can't happen to me."

The availability bias also suggests that employees of watch offices will tend to overestimate the probability of whatever it is they are watching for. Having been briefed and trained to recognize certain indicators, and having imagined and rehearsed scenarios that include the watched-for developments, it is not surprising that these developments are at the forefront of their minds as they try to forecast the future course of events.

If the goal of deception is to induce ambiguity or to persuade the watch officers that what they are watching for is *not* happening (for instance, that there is no intent to attack when an attack is in fact being prepared), a watch office is an extremely difficult deception target. On the other hand, it may be possible to exploit the watch officers' preconceptions, for example, as part of a plan to rely on the "cry wolf" syndrome. The watch office might be provoked to issue an alert of impending attack several times when no attack is in fact planned, so that future alerts will be received more skeptically. In this procedure, the availability of the attack scenario is countered by building up in the watch officers another availability, the memory of recent false alarms.

The significance of the anchoring bias to the deception planner depends upon the type of deception being planned. If the goal is to reinforce a target's preconceptions, anchoring will facilitate this objective. The prognosis for overcoming anchoring is not favorable. In one experiment, the bias persisted even after test subjects had been given feedback to show the bias and after they had been urged to try to overcome this tendency in answering a new set of estimation questions (Alpert and Raiffa, 1968). This is a common finding in experiments dealing with cognitive biases; the biases persist even after test subjects are informed of them and instructed to try to avoid them or compensate for them.

One possible technique for avoiding the anchoring bias is to ignore one's own or others' earlier judgments and rethink a problem from scratch. In other words, an analyst should consciously avoid using any prior judgment as a starting point. There is no experimental evidence to show that this is possible or that it will work, but it seems worth trying. Alternatively, it is sometimes possible to avoid human error by employing formal statistical procedures. Bayesian statistical analysis, for example, can be used in intelligence analysis to revise prior judgments on the basis of new information in a way that is designed to avoid anchoring bias (Schweitzer, 1978; Andriole, 1980; Heuer, 1980b).

BIASES IN EVALUATION OF EVIDENCE

The most salient characteristic of the information environment in which an intelligence analyst works is its diversity. Multiple sources, with varying degrees of reliability, commonly report information which by itself is incomplete and often inconsistent or even incompatible with reports from other sources. Conflicting evidence of uncertain reliability is endemic to intelligence analysis. Because of the nature of this analytical environment, the intelligence analyst may be more vulnerable to some biases in the evaluation of evidence than analysts in many other domains.

Oversensitivity to Consistency

Consistency is, in many circumstances, an appropriate standard for evaluating evidence. When we evaluate alternative explanations or estimates, we select the one which encompasses the greatest amount of evidence within a logically consistent scenario. A hypothesis may be invalidated by a single inconsistent datum.

The proper preference for consistency carries over to other circumstances when it is inappropriate, however. This occurs when one is working with a small sample of evidence reflecting a high level of consistency that may not be found in a much larger

sample. One is likely to see two or three heads in a row when flipping a coin, for example, but this consistency is misleading as to what one might expect from a larger number of flips of a fair coin.

The same type of problem arises in intelligence analysis when there is little information available, as on political attitudes of Soviet military officers or among certain African tribes. If the available evidence is consistent, one tends to overlook the fact that it represents a very small and hence unreliable sample taken from a large and heterogeneous group. As a general rule, people are quite willing to make confident judgments on the basis of extremely small samples. They have more confidence in judgments based on a small amount of consistent evidence than on a larger body of evidence that contains some inconsistencies (Kahneman and Tversky, 1979).

Coping with Evidence That Is Less Than Perfectly Reliable

Evidence is usually less than perfectly reliable, especially evidence from human as opposed to documentary or photographic sources. If there is, for example, an 80% probability that a given item of information is accurate, a degree of uncertainty should accompany that information as it is used in reasoning and inference. The human mind has difficulty coping with complicated probabilistic relationships, however, so we tend to employ simple rules of thumb that reduce the burden of processing such information.

In dealing with evidence that is less than perfectly reliable we do focus on source reliability, but then tend to make a simple yes/no decision. If the evidence is rejected as unreliable, it is rejected so fully that it plays no further role in our mental calculations. If it is accepted, we tend, in subsequent mental calculations, to process it as though it were wholly reliable, ignoring the probabilistic nature of the reliability judgment. This is a "best guess" strategy (Schum and DuCharme, 1971; Gettys et al., 1973). Other more sophisticated strategies may be used

(Johnson, 1974), but they, too, involve ignoring some of the uncertainty. If an intelligence analysts treats information that is 80% reliable as though it were 100% certain, judgments based on that information will be overconfident.

Absence of Evidence

The intelligence analyst is often required to address issues for which few data are available. Ideally, analysts should recognize what relevant evidence is lacking and should consider this in their reasoning. The potential impact of the missing data should be estimated and confidence in their judgment adjusted downward in recognition that key information is unavailable. Unfortunately, this ideal may not be the norm.

In an experiment designed to test how sensitive even experts in their field are to information that is omitted from presentation of a problem, two groups were given information in the form of a "fault tree," which is a schematic drawing showing all the things that might go wrong with any endeavor. Fault trees are used to study the fallibility of complex systems such as a nuclear reactor or space capsule. One group was given the full tree, the other an incomplete version in order to test how sensitive the subjects were to what was left out. The information that was missing should have been easily recognized, but it was not, and judgments suffered as a result. "Out of sight, out of mind" was an apt description of the performance of the test subjects (Fischhoff et al., 1978). Intelligence analysts may have similar problems in recognizing gaps in their data and adjusting their judgments accordingly.

Persistence of Impressions Based on Discredited Evidence

Impressions tend to persist even after the evidence that created those impressions is fully discredited. Psychologists have become interested in this phenomenon because many of their experiments require that the test subjects be deceived; for example, they are

made to believe that they were successful or unsuccessful in performing some task or that they possess certain abilities or personality traits when this is not true. Professional ethics require that test subjects be disabused of these false impressions at the end of the experiment, but this has proven surprisingly difficult to achieve (Lau et al., 1976).

Test subjects asked to distinguish true from fictitious suicide notes were given feedback that had no relationship to actual performance. The test subjects had been divided randomly into two groups, with members of one group given the impression of above average success and the other of relative failure at this task. The subjects' erroneous impressions of the difficulty of the task and of their own performance persisted even after they were informed of the deception, that is, informed that their alleged performance had been preordained by their assignment to one or the other test group. Moreover, the same phenomenon was found among observers of the experiment as well as the immediate participants (Ross et al., 1975). The impressions persisted even after the evidence on which they were based was fully discredited.

Several cognitive processes might account for this phenomenon. An interesting but somewhat speculative explanation draws on the strong human tendency to seek causal explanations. When evidence is received, we postulate a set of causal connections that explain this evidence. Even though the evidence may subsequently be discredited, the causal linkages remain plausible and may seem sufficient to imply the existence of an event even in the absence of the now-discredited evidence. The previously perceived causal linkage comes easily to mind. It is a readily "available" explanation that makes the event seem more likely than it would have appeared prior to receipt of the discredited evidence.

Implications for Deception

The bias favoring a small amount of consistent information over a larger body of less consistent data supports the common maxim in deception operations that the deceiver should control

as many information channels as possible in order to reduce the amount of discrepant information available to the target. Deception can be effective even with a small amount of information as long as the target does not receive credible contradictory data. Difficulties in processing evidence that is not completely reliable are relevant because they can be a source of overconfidence in one's judgment.

To deception planners, problems of dealing with missing evidence suggest that deception is unlikely to fail because of information that is *not* provided. The absence of evidence is often overlooked, so errors of omission will be less serious than errors of commission. Conversely, the analyst attempting to detect deception would be well advised to consider carefully what information is missing. If the enemy were planning X, what would be the observable consequences of this plan, what is the likelihood that this evidence could in fact be observed, and what inferences should be drawn from the fact that certain evidence is not observed?

The above conclusions are certainly not surprising. The persistence of impressions based on discredited evidence, however, does have counterintuitive implications. The impressions created by information fed through a double agent may persist even after the opposition learns that its agent has come under control of another party, and that information from this source cannot be trusted. If we give credence to information and it affects our thinking, and we subsequently learn that this information was deliberately leaked by an enemy, this subsequent knowledge does not necessarily reduce the impact of the initial report. Once information "rings" a bell, so to speak, the bell cannot be "unrung."

The ambiguity of most real world situations contributes to the operation of this tendency for images to persevere in spite of contradictory evidence. Rarely in the real world is evidence so thoroughly discredited as is possible in the experimental laboratory. Let us assume that an intelligence officer receives a report that one of his or her agents has come under hostile control. Assume further that the officer has formed a number of impressions based on reporting from this agent. It is easy for the

officer to rationalize the perseverance of these impressions by arguing that the information was true despite the agent being under hostile control, or by doubting the validity of the report claiming the agent's duplicity. In the latter case, the phenomenon of impression perseverance may itself affect evaluation of the evidence that supposedly discredits the impression; it is because one retains the initial impression that one disbelieves the new evidence.

It is a truism that security is an essential element of successful deception. If the deception is undertaken to protect the security of an operational plan, compromise of the deception might be worse than no deception at all, for it could attract attention to the true plan. While security is obviously desirable, it may not be quite as essential as past deception planners have believed, for impression perseverance helps reduce the adverse consequences of security leaks.

BIASES IN ATTRIBUTION OF CAUSALITY

We cannot see causation in the same sense that we see a desk or a tree. Even when we observe one billiard ball strike another and then observe the previously stationary ball begin to move, we are not seeing causation. The most we can see is the juxtaposition of events in time and space. The perception of causation results only from a complex process of inference, not from direct observation. As other forms of inference, it is subject to systematic biases.

Bias Toward Causal Explanations

People have a deep psychological need to understand their environment. Understanding implies order, so we arrange our observations into regular patterns. Intelligence analysts generally look for and find causal relationships. Others, exposed to inexplicable events, may attribute them to God's will or to fate, which is somehow preordained. People resist the thought that outcomes may be determined by forces that interact in random,

unpredictable ways. People generally do not accept the notion of chance or randomness. Even dice players behave as though they exert some control over the outcome of a throw of dice (Langer, 1977).

In foreign and military affairs, where the patterns are at best very difficult to fathom, there may be events for which there are no valid causal explanations. The need to impose some orderly pattern on their environment causes people to overestimate the extent to which other countries or other people are pursuing a coherent, rational, goal-maximizing policy. We tend to see the actions of other governments as the intentional result of central direction and planning, and to overlook the fact that the same behavior might be more accurately explained by accident, blunder, the unintended consequence of well-intentioned policy, improperly executed orders, bargaining among semi-independent bureaucratic entities, or following standard operating procedures under inappropriate circumstances (Jervis, 1976: 320).

Internal vs. External Causes of Behavior

Attribution theory is the subfield of psychology dealing with how people assess the causes of behavior. Most research in attribution theory employs a basic dichotomy between internal and external causes of behavior. Internal causes include a person's attitudes, beliefs, and personality. External causes include such factors as incentives and constraints, role requirements, or difficulty of a task. Attribution theory examines the circumstances under which we attribute behavior to either internal or external causes.

The fundamental attributional error is to overestimate the importance of personal traits and dispositions in determining behavior. When we observe another's behavior, we are too quick to infer broad personal qualities or dispositions from this behavior and to expect that these same dispositions will determine the actor's behavior in other contexts (Ross, 1977). Much research into personality traits demonstrates that personal traits

are not consistent determinants of behavior; which trait predominates at any given time is heavily dependent upon the situational context in which the behavior takes place (Mischel, 1968, 1969).

Susceptibility to this attributional error depends upon whether we are examining our own behavior or observing the behavior of others. We tend to attribute the behavior of others to the nature of the person, while seeing our own behavior as conditioned by the nature of the situation in which we find ourselves (Jones, 1976).

This bias is partially explained by differences in information available to actors and observers. In evaluating our own behavior, we compare our present behavior with our own past behavior in similar or different contexts. This past behavior is well known to us, so it is easy to compare the impact of different situations on our behavior over time. This causes us to focus on the nature of the situation as the principal variable explaining differences in our own behavior. The observer of another person, on the other hand, typically lacks this depth of knowledge of the other person's behavior in other circumstances. So the observer's orientation is to examine how the actor's behavior compares with the behavior of other persons under similar circumstances. This prompts a focus on the nature of the person rather than on the nature of the situation.

American intelligence analysts responsible for the Soviet Union and those responsible for China, both working on Sino-Soviet relations, persistently tend to accept quite different assumptions. Soviet analysts tend to attribute Chinese behavior to the nature of the Chinese, while they see Soviet options as circumscribed by many situational constraints. Chinese analysts tend to take the opposite view, that is, that the Russians behave like Russians while Chinese actions are the product of the situation in which the Chinese find themselves.[3]

Familiarity with a country the analyst is assigned analytical responsibility for may produce empathy, understanding, and consequent attribution of behavior to external circumstances rather than to the nature of the actor. Lack of information

3. The source is personal discussions with CIA analysts.

concerning the past behavior and current circumstances of an actor, or lack of empathy for whatever reason, causes one to perceive that actor's behavior as stemming from its own inherent nature (Regan and Totten, 1975). As with all cognitive biases, this is a tendency, not a black-and-white rule that applies to all people at all times. In assessing the behavior of others, we normally make some allowance for situational pressures and role requirements, but this allowance is often insufficient.

If we fall prey to the attributional bias of judging another country's behavior as more heavily influenced by the nature of the government or its leaders than is in fact the case, we tend to perceive that state as more hostile than it really is. Actions that adversely affect our interests are attributed to the predispositions and attitudes of the other country and are, therefore, seen as expressing hostility. If, however, the other nation's actions are actually responsive to situational constraints, it would be unnecessary to assume hostile intent.

Attribution of behavior to personal or national characteristics and the assumption that these characteristics are consistent over time leads to the perception of behavior as inflexible and unchanging. Conversely, to the extent that behavior is attributed to external circumstances, it is perceived as flexible and subject to influence by our own actions. Jervis (1976: 319-355) cites many historical examples of these biases. Heuer (1980a) has applied hypotheses from attribution theory to analysis of the causes of the Soviet invasion of Afghanistan.

Implications for Deception

Deception planners need to avoid these biases relating to causality in order to evaluate accurately the situation in which they find themselves, and estimate how a target is likely to respond to whatever information is provided. The most direct relevance of these biases to the question of deception, however, is their impact on the analyst seeking to detect and avoid deception. Both biases tend to make analysts perceive deception when it is not really there. Of course, there are also other influences that work in the opposite direction.

Deception is an example par excellence of a policy that is centrally directed, well-planned, and highly coherent and rational. As a causal explanation, deception is intrinsically satisfying precisely because it is so orderly and rational. When other persuasive explanations are not available (perhaps because the phenomena we are seeking to explain were actually caused by mistakes, failure to follow orders, or other factors unknown to us), deception offers a convenient and easy explanation. It is convenient because intelligence officers are generally sensitive to the possibility of deception, and its detection is often taken as indicative of sophisticated, penetrating analysis.[4] It is easy because almost any evidence can be rationalized to fit the deception hypothesis; in fact, one might argue that once deception is assumed, this hypothesis is almost immune to disconfirmation. It is precisely this problem that plagued the CIA in evaluating the bona fides of an apparent Soviet intelligence defector, Yuri Nosenko (Martin, 1980).

Any tendency to perceive deception may be reinforced by bias toward perceiving the behavior of others as caused by the nature of the person rather than by situational constraints. It is satisfying to attribute deviousness and malevolence to our enemies; and if they are devious and malevolent, of course they will engage in deception. When we observe activity that we do not otherwise understand, deception may be a more attractive explanation than simply to admit that we have insufficient information or understanding of the situation.

Problems of Counterdeception

The diverse perceptual tendencies and cognitive biases and their implications for deception and counterdeception are summarized in Table 1. The two primary conclusions that emerge from this examination highlight the unenviable position of the decision maker or intelligence analyst seeking to detect deception.

4. This is especially true of operational personnel engaged in intelligence collection and counterintelligence, less true of intelligence analysts.

TABLE 1
Review of Biases and Their Implications for Deception

Bias	*Implication*
	Perceptual Biases
Perceptions are influenced by expectations. More information, and more unambiguous information, is needed to recognize an unexpected phenomenon than an expected one.	It is far easier to reinforce a target's existing preconceptions than to change them.
Perceptions are quick to form but resistant to change. Once an impression has been formed about an object, event, or situation, one is biased toward continuing to perceive it in the same way.	It is far easier to reinforce a target's preconceptions than to change them. Ability to rationalize contradictory information may offset risks of security leaks.
Initial exposure to ambiguous or blurred stimuli interferes with accurate perception even after more and better information becomes available.	Impact of information can be affected by the sequence used in feeding it to a target.
	Biases in Estimating Probabilities
Probability estimates are influenced by availability–how easily one can imagine an event or remember instances of the event.	Employees of watch offices will generally overestimate the probability of whatever they are watching for. Cases of deception are more memorable, hence more available, than instances when deception was not employed.
Probability estimates are anchored by some natural starting point, then adjusted in response to new information. Normally they are not adjusted enough.	It is easier to reinforce a target's existing preconceptions than to change them.
	Biases in Evaluating Evidence
People have more confidence in conclusions drawn from a small body of consistent data than from a larger body of less consistent information.	Deceiver should control as many information channels as possible to limit discrepant information available to target. Deception can be effective even with small amount of information.
Less-than-perfectly-reliable evidence is often processed as though it were wholly reliable.	Judgments may be overconfident.

(Continued)

TABLE 1 (Continued)

Bias	*Implication*
Biases in Evaluating Evidence (Continued)	
People have difficulty factoring the absence of evidence into their judgments.	For deception planners, errors of omission are less serious than errors of commission. To detect deception, analyze what inferences may be drawn from fact that some evidence is *not* observed.
Impressions tend to persist even after the evidence on which they are based has been fully discredited.	Consequences of a security leak may not be as serious as might otherwise be expected.
Biases in Attributing Causality	
Events are seen as part of an orderly, causal pattern. Extent to which other countries pursue a coherent, goal-maximizing policy is overestimated. Randomness, accident, and error tend to be rejected as explanations.	As a causal explanation, deception is intrinsically satisfying because it is so orderly and rational.
Behavior of others is attributed to the nature of the person or country, while our own behavior is attributed to the nature of the situation.	It is satisfying to attribute deviousness and malevolence to our enemies, and if they are devious and malevolent, of course they engage in deception.

—Perceptual tendencies and cognitive biases strongly favor the deceiver as long as the goal of deception is to reinforce a target's preconceptions, which is by far the most common form of deception. Under these circumstances, the deceiver clearly holds most of the cards. If the situation is such that the deceiver can achieve planned goals only by changing the target's preconceptions, however, the target is shielded by many of the same cognitive processes that otherwise work to his or her disadvantage.

—While security is obviously desirable for any deception plan, perfect security is rarely attained and deceptions succeed without it. When the deception is planned to reinforce preconceptions, the target's propensity to rationalize discrepant information commonly offsets security leaks and uncontrolled channels of information. The counterdeception analyst, therefore, cannot even count on being able to interpret accurately windfalls that seemingly ought to reveal the deception plan.

These conclusions based on psychological research are confirmed by Barton Whaley's empirical analysis of 68 historical cases of strategic surprise or deception between 1914 and 1968. Of the cases studied by Whaley, deception was successful in 91% of the cases in which it was attempted; 79% of the cases exploited the target's preconceptions. None of the cases studied by Whaley enjoyed perfect security. Some more or less specific warnings were present in every instance, yet surprise or deception was successful nonetheless (Whaley, 1969: 164).

The problem, however, is not only that deception is generally successful. A closely related problem is the fact that concern about deception often leads to the perception of deception when it is, in fact, not present. Whaley's (1969: 230) research provides a fascinating insight on this point. He found ten cases in which detailed military plans were compromised to an enemy prior to an intended military attack. In half of these cases, the plans were a carefully fabricated deception, while in the other half they represented a genuine breach of security. The fabricated plans were accepted as genuine in all five cases, while the genuine plans were rejected as fabrications in four of the five instances!

A more recent, dramatic example was the November 1977 estimate by Israeli military intelligence that President Sadat's announced intention to visit Jerusalem was most likely deception intended to mask preparations for Egyptian attack (Stein, 1980). These examples suggest that perception of deception when it does not exist may be a common phenomenon: We may be relatively unaware of it only because such instances are less likely to be studied by historians than cases in which deception has been pursued and has met with success.

Clearly, the accurate detection of deception is extraordinarily difficult. No counterdeception program will ever eliminate vulnerability to deception, but incremental gains in reducing vulnerability may be possible. I shall now critique several commonly advocated approaches to countering deception and suggest two others that might be usefully employed.

IMPROVED INTELLIGENCE COLLECTION

One potential approach to overcoming deception is, of course, improved intelligence collection. This has been the course pursued by the U.S. intelligence community for many years. Major advances in technical collection systems have certainly improved the intelligence community's ability to provide accurate answers to specific questions of limited scope; but they have contributed little toward improving estimates of intentions, strategy, or political dynamics.

Experimental research on the relationship between amount of information available to an analyst and the accuracy of judgments based on that information shows that, as a general rule, acquisition of additional increments of information does not improve accuracy of judgment but does strongly increase self-confidence in one's judgments. The new information continues to be analyzed within the framework of the same mental set and is perceived as confirming that set (Heuer, 1979). There certainly are circumstances when new information is highly diagnostic and does improve estimative accuracy, and improved intelligence collection is much desired. The kinds of additional information one might realistically expect to obtain through enhanced collection capabilities, however, are unlikely to reduce vulnerability to deception significantly. Any systematic counterdeception program must focus primarily on problems of analysis, only secondarily on collection.

INCREASED ALERTNESS TO DECEPTION

A second approach to counterdeception assumes that increased alertness to deception will enhance one's ability to detect it. This assumption is implicit in the views of those who believe CIA analysts are not sufficiently tough-minded and realistic (Ellsworth and Adelman, 1979) and have, as a result, been victimized by longstanding Soviet deception concerning strategic

missile systems (Lee, 1977; Sullivan, 1979, 1980). There are two aspects to the alertness question. How alert are the analysts already? Would greater alertness help detect deception?

Among current employees and observers of American intelligence, there is no consensus on whether analysts are properly sensitive or insufficiently sensitive to the possibility of deception, especially deception by the Soviet Union—and there is no way to measure this sensitivity objectively. From the standpoint of psychological theory, I have previously noted psychological tendencies that may cause people to be oversensitive to deception. The availability bias suggests that because instances of deception are far easier to recall than cases in which deception was not employed under similar circumstances, the ubiquity of deception will tend to be overestimated. We are also attracted to deception as an explanation for otherwise incongruous events, because this explanation imposes order and reason on an otherwise disorderly set of data, and it enables us to attribute deviousness and malevolence to our enemies.

These are not the only factors that determine one's sensitivity to deception, however. They may well be offset by contrary tendencies, and probably are in many instances. Evidence on most situations of interest to decision makers and intelligence analysts is incomplete and ambiguous under any circumstances. Considering the possibility of deception imposes yet another intellectual and psychological burden. This undermines the credibility of whatever evidence is available and reduces the likelihood of arriving at a meaningful analytical conclusion to guide decision making. As a consequence, decision makers and analysts alike often resist seriously coming to grips with this possibility.

Even if analysis were more alert to deception, this may not be helpful. The alertness of a magician's audience certainly does not impair the magicians ability to deceive; on the contrary, the magician commonly exploits this alertness to control where the audience focuses its attention.

Alertness to deception presumably prompts a more careful and systematic review of the evidence. Up to a point, this may be

useful. If one has not previously given serious consideration to the possibility of deception, simply focusing on this possibility may be sufficient to identify overlooked information or prompt a changed analytical perspective. Often, however, increased alertness will be of no value, as it simply leads the analyst to be more skeptical of all the evidence. To the extent that evidence is deemed unreliable, the analyst's preconceptions must play a greater role in determining what to believe, and there is no reason to believe these preconceptions will necessarily be accurate.

If deception is not present, increased alertness may predispose an analyst to perceive it erroneously. If deception is present, and if the deceiver's goal is to exploit and reinforce one's preconceptions, heightened alertness may lead the analyst to dismiss the wrong evidence. The evidence that would be identified as deceptive, and hence be dismissed, would almost certainly be that which does not fit preconceptions.

WEIGHTING OF TACTICAL INDICATORS

A third approach to the deception problem is derived from Abraham Ben-Zvi's (1976) study of surprise military attacks. Ben-Zvi suggests that the incidence of surprise might be reduced if estimates of impending attack accorded greater weight to what he calls tactical indicators as distinct from strategic assumptions. Examples of strategic assumptions include the U.S. belief in 1941 that Japan wished to avoid war at all costs because it recognized U.S. military superiority; and the Israeli belief in 1973 that the Arabs would not attack Israel as long as they lacked sufficient airpower to secure control of the skies. Such preconceptions are based on a large body of interrelated evidence and have usually persisted for a long time. Tactical indicators are the specific reports concerning preparations or intent to initiate hostile action, or more generally, specific evidence from current events that indicates the direction in which events are moving. This distinction between strategic assumptions and tactical indicators is very similar to the distinction between preexisting beliefs and new information.

Ben-Zvi studied five cases of intelligence failure to foresee a surprise attack: Pearl Harbor, German attack on the Soviet Union in 1941, Chinese intervention in the Korean War, Chinese attack on India in 1962, and the Arab attack on Israel in 1973. He found in each case that tactical indicators of impending attack were present but were discounted because they conflicted with analysts' and decision makers' preconceptions. The strategic assumptions were not revised in the light of the increasing flow of contrary tactical information.

Ben-Zvi argues that whenever strategic assumptions of intention to attack and tactical indicators of impending attack converge, an immediate threat is perceived and appropriate preparations made. When there is a divergence between strategic assumptions and tactical indicators, however, the strategic assumptions always prevail. Thus despite evidence of preparations for an attack, the actual attack comes as a "surprise," as in the five cases analyzed. Ben-Zvi concludes that tactical indicators should be given increased weight in the decision-making process.

This may well be appropriate advice. It certainly accords with the finding that people err most often by being too quick to reject new information that does not conform to their preconceptions. But Ben-Zvi does not consider cases in which alarming tactical indicators have been properly discounted as maneuvers, bluff, or deception rather than as indicators of impending attack. Ascribing more weight to tactical indicators in all cases will increase the frequency of false alarms, and this, too, entails costs. While we should, *in general,* be more open to changing our minds as a result of discrepant tactical or other information, in any single case it is impossible to know a priori whether to revise an estimate or stick with a long-established view.

COGNITIVE AIDS TO ANALYSIS

Deception is, above all, a cognitive phenomenon; it occurs in our minds. Enhanced ability to detect deception largely depends upon improved cognitive processing of information. Research in cognitive psychology does not provide direct and immediate

solutions to the counterdeception problem. It does, however, offer insights that are of indirect assistance.

Once we understand how the mind processes information, including the diverse perceptual and cognitive biases to which people are subject, we can then seek ways to compensate for some of these basic problems in human information processing. At the very least, we can identify situations in which our normal faith in our impressions should be suspended, and in which some more systematic means of handling the evidence may be appropriate.

Psychological research also helps identify analytical procedures and methods that are useful to guide or supplement intuitive judgment. Current research, for example, suggests that people perform poorly at generating a full set of hypotheses (Gettys et al., 1980). If the correct hypothesis is not even formulated for consideration, there is clearly little chance of making an accurate judgment. More attention devoted to formation of alternative hypotheses and identification of the indicators and observables associated with each hypothesis would help guide the search for and evaluation of evidence. A full set of hypotheses and indicators also serves as an organizational structure for storage and recall of information from memory.

There is a strong tendency to view the significance of evidence in terms of the degree to which it supports, contradicts, or seems irrelevant to a single hypothesis that we already believe to be true. We overlook the fact that evidence we think of as supporting our case may also be quite consistent with several alternative hypotheses; we then draw from the evidence false confirmation of preexisting beliefs. This can be avoided only by evaluating the evidence in terms of its diagnostic value in helping revise our estimates of the relative likelihood of all possible hypotheses. The systematic identification, examination, and testing of alternative hypotheses is one of the keys to the successful uncovering of deception.

A common factor in cases of successful deception, and in most cases of intelligence surprise in general, is that analysts become fixed in a mental set that does not respond effectively to discrepant information. It is difficult to view familiar data from a

different perspective, yet this is exactly what may be required to identify deception. Therefore, methods for breaking mental sets are particularly relevant for counterdeception analysis. This includes such practices as competitive analysis, use of a devil's advocate to analyze deception scenarios, interdisciplinary brainstorming, and other techniques that facilitate the identification and systematic analysis of alternative perspectives. The next section suggests that an organizational solution to this problem might be found through formation of a counterdeception staff charged with responsibility for representing the deception perspective.

ORGANIZATIONAL MEASURES

At a colloquium on intelligence analysis organized by the Consortium for the Study of Intelligence (Godson, 1980), William Harris observed that the counterintelligence function within the U.S. intelligence community has been limited to operational departments concerned with the collection of intelligence from human sources. There is no functional equivalent of counterintelligence within the analytical components. In short, the analytical side of the intelligence community lacks any focal point for the analysis and detection of deception.

The creation of a counterdeception staff within one or more analytical components might be a useful form of "deception insurance." It may seem inappropriate to suggest organizational innovation as a response to cognitive problems occurring at the individual level. However, analysts function within an organizational environment, and their thinking is influenced by that context. Moreover, research on perception clearly indicates that taking a familiar body of data, then reorganizing it mentally to view it from a totally different perspective, is a most difficult cognitive task. The more complex the body of data, and the longer one has held an image of that data, the more difficult it is to view it differently. When analysis of the alternative perspective is

unusually complex, technical, time consuming, or costly, it is unlikely to be pursued without strong organizational support.

As a general rule, the examination of evidence from alternative perspectives to test multiple hypotheses, that is, several hypotheses assuming both deception and no deception, must be a responsibility of the individual analyst. The cognitive strain involved in simultaneous evaluation of multiple hypotheses should be relieved by cognitive aids to analysis, rather than by organizational engineering. When the size and complexity of the task requires a major organizational effort, however, some organizational adjustment may be necessary.

The most important issue of deception facing the U.S. intelligence community today is of this type. It concerns possible Soviet deception with respect to strategic missile systems. Has the U.S.S.R. succeeded in manipulating U.S. perceptions of its capabilities, strategies, and plans in order to gain advantage during SALT negotiations and after achieving SALT agreements? Some analysts would assert that the United States has been the victim of continuing deception in this field (Lee, 1977; Freedman, 1977; Sullivan, 1979, 1980).

Evaluation of Soviet strategic plans and capabilities is one of those enormously complex issues that transcends the capabilities of any single individual. It is too much to expect a single analyst to make the strongest possible case for a scenario without deception *and* for a scenario that assumes deception. Analysis of such issues is an organizational effort, and the procedures that guarantee a systematic testing of alternative hypotheses might best be built into the organizational structure in the form of a counterdeception staff.

Organizational change to solve one problem is, of course, likely to cause others. Such a staff should become neither an analytical elite nor an institutionalized devil's advocate (George, 1980: Ch. 9). The staff would have a delicate role, but analogy to the functioning of a counterintelligence staff within an intelligence collection unit offers hope that this role could be played effectively.

CONCLUSION

My intention in these final paragraphs has been to be suggestive, not prescriptive. Traditional, intuitive methods of analysis have not been sufficiently effective in detecting deception, so it is necessary to explore other alternatives. I have tried to point out some useful directions that this exploratory effort might take, but a fuller discussion of such proposals is beyond the scope of the present study.

Date of receipt of final manuscript: 1/4/81

REFERENCES

ALPERT, M. and H. RAIFFA (1968) "A progress report on the training of probability assessors." Harvard University. (unpublished)

ANDRIOLE, S. (1980) "Computer-based Bayesian forecasting methodologies," in G. Hopple and J. Kuhlman (eds.) Expert Generated Data: Applications in International Affairs. Boulder, CO: Westview.

BEN-ZVI, A. (1976) "Hindsight and foresight: a conceptual framework for the analysis of surprise attacks." World Politics 28, 3: 381-395.

BRUNER, J. and M. POTTER (1964) "Interference in visual recognition." Science 144, 3617: 424-425.

CARROLL, J. (1978) "The effect of imagining an event on expectations for the event: an interpretation in terms of the availability heuristic." J. of Experimental Social Psychology 14: 88-96.

CHAN, S. (1979) "The intelligence of stupidity: understanding failures in strategic warning." Amer. Pol. Sci. Rev. 73 (March): 171-180.

Decisions and Designs, Inc. (1977) Handbook for Decision Analysis. Technical Report TR-77-6-30. McLean, VA.

DeRIVERA, J. [ed.] (1968) The Psychological Dimension of Foreign Policy. Columbus, OH: Merrill.

DE WEERD, H. (1962) "Strategic surprise in the Korean War." Orbis 6 (Fall): 435-452.

EDWARDS, W. (1968) "Conservatism in human information processing," pp. 17-52 in B. Kleinmuntz (ed.) Formal Representation of Human Judgment. New York: John Wiley.

ELLSWORTH, R. and K. ADELMAN (1979) "Foolish intelligence." Foreign Policy 36 (Fall): 147-159.

FISCHHOFF, B., P. SLOVIC, and S. LICHTENSTEIN (1978) "Fault trees: sensitivity of estimated failure probabilities to problem presentation." J. of Experimental Psychology: Human Perception and Performance 4 (May): 330-344.

FREEDMAN, L. (1977) U.S. Intelligence and the Soviet Strategic Threat. New York: Macmillan.

GEORGE, A. (1980) Presidential Decisionmaking in Foreign Policy: The Effective Use of Information and Advice. Boulder, CO: Westview.

GEORGE, A. and R. SMOKE (1974) Deterrence in American Foreign Policy. New York: Columbia Univ. Press.

GETTYS, C., C. KELLY, and C. PETERSON (1973) "The best guess hypothesis in multi-stage inference." Organizational Behavior and Human Performance 10, 3: 364-373.

GETTYS, C., C. MANNING, T. MEHLE, and S. FISHER (1980) Hypothesis Generation: A Final Report of Three Years of Research. Technical Report 15-10-80. Norman, OK: Decision Processes Laboratory, Univ. of Oklahoma.

GODSON, R. [ed.] (1980) Intelligence Requirements for the 1980's: Analysis and Estimates. Washington, DC: National Strategy Information Center.

HANDEL, M. (1976) "Perception, deception and surprise: the case of the Yom Kippur War." Jerusalem Papers on Peace Problems 19. Jerusalem: Hebrew Univ.

HEUER, R. (1980a) "Analyzing the Soviet invasion of Afghanistan: hypotheses from causal attribution theory." Studies in Comparative Communism 13 (Winter).

——— (1980b) "Applications of Bayesian inference in political intelligence," in G. Hopple and J. Kuhlman (eds.) Expert Generated Data: Applications in International Affairs. Boulder, CO: Westview.

——— (1979) "Improving intelligence analysis: some insights on data, concepts, and management in the Intelligence Community." Bureaucrat 8, 4: 2-11.

HOGARTH, R. (1980) Judgement and Choice. New York: John Wiley.

JERVIS, R. (1976) Perception and Misperception in International Politics. Princeton, NJ: Princeton Univ. Press.

JOHNSON, E. (1974) "The effect of data source reliability on intuitive inference." Technical Paper 251. Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.

JONES, E. (1976) "How do people perceive the causes of behavior." Amer. Scientist 64: 300-305.

——— and R. NISBETT (1971) The Actor and the Observer: Divergent Perceptions of the Causes of Behavior. New York: General Learning.

KAHNEMAN, D. and A. TVERSKY (1979) "Intuitive prediction: biases and corrective procedures." TIMS Studies in the Management Sciences 12: 313-327.

KNORR, K. (1964) "Failures in national intelligence estimates: the case of the Cuban missiles." World Politics 16 (April): 455-467.

LANGER, E. (1977) "The psychology of chance." J. for the Theory of Social Behaviour 7: 185-208.

LAU, R., M. LEPPER, and L. ROSS (1976) "Persistence of inaccurate and discredited personal impressions: a field demonstration of attributional perseverance." Presented at fifty-sixth Annual Meeting of Western Psychology Association, Los Angeles.

LEE, W. (1977) Understanding the Soviet Military Threat: How CIA Estimates Went Astray. New York: National Strategy Information Center.

MARTIN, D. (1980) Wilderness of Mirrors. New York: Harper & Row.

MASTERMAN, J. (1972) The Double-Cross System in the War of 1939 to 1945. New Haven: Yale Univ. Press.

MISCHEL, W. (1969) "Continuity and change in personality." Amer. Psychologist 24, 11: 1012-1018.

——— (1968) Personality and Assessment. New York: John Wiley.
NISBETT, R. and L. ROSS (1980) Human Inference: Strategies and Shortcomings of Social Judgment. Englewood Cliffs, NJ: Prentice-Hall.
REGAN, D. and J. TOTTEN (1975) "Empathy and attribution: turning observers into actors." J. of Personality and Social Psychology 32, 5: 850-856.
ROSS, L. (1977) "The intuitive psychologist and his shortcomings; distortions in the attribution process," pp. 173-220 in L. Berkowitz (ed.) Advances in Experimental Social Psychology, Vol. 10. New York: Academic Press.
——— M. LEPPER, and M. HUBBARD (1975) "Perseverance in self-perception and social perception: biased attributional processes in the debriefing paradigm." J. of Personality and Social Psychology 32, 5: 880-892.
SCHUM, D. and W. Du CHARME (1971) "Comments on the relationship between the impact and the reliability of evidence." Organizational Behavior and Human Performance 6: 111-131.
SCHWEITZER, N. (1978) "Bayesian analysis: estimating the probability of Middle East conflict," pp. 11-30 in R. Heuer (ed.) Quantitative Approaches to Political Intelligence: the CIA Experience. Boulder, CO: Westview Press.
SHLAIM, A. (1976) "Failures in national intelligence estimates: the case of the Yom Kippur War." World Politics 28, 3: 348-380.
SIMON, H. (1957) Models of Man: Social and National. New York: John Wiley.
STECH, F. (1980) Political and Military Intention Estimation. Technical Report AD-A081486. Bethesda, MD: Mathtech, Inc.
STEIN, J. (1980) "Intelligence and stupidity reconsidered: estimation and decision in Israel, 1973." J. of Strategic Studies (September).
SULLIVAN, D. (1980) "Evaluating U.S. intelligence estimates," pp. 48-73 in R. Godson (ed.) Intelligence Requirements for the 1980's: Analysis and Estimates. Washington, DC: National Strategy Information Center.
——— (1979) "A SALT debate: continued Soviet deception." Strategic Rev. 7, 4: 29-38.
TVERSKY, A. and D. KAHNEMAN (1974) "Judgment and uncertainty: heuristics and biases." Science 185 (September): 1124-1131.
——— (1973) "Availability: a heuristic for judging frequency and probability." Cognitive Psychology 5: 207-232.
——— (1972) "Anchoring and calibration in the assessment of uncertain quantities." Oregon Research Institute Research Bulletin 12.
WASSERMAN, B. (1960) "The failures of intelligence prediction." Pol. Studies 8 (June): 156-169.
WHALEY, B. (1969) Strategem, Deception and Surprise in War. MIT. (unpublished)