# SO MANY WAYS TO LIE:
# THE COMPLEXITY OF DENIAL AND DECEPTION[1]

David T. Moore and William N. Reynolds

*The views expressed in this paper are those of the authors and do not reflect the official policy or position of the National Security Agency, the Department of Defense, the Advanced Research and Development Activity, the Central Intelligence Agency, the Office of the Director of National Intelligence, or the U.S. Government.*

## INTRODUCTION

In recent years, the Intelligence Community has paid increasing attention to the role of complexity science in intelligence analysis. It is well known that intelligence problems are "complex," insofar as they are detailed, multi-faceted, and extremely dynamic. However, this insight has remained qualitative in nature, precluding the development of methods for reducing the complexity of these problems to a level within the capabilities of human reasoning. A more realistic goal is to quantitatively measure the complexity of modern intelligence problems so that their difficulty can be assessed up front. Such measurements will help determine the cost-benefits associated with a problem, the resource allocation it demands, and the most useful analytic methods to solve it.

In this paper, we present a simple quantitative metric for estimating the complexity of denial and deception problems. We show that the complexity of a problem increases as a product of the numbers of possible states (in essence, true, deceptive, etc.) for each of the possibly deceptive pieces of evidence. We enumerate the complete set of contingencies that

[1] The authors gratefully acknowledge the assistance of Rita Bush, David Dixon, William Mills, George Mitroka, Amanda Redmond-Neal, William Parquette, Suzanne Sluizer, and Marta Weber in the preparation of this paper.

must be considered in a denial and deception problem and provide a heuristic-based method for pruning these down to a manageable set that can reasonably be considered by analysts and decision makers.

## WAYS TO THINK ABOUT COMPLEXITY

### Terms of Reference

The term "complexity" is frequently used but poorly understood. Colloquially, all sorts of things may be called "complex" whether or not this description is backed up by a quantitative argument. Naturally, complexity scientists have an interest in eliminating this ambiguity, and there have been literally dozens of attempts to define "complexity" in such a way that it can be quantified in many different contexts.[2] Two formulations of particular note are Andrey Kolmogorov's *descriptive complexity*, the length of the shortest computer program that can reproduce a system's output,[3] and Ludwig Boltzmann's concept of *entropy*[4] (called *information* by Claude Shannon[5]). Following Kolmogorov's approach, Murray Gell-Mann has proposed *crude complexity*; that is, the length of a system's description given by one human expert to

[2] Bruce Edmonds, *Syntactic Measures of Complexity*, Doctoral Dissertation, University of Manchester, 1999, URL: <http://bruce.edmonds.name/thesis/>, accessed 30 August 2005. In this comprehensive survey of complexity metrics, Edmonds identifies over fifty different mathematical and conceptual techniques for measuring complexity.

[3] Thomas M. Cover, and Joy Thomas, *Elements of Information Theory* (New York, NY: Wiley. And Sons, 1999), 144-182.

[4] Francis Weston Sears, *An Introduction to Thermodynamics, the Kinetic Theory of Gases and Statistical Mechanics* (Boston, MA: Addison-Wesley, 1949).

[5] Claude E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal,* 27 (July and October, 1948), 379-423, 623-656, URL: <http://pespmc1.vub.ac.be/LIBRARY.html>, accessed 30 August 2005.

another.[6] Recently, Yaneer Bar-Yam has developed a metric for *scale-dependent complexity* that attempts to unify both entropy and descriptive complexity.[7]

Fundamentally, reasoning about a complex system considers two aspects of the system: First, the constituent elements that make up the system, and second, the configurations those constituent elements can take.

The Kolmogorov/Gell-Mann formulations focus on the first aspect of a complex system. These gauge the complexity of a system according to the number of elements that make up that system. For example, the complexity of a paused chess game would be given by a description of the positions of the pieces, along with the rules of chess. More pieces would lead to a longer description, hence a more complex configuration. In general, this corresponds to our intuitive notion of complexity. We tend to assume that the more features that are to be considered – the more complex the system.

Boltzmann and Shannon's entropy quantifies the second aspect. It simply counts the ways that a system can be configured, and uses this number as a measure of the system's complexity.[8] For example, the entropy of a certain setup of a chessboard would be given as the number of possible games that can be played from that starting point. In intelligence problems, this is an extremely important concept – how many contingencies does the analyst or decision-maker have to consider? In our view, the answer is a two-step process: First, we must determine the complete space of all possibilities – in other words calculate the entropy, and second, we

[6] Murray Gell-Mann, *The Quark and the Jaguar: Adventures in the Simple and Complex* (New York NY: W. H. Freeman and Company), 24.

[7] Yaneer Bar-Yam, "Multiscale Complexity/Entropy," *Advances in Complex Systems,* 7 (2004), 47-63.

[8] Formally, entropy is defined as the logarithm of the number of configurations, however we will ignore this distinction, although this does bring up some interesting issues – Bar-Yam's formulation of complexity may be viewed as a quantification of the extent to which the number of components in system departs from logarithmic dependence on the number of configurations.

must reduce this space to those possibilities relevant to the decision to be made. Every such reduction should be explicitly justified, as discounting contingencies without justification invites strategic surprise.

Finally, the Bar-Yam approach attempts to unify these two views of complexity by asking: how do the elements of a system impact the number of configurations that a system can take? Using our chess example, if we were to remove a piece from the board, would the number of possible games increase or decrease? In general, we would expect the number of games to decrease, since we are removing all of the possible moves and stratagems that the deleted piece made available. However, it is quite conceivable that there are some circumstances where the removal of a piece could increase the number of possible games instead. Bar-Yam's approach quantifies the impact that constituent elements have on a system's configurations.

### Complexity and Intelligence

| Indicator | Status | | Conclusion |
|---|---|---|---|
| Troops | Garrison | Deployed | Normal (Peacetime) |
| Communications | Normal | OTA | |
| Artillery | Garrison | Border | |
| Aircraft Sorties | Low | High | |
| Leadership | Visible | Bunker | |
| **Indicator** | **Status** | | **Conclusion** |
| Troops | Garrison | Deployed | War Pending |
| Communications | Normal | OTA | |
| Artillery | Garrison | Border | |
| Aircraft Sorties | Low | High | |
| Leadership | Visible | Bunker | |
| **Indicator** | **Status** | | **Conclusion** |
| Troops | Garrison | Deployed | Exercise? Denial and Deception before going to War? |
| Communications | Normal | OTA | |
| Artillery | Garrison | Border | |
| Aircraft Sorties | Low | High | |
| Leadership | Visible | Bunker | |

**Table 1: Indicators of Peace, War and Uncertainty**

So what do these technical musings on the nature of complexity have to do with intelligence problems? We submit that the increase in contingencies with the number of elements is a basic confounding mechanism in intelligence problems. For example, consider a simple indicators and warnings problem. The problem

consists of five indicators, and each one of these occurs in one of two states, hostile or peaceful, as shown in table 1.

If troops are in garrison, communications are normal, artillery is not on the border, aircraft sorties are low, and leadership is visible in public, then the situation is normal. If troops are deployed, communications are off the air, artillery is relocated to the border, aircraft sorties are high, and leadership is not in public (*i.e.*, deployed to a protective bunker), then war is imminent. But, what if all of the previous conditions are true *except* that leadership is still visible in public? This, it is learned, is the profile for an exercise. This was observed in the past, and the other side mobilized its troops only to have the adversary redeploy its troops and artillery to garrisons, restart communications, and reduce aircraft sorties. Since responding troop mobilizations are expensive and dangerous – one side might preemptively attack first – the pattern of an exercise is learned. Now, when all the indicators for war but one in particular are present, the conclusion is reached that it is an exercise.

| Indicator | Condition (G=In Garrison, D=Deployed) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Troops | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D |
| Communications | G | G | G | G | G | G | G | G | D | D | D | D | D | D | D | D | G | G | G | G | G | G | G | G | D | D | D | D | D | D | D | D |
| Artillery | G | G | G | G | D | D | D | D | G | G | G | G | D | D | D | D | G | G | G | G | D | D | D | D | G | G | G | G | D | D | D | D |
| Aircraft Sorties | G | G | D | D | G | G | D | D | G | G | D | D | G | G | D | D | G | G | D | D | G | G | D | D | G | G | D | D | G | G | D | D |
| Leadership | G | D | G | D | G | D | G | D | G | D | G | D | G | D | G | D | G | D | G | D | G | D | G | D | G | D | G | D | G | D | G | D |

**Table 2: The Set of Indicators and Conditions of a Five-Indicator Binary Warning System. Which indicate peace? Which indicate war? What do the others signify?**

What of the other possibilities (as shown in table 2)? One reason why indicator-based assessments fail is that the number of indicator combinations exceeds the sense-making capabilities of analysts. The "additive misperception" arises when a linearly thinking analyst considers that adding a single indicator to five preexisting indicators merely increases the things

she has to worry about by 20%. If another indicator is added, her manager may suggest adding another analyst to the team to cope with the increase.[9]

However, a Kolmogorov/Gell-Mann formulation of the complexity of this indicators and warnings problem would place its complexity at 5, meaning the addition of a sixth indicator increases the complexity of the problem by 20%. If we use an entropic metric, we must also consider every state that the indicators can take. In this case, that number is 2 (the number of states) to the power of 5 (the number of indicators), or 32. Adding a new indicator increases the exponent to 6, yielding 64 contingencies – an increase of 100%. Adding yet another new indicator, for a total of seven, a 40% change, leads to a 400% increase. This is a nonlinear, *multiplicative* progression that is typically and erroneously thought of as *additive*. The addition of the extra analyst to the problem is an insufficient solution to the combinatorial explosion.

Further, what happens if the adversary knows what indicators are employed in making determinations of war, peace, and exercises? In this case adversarial denial and deception can disguise or mask key indicators, leading to miscalculations. As illustrated in the third table in table 1, the leadership might remain in public, offering statements of peace even while the troops are massing on and then pouring over the border. The leadership subsequently disappears into the bunkers as hostilities begin. The adversary knows that providing the other side – and perhaps its U.S. allies – with little or no advanced warning increases the likelihood of (at least initial or partial) success.

An illustration of such denial and deception occurred when the United States government issued a demarché to India in 1995. By warning the Indian government not to conduct what appeared to be a nuclear test, the U.S. officials revealed the indicators employed in making such

[9] A related argument was developed by IBM vice-president Frederick P. Brooks based on his management experiences during the 1960s and 1970s. See Frederick P. Brooks, *The Mythical Man-Month: Essays on Software Engineering,* 20th Anniversary Edition (Boston, MA: Addison-Wesley Professional, 1995).

assessments. U.S. intelligence professionals believed their subsequent analyses showed no Indian nuclear test preparations. Instead, they were being denied access to the indicators of such a test. When, in 1998 India successfully conducted a nuclear test, surprising the United States, the Indian government boasted of its success.[10]

There are several considerations that require further discussion. First, indicators themselves are a coarse-grained shorthand for reality. "Troops in Garrison" is a binary summary of a continuous reality. In fact, some troops are always in garrison while others are not. The same is true for other indicators in the example cited above. Making them discrete indicators introduces approximations that may not correspond to the actual situation.

The reality is actually much more complex. Such systems are rarely based on only five (or six, or seven) binary indicators. Many different indicators with trinary or greater outcomes are possible and likely. These combine in novel fashions that quickly outstrip assessment capabilities of people and even computers. So, while too coarse-grained a scale may not capture reality, a too fine-grained one overwhelms the capacity to detect significant changes.

Also, it may be that an evolving pattern of relationships among the indicators reveals the adversary's intentions. An emerging behavior develops based on the noted indicators and the responses by the other side. Finally, a temporal dimension can be added, compounding further what is already complex.

As the indicators in table 1 move from blue to red, a decision point is reached. While analysts may not understand what the pattern means, a warning must be issued to the policy community. Deterrents – either diplomatic or military – require preparation in advance. If the situation really is a prelude for an attack then the deterrent may effectively prevent it. If no

[10] Paul J. Raasa, "The Denial and Deception Challenge to Intelligence," in Roy Godson and James J. Wirtz, *Strategic Denial and Deception* (New Brunswick, NJ: Transaction Publishers, 2002), 178, 223-224.

attack was planned, perhaps because the other side was conducting an exercise, then both sides can refer to their actions as "exercises." There is of course, a risk that if the adversary misperceives the deterrent preparations then their own actions may escalate.

Ultimately, can such judgments reliably be made in the first place? David Schum notes: "There is never any base of relevant evidence that can be analyzed statistically."[11] In other words, every indication-based situation is unique. Therefore, the premises on which such considerations are made are false: The fact that something occurred in the past is no guarantee that it will happen again in the future. Indeed, the closer one gets to individual actors, the less likely it is that specific actions will be repeated. As noted, a response to an adversary's state could trigger further actions leading to an accelerating pattern of miscalculations that results in hostilities.

In a sense, this is what happened during the Cold War. Both sides engaged in brinksmanship based on a series of indicators and warnings, but fortunately backed down when things got too heated. Somehow, each side assessed correctly when the other was engaged in an exercise. Although mistakes were made, neither side overreacted; perhaps because the ultimate consequences were mutual destruction.[12]

Finally, complexity is not simply multiplication – these indicators are related to one another in subtle ways. A human is needed to determine, of the 100% increase in states that

---

[11] David A. Schum, "Evidence Marshaling for Imaginative Fact Investigation," *Artificial Intelligence and Law,* 9 (2001), 165. Of note is the fact that the insurance industry bases its business on capitalizing the opposite view. However, insurance is based on predictions about things not happening. Further, acceptance and premiums are based on the absence of risk in policyholders. Houses on eroding cliffs and policyholders with terminal illnesses are routinely denied insurance policies.

[12] The notion of "transparency" combined with a couple of assumptions contributed to each side's being able to predict the likely actions of the other. Adversaries invited observers at exercises. Training followed scripts that were predictable. And both sides assumed the other would not want to start something that led to its own annihilation. Even so, the Soviet Union successfully surprised the United States on several occasions, as the 1956 Hungarian repression, the 1962 Cuban missile crisis, the 1968 Czech repression, and the 1979 invasion of Afghanistan make clear.

comes with each new indicator, how many really convey new information. This task cannot be trusted to a formula or other automation because the different indicators have highly non-linear relationships with one another that depend on hypotheses about the intentions and capabilities of the adversary as well as the meanings of the indicators. The addition of constituent elements to a problem frequently has a confounding impact, wherein the number of configurations increases, but sometimes it *disambiguates* existing configurations instead, reducing the set of contingencies that must be considered. Each of the indicators can be characterized by its impact, confounding or disambiguating, on the complexity of the problem.

## THE CHALLENGE OF DENIAL AND DECEPTION

Denial and deception is an ongoing problem because it works so well. As Cynthia Grabo observes, even elementary deceptions are often very effective.[13] In our view, they succeed because our analytic process either does not generate correct hypotheses in the first place, or allows hypotheses to be discarded without justification. With this in mind, we argue that the first step in a method to counter denial and deception should be to *systematically generate all possible deception hypotheses*. As we have argued above and will demonstrate further, there are multiple difficulties with this approach – difficulties that reflect the underlying complexity of the denial and deception problem.

As previously described, the possibility of deception introduces a combinatorial explosion of hypotheses that must be considered, and the limitations of human reasoning makes addressing all possible hypotheses unreasonable. Thus a second requirement for a method to counter denial and deception is that it must efficiently and correctly prune the number of

[13] Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, 2002), 129.

deception hypotheses, removing those hypotheses that are disconfirmed by evidence. The output of the method should be a set of related hypotheses of cognitively manageable size; that is, five to seven items at a time. [14] By *efficiently* we mean that the method must be useable by analysts in realistic timeframes (requiring an analyst to exhaustively consider 10,000 deception hypotheses one by one is clearly not realistic). By *correctly* we mean that the method should only weed out those deception hypotheses that are explicitly disconfirmed by evidence.

One approach to denial and deception problems is Heuer's Analysis of Competing Hypotheses (ACH).[15] ACH involves marshalling the available information into a set of evidentiary elements, and then listing the evidence in a table, along with a set of hypotheses generated by the analyst. For each evidence/hypothesis combination, the analyst determines whether the evidence is confirmatory, disconfirmatory, or irrelevant to the hypothesis, with disconfirmatory evidence carrying the greatest weight.[16] To address denial and deception problems, the analyst provides a deception hypothesis, which is also scored against the evidence.

Unfortunately, the addition of a single deception hypothesis does not properly capture the complexity of any denial and deception problem. Although it is an absolutely essential first step, admitting the possibility that one is being deceived does not answer *whether* one is being deceived, and in particular, it does not answer *how* one might be deceived – a fundamental problem for the victim of deception is that there are so many ways to lie. Barton Whaley suggests that one response to the deception problem is to seek inconsistencies in one's perceived

[14] George A. Miller. "The Magical Number Seven, Plus or Minus Two," *The Psychological Review*, 63 (1956), 87, URL: < http://psychclassics.yorku.ca/Miller/>, accessed 14 March 2006.

[15] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: CIA Center for the Study of Intelligence, 1999), 95-110.

[16] This is based on the theory of scientific falsifiability, advocated most famously by Karl R. Popper in *The Logic of Scientific Discovery* (New York, NY: Routledge, 2002).

information.[17] The problem with this approach is, again, combinatorial explosion – for N pieces of evidence, there are $(N^2-N)/2$ two-way possible comparisons that should be examined. Since inconstancies typically occur at very fine-grained levels, where there are lots of data, this leads to enormous numbers of comparisons (*e.g.,* 1000 data elements would require 999,000 comparisons). If data need to be compared three at a time or more to detect a deception, the problem worsens, increasing as the number of elements to the power of the number of comparisons.

Since discovering deception, *a priori*, from data is difficult, it seems reasonable to generate specific hypotheses as to how an adversary may attempt to deceive us, and use these hypotheses as guides for detecting deception and developing contingencies to respond to possible deceptions (*i.e.,* take measures to avoid surprise). How then do we generate appropriate deception hypotheses? One approach is indicated by insights into the nature of deception:

- If we are being deceived, then something we believe is wrong.
- Through a process of inversion, we should use each of our potentially erroneous beliefs as a starting point for generating deception hypotheses.
- We do not know which, if any, of our beliefs to distrust, and are thus faced with an overwhelming set of deception hypotheses.

Above, in speaking of "things we believe," we are referring to items of evidence. Evidence consists of beliefs we hold about the state of the world that are created through a process of marshaling data and information. At their most basic level, these beliefs depend on credibility, relevance, and inferential or probative force. In other words, our beliefs are scrutinized in terms of whether they are indeed believable, bear on the issue, and are persuasive. Unfortunately, the analysts involved must establish these properties for each fact or collection of

[17] Barton Whaley, and Jeffrey Busby, "Detecting Deception: Practice, Practitioners and Theory" in Roy Godson and James J. Wirtz, eds., *Strategic Denial and Deception: The Twenty First Century Challenge* (New Brunswick, NJ: Transaction, 2005), 181. Cited hereafter as Whaley and Busby, "Detecting Deception."

facts that ultimately will become evidence. When effective, such considerations abet uncertainty reduction. This occurs through a process of argument, creative hypothesis generation, and the development of chains of reasoning.[18]

For purposes of denial and deception discovery, we must consider two potential states for each piece of evidence: "true" or "deceptive." A more sophisticated approach uses multiple evidentiary states, for example, "true," "deception by adversary," or "self-deceptive." In fact, reasoning with uncertain or contradictory evidence is a hallmark of intelligence analysis – consequently, this uncertainty will often be incorporated in the possible states we will attribute to the evidence. Since we do not know exactly which, if any, items of evidence are deceptive, we must consider all possible configurations of the evidence. For example, we may be uncertain about the state of a given piece of evidence – we have contradictory statements about leadership's visibility. We could assign such an indicator four states: "visible, true" – we perceive the leadership are visible and we are not being deceived; "visible, deceptive" – we perceive the leadership is visible and we are being deceived; "hidden, true" – we perceive the leadership is hidden and we are not deceived; and "hidden, deceptive" – we perceive leadership is hidden and we are being deceived. Since we must consider the possibility of deception for each evidentiary element, the analyst must deal with a combinatorial explosion of possible deceptions. We can incorporate additional sources of uncertainty and deception, such as the possibility of self-deception by adding possible states that each evidentiary element can take.

Let us revisit our earlier indicators and warnings problem, which involved five pieces of evidence – only this time, the evidence items can be either true or deceptive (rather than hostile

[18] For more information on evidentiary considerations see Francis J. Hughes and David A. Schum, *Credibility Assessment: A First Step in Intelligence Analysis,* unpublished tutorial, Joint Military Intelligence College, April 2003; and David T. Moore, *Critical Thinking and Intelligence,* Occasional Paper Number 14 (Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, in press). Cited hereafter as Moore, *Critical Thinking*.

versus peaceful), and we have no uncertainty in our perceptions of their state. Considering the possibility that any combination of these could be true or deceptive gives us $2^5 = 32$ different configurations of the evidence. Thus, instead of considering a single problem with 5 pieces of evidence, in order to completely cover the deception space, we must consider 32 separate problems: the original problem plus 31 deception problems. If there were 3 possible deception states for each indicator, then the number of deception hypotheses would be $3^5 = 243$. These numbers provide a rough metric of the extent to which deception compounds complexity in this type of problem. Informally, we are counting *the number of ways to lie.* In the context of the original ACH approach, we now have two separate types of hypotheses: *evidentiary* hypotheses, which conjecture on the deceptiveness of the evidence, and *causal* hypotheses, which provide explanations of the evidence (including its deceptive nature). As in the original ACH method, the causal hypotheses must be generated separately for each evidentiary hypothesis and scored against the potentially deceptive evidence. However, in this new approach, we no longer need to add a special deception hypothesis because each configuration of the evidence indicates how the deception is being conducted.

This first step provides a systematic enumeration of possible deceptions, given a particular set of evidentiary beliefs. The next question is how to effectively handle this potentially enormous set of evidentiary hypotheses? A natural place to start is at the source of our combinatorial explosion – the likely deceptiveness of the evidence. If we are considering the possibility of active deception by our adversary, then we must ascertain the likelihood that each individual piece of evidence is deceptive. A short list of indicators that helps in that task is: means, opportunity, motive, and past operational practices.

### Means

The first question is whether the adversary is capable of faking a particular piece of evidence. Some evidence, such as that based on signals, is fairly easy to falsify, but other evidence, such as that provided by multiple types of sensors, is more difficult to falsify.[19] For our modified ACH method, the means test is to sequentially consider each piece of evidence that represents our belief and determine whether the adversary has the means to falsify it. If the answer is no, then evidentiary hypotheses that assume the piece of evidence is falsified can be discarded. For each such elimination, we reduce the number of evidentiary hypotheses by a factor of the number of states for that piece of evidence.

### Opportunity

This next test asks whether our adversary is aware of our collection mechanisms and is able to transmit falsified data for our sensors. Again, the type of the evidence will determine whether there are reasonable grounds to suspect falsification. If insufficient opportunity exists for falsification of a given piece of evidence, we can eliminate all deception hypotheses that include the falsification of that evidence. Again, we expect a factor-of-state-number reduction in evidentiary hypotheses for each such elimination.

### Motive

Motive deals with the *why* of deception. What is the purpose the adversary is trying to achieve by engaging in a deception? In the context of ACH using evidentiary hypotheses, questioning motive puts the cart before the horse. In the proposed approach, we instead *posit* certain patterns of deception and then generate hypothetical motives that fit the evidentiary

[19] Whaley and Busby, "Detecting Deception," 196.

hypotheses. In this method, the absence of a reasonable motive to fit into a particular evidentiary hypothesis would constitute a disconfirmatory argument, allowing us to discard that hypothesis. However, this approach means that each evidentiary hypothesis must be considered in turn, so it does not meet our requirement for efficiency. In the interest of efficiency, analysts should only speculate about motive *after* applying the tests of means and opportunity.

### Past Operational Practices

Does the adversary have a past history of deception? This question gets to the heart of whether the adversary is likely to engage in a deception *today.* In other words, how seriously do we need to take the likelihood of deception? Knowledge of an adversary's culture may reveal evidence of the likelihood of deception. For example, how does the fact that Russians have ingrained cultural concepts, such as *maskirovka*, increase or decrease the likelihood that their armed forces will engage in deceptive practices as a matter of military doctrine? How does what they have done in the past – such as the deceptions that paralleled Operation ANADYR, the deployment of medium-range and intermediate-range ballistic missiles in Cuba in 1962 – indicate what, when, and how they will deceive forty-four years later?

### Evidentiary Combinations

As mentioned in our discussion of the indicators and warnings example, evidence does not exist in a vacuum, one piece isolated from another. Different evidentiary elements are often coupled to one another, and inconsistencies in evidence are one of the best indicators of deception.[20] Typically, skilled adversaries know better than to concoct self-contradicting

[20] Whaley and Busby, "Detecting Deception," 193.

evidence. With this knowledge, contradictory hypotheses can be eliminated, again reducing by multiplicative factors the number of problems to be considered.

## DENIAL AND DECEPTION IN CUBA, A CASE STUDY[21]

### The Deployment of Missiles in Cuba

During the summer of 1962, analysts at the Central Intelligence Agency (CIA) and the newly formed Defense Intelligence Agency (DIA) received a spate of potentially alarming reports about Russians being seen in Cuba. The reports, however, were only part of a stream of similar, "farfetched tales of African troops with rings in their noses, lurking Mongolians, and even Chinese troops" on the island.[22] Most or all of these reports were discounted by analysts who were inured to spurious reports of Soviet equipment secreted away in caves.[23]

James Hansen – who worked in both the CIA and DIA – posits that the U.S. Intelligence and Policy Communities were the victims of a concerted Soviet campaign of denial and deception that masked the deployment of Soviet forces and missiles into Cuba.[24] The deception campaign included "accurate information about the deployment [leaked] so as to mask it."[25] As Raymond Garthoff relates, "there were literally thousands of reports of missiles in Cuba in the period *before* any missiles were actually brought there."[26]

---

[21] An expanded version of this case study is included in Moore, *Critical Thinking.*

[22] James H. Hansen, "Soviet Deception in the Cuban Missile Crisis," *Studies in Intelligence,* 46, no. 1 (2002), 56. Cited hereafter as Hansen, "Soviet Deception."

[23] Hansen, "Soviet Deception," 56.

[24] Hansen, "Soviet Deception," 49-58.

[25] Domingo Amuchastegui, "Cuban Intelligence and the October Crisis," in James G. Blight and David A. Welch, Eds., *Intelligence and the Cuban Missile Crisis* (London, UK: Frank Cass, 1998), 101.

[26] Raymond L. Garthoff, "US Intelligence in the Cuban Missile Crisis," in James G. Blight and David A. Welch, Eds., *Intelligence and the Cuban Missile Crisis* (London, UK: Frank Cass, 1998), 22. Emphasis in original. Cited hereafter as Garthoff, "US Intelligence."

Indeed, the Soviets were able to deploy more than the offensive nuclear missiles that became the centerpiece of the subsequent crisis with the United States. While U.S. analysts and policymakers knew of the conventional weapons buildup, they were blind to the presence of SS-4 Medium Range Ballistic Missiles (MRBM) and SS-5 Intermediate Range Ballistic Missiles prior to the U-2 overflights of 14 and 15 October. Additionally, they never discovered the presence of approximately 100 tactical nuclear weapons deployed on the island.[27] There is contradictory evidence whether U.S. intelligence also *underestimated* the number of Soviet troops deployed to Cuba. Garthoff reports that one CIA unit concluded there were between 45,000 and 50,000 Soviet troops in Cuba (the actual number was about 42,000) but that the official estimate was between 4,500 and 5,000 prior to the crisis.[28]

The Soviet campaign of denial and deception took advantage of American points of view about the likelihood of Soviet weapons being located in Cuba. As Robert Jervis makes clear:

> The U.S. did not expect the Russians to put missiles into Cuba or Japan to attack Pearl Harbor because American officials knew that the U.S. would thwart these measures if they were taken. These judgments were correct, but because other countries saw the world and the U.S. less accurately, the American predictions were inaccurate.[29]

It could have been worse. As Gil Merom writes, the Soviets might have *completed* the bases and "threatened major U.S. cities with extinction."[30]

---

[27] Garthoff, "US Intelligence," 29.

[28] Garthoff, "US Intelligence," 28, 58. The number of Soviet troops in Cuba eventually increased to about 22,000, calculated in early 1963. This number still fell far short of the total number of Soviet troops deployed on the island.

[29] Robert Jervis, *System Effects: Complexity in Political and Social Life* (Princeton, NJ: Princeton University Press, 1997), 45. Jervis draws on the work of Klaus Knorr. See Klaus Knorr, "Failures in National Intelligence Estimates: The Case of the Cuban Missiles," *World Politics,* 16 (April 1964): 455-67.

[30] Gil Merom, "The 1962 Cuban Intelligence Estimate: A Methodological Perspective," *Intelligence and National Security,* 14, no. 3 (Autumn 1999), 49. Cited hereafter as Merom, "Estimate."

It should be noted that the U.S. Intelligence Community was not blind to the possibility that the Soviets might conduct a military buildup in Cuba. In fact, there were two theories being debated about such a buildup: One, that the Soviets would deploy *defensive* weapons, and the other, that they would deploy *offensive* weapons. Senior analysts in the Intelligence Community held the former theory while John McCone, then Director of Central Intelligence, favored the latter. The defensive weapons theory predominated.[31]

The Soviets took advantage of the American beliefs and faulty reasoning. Capitalizing on the idea that it is easier to lead a target astray than to try to change his mind, they successfully placed the nuclear missiles in Cuba.[32] Heuer observes:

> [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 compromise their efforts.[33]

Roberta Wohlstetter commented about the crisis in retrospect, "We would like to know not only how we felt, but what we did and what we might have done, and in particular what we knew or what we could have known."[34] Wohlstetter's musings lead to a key question for analysts: How could this successful deception campaign have been thwarted?

Simply looking at additional evidence is sometimes promoted as a means of detecting denial and deception by adversaries. In the Cuban case, however, analysts had already processed

---

[31] Merom, "Estimate," 58.

[32] Richards J. Heuer, Jr., "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly* 25, no. 2 (June 1981), 200. Cited hereafter as Heuer, "Strategic Deception." It is interesting to speculate whether the Soviets had a feedback channel that informed them of the predominant theory.

[33] Heuer, "Strategic Deception," 200.

[34] Roberta Wohlstetter, "Cuba and Pearl Harbor: Hindsight and Foresight," *Foreign Affairs,* 46, no. 3 (July 1965), 691. Cited hereafter as Wohlstetter, "Cuba."

a superabundance of evidence. Wohlstetter suggests that such riches can be "embarrassing."[35] This is because, even as "signals" point

> to the action or to an adversary's intention to undertake it, "noise" or a background of irrelevant or inconsistent signals, [and] signs pointing in the wrong directions…tend always to obscure the signs pointing the right way.[36]

In the Cuban case, HUMINT assets overwhelmed analysts' abilities to distinguish signals from noise. Heuer and Hansen agree that, once "locked in," analysts resisted changing their minds. More evidence alone fails to change an analyst's mind because "[new] information is assimilated to existing images" – a common means by which people cope with the combinatorial explosion of evidence, inferences, and hypotheses.[37] As Gil Merom notes, "information that was inconsistent with the prevailing conservative theory was not considered as alarming and necessitating revision, but rather was 'rehabilitated' and rendered 'harmless' on the basis of *ad hoc* statements."[38] Instead, inductive reasoning generally led analysts to "prove" their theory and subsequently to adhere to it "*until it was proven wrong* by conclusive hard evidence," evidence provided by the U-2 photos.[39]

What tipped off the overhead surveillance were two HUMINT reports of "a Soviet truck convoy that appeared to be towing ballistic missiles toward the San Cristobal area."[40] That these reports were taken seriously is one of the curious serendipities that occur from time to time in intelligence analysis (and other research-based domains). It remains a mystery what prompted

---

[35] Wohlstetter, "Cuba," 691.

[36] Wohlstetter, "Cuba," 691.

[37] Heuer, *Psychology,* 10-11.

[38] Merom, "Estimate," 69.

[39] Merom, "Estimate," 69. (Emphasis in original.)

[40] Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis,* 2nd Edition (New York, NY: Longman, 1999), 220. Cited hereafter as Allison and Zelikow, *Essence of Decision.* Raymond Garthoff also notes this fact. See Garthoff, "US Intelligence," 23.

the CIA and DIA analysts to take these reports seriously while earlier reports had been dismissed. Garthoff asserts that it was new information taken in context with the observed "pattern of SA-2 surface-to-air missile sites in Western Cuba" that led to the tasking of the U-2 flight on 14 October.[41]

**Analysis of the Deception**

The question on the minds of the CIA analysts and their policymaking customers was: Why are the Russians in Cuba, and what are they doing? For purposes of this counterfactual analysis, we must ask another question: Given their point of view, could analysts have known they were being deceived? Reviewing the evidence, an analyst would be faced with significant uncertainty as to the deployment of either missiles or troops. Further, Soviet doctrine and the extremely high volume of reports coming out of Cuba – "dazzling" in the language of J. Barton Bowyer[42] – would give analysts good reason to hypothesize deception. But if the Soviets were conducting a deception, then how? What type of lie could the Russians be telling?

To answer these questions, we focus on the potential falsification of two key pieces of evidence in the problem: the presence of offensive Soviet strategic missiles and the presence of Soviet troops. The Soviets had both the means and opportunity to falsify the presence of both missiles and troops, and past operational practices indicated that they were very likely to employ deception, but the analysts of the day apparently were not predisposed to consider this possibility.

[41] Garthoff, "US Intelligence," 23.

[42] J. Barton, Bowyer, *Cheating (*New York, NY: St. Martins Press, 1980), 55.

Given that there was a great deal of uncertainty regarding the presence of strategic missiles, and the number of Soviet troops in Cuba, the evidentiary states for both should have included "present" and "absent." In either case, the perceived presence or absence could be deceptive, meaning the most reasonable interpretation of the evidence would be misleading. Enumerating the possible states of deception would have given the analyst insight as to, not only what types of deception he should consider, but also the possible motives underlying the deception.

| | Evidentiary Hypotheses | |
|---|---|---|
| | **Missile Deployment** | **Troop Deployment** |
| 1 | Present (deception) | Present (deception) |
| 2 | Present (no deception) | Present (deception) |
| 3 | Absent (deception) | Present (deception) |
| 4 | Absent (no deception) | Present (deception) |
| 5 | Present (deception) | Present (no deception) |
| 6 | Present (no deception) | Present (no deception) |
| 7 | Absent (deception) | Present (no deception) |
| 8 | Absent (no deception) | Present (no deception) |
| 9 | Present (deception) | Absent (deception) |
| 10 | Present (no deception) | Absent (deception) |
| 11 | Absent (deception) | Absent (deception) |
| 12 | Absent (no deception) | Absent (deception) |
| 13 | Present (deception) | Absent (no deception) |
| 14 | Present (no deception) | Absent (no deception) |
| 15 | Absent (deception) | Absent (no deception) |
| 16 | Absent (no deception) | Absent (no deception) |

**Table 3: Possible Deceptions (Evidentiary Hypotheses) for Deployment of Troops and Strategic Weapons in Cuba in 1962.**

To demonstrate, for both missile and troop deployments, we will construct four evidentiary states:

1. Present, but we are deceived to think that it is absent
2. Present, and we are not being deceived.
3. Absent, but we are deceived to think that it is present.
4. Absent, and we are not being deceived.

Our two evidentiary elements, each with four possible states, yield a total of $4^2 = 16$ evidentiary hypotheses, each of which must be considered in turn. Table 3 summarizes the possible evidentiary hypotheses.

In principle, each of these evidentiary hypotheses should have been considered individually, whereupon new hypotheses could be generated and compared against the other (presumably non-deceptive) evidence. We begin by ruling out those evidentiary hypotheses that contain a perceived presence of strategic missiles combined with a perceived absence of Soviet troops. Such a combination – strategic weapons unsupported by ground forces – clearly is unrealistic. On these grounds, we discard evidentiary hypotheses 2, 3, 14, and 15. This leaves twelve evidentiary hypotheses to consider. We will only consider one of them here, in the interest of brevity:

*Evidentiary Hypothesis 1*: In this case, we are being deceived that there are neither strategic weapons nor troops in Cuba. We construct an ACH table, listing, among other items, these two assumptions as evidence: First, in the event of attack, the United States would still have had a devastating retaliatory strike capability due to deployments of strategic weapons in Turkey, and second, the United States had the capability to interdict shipments of nuclear missiles to Cuba if it became aware that they were being deployed.

Based on the evidence, we construct two hypotheses: That the Soviets are planning a surprise attack on the continental United States using nuclear weapons, and that the Soviets are deploying the missiles to obtain a better strategic negotiating position. We score the hypotheses with a '+' for supporting evidence, '-' for disconfirmatory evidence, and '0' for indeterminate evidence, with the number of pluses and minuses representing the strength of the evidence. The results are given in table 4. The most likely hypotheses, given that we are being deceived about both troop and missile deployment, is that the Soviets are attempting to obtain strategic leverage over the United States. They are less likely to attempt a pre-emptive strike due to U.S. retaliatory capabilities.

| Evidence | H1: Surprise Attack | H2: Establishing a Strong Bargaining Position |
|---|---|---|
| Hidden Deployment of Strategic Weapons | + + + | + + + |
| Hidden Deployment of Support Troops | + + + | + + + |
| Strong U.S. Capability for retaliatory strike. | - - | + + |
| Strong U.S. Capability for U.S. to interdict deployment | 0 | + + |

**Table 4: ACH Table for Evidentiary Hypothesis 1**

There are 11 other such ACH tables, each with their own hypotheses that should be constructed in order to fully consider the possibilities and implications of Soviet deception operations in Cuba. This process is the key to generating specific and novel deception hypotheses.

## SO WHAT?

We have argued that one thing that makes denial and deception so difficult to detect is the tremendous variety of channels and means. Considering all possible combinations of more than a few elements is well beyond unaided human cognitive capacity. Although talented analysts can and have captured the subtleties of denial and deception problems, the great potential for committing critical errors necessitates techniques for exploring these complex deception spaces. Even problems that are conceptually simple to describe can spawn deception-induced combinatorial explosions, a dangerous trap for analysts that can lead to strategic surprise, as it did with Cuba in 1962. Short descriptions and explosive combinations make denial and deception problems good candidates for intervention with automated methods – input time is relatively short, and the hard work of enumerating combinations is exactly the strength of computational approaches. Sadly, the analysts of 1962 had neither appropriate methods, technology, nor experts in their application, to help them detect the Soviet denial and deception

or even understand the Soviets' intentions and actions. By contrast, contemporary analysts *do* have such aids. The means and experts in structured, methodological intelligence sensemaking are available and can be integrated into teams of analyst working hard problems. Technology to manage the ensuing collaboration has been proposed.

## CONCLUSION

In this paper, we have developed a procedure for characterizing the complexity of denial and deception problems by counting the number of lies that are possible given the evidence and the characteristics of the adversary. We find that that introducing deception into a problem enormously complicates analysis. Even problems that are easily described can have extremely large deception spaces that quickly outstrip human cognitive capability. We have presented a simple method, based on Heuer's Analysis of Competing Hypotheses and well known features of denial and deception, that systematically explores the deception space, considering each possible deception and either eliminating it or developing causal hypotheses that might explain it.

By quantifying the complexity of denial and deception problems, analysts and decision makers can gauge how difficult their problems are. This will help them calibrate both the level of effort they expend on these problems and the confidence with which they make assessments. These metrics can also help the community determine the level of effort that should be put into research to address these and related problems – if the typical deception problem contains 100 billion possible deceptions, it will require a different approach from problems that must onl consider several hundred alternatives.

## ABOUT THE AUTHORS

DAVID T. MOORE is a career senior intelligence analyst and technical director at the National Security Agency. He is an adjunct faculty member of the National Cryptologic School and has taught at the Joint Military Intelligence College, Washington, DC, and at Trinity University, Washington, DC. He holds a Master of Science of Strategic Intelligence from the Joint Military Intelligence College. He is the author of *Critical Thinking and Intelligence* (Washington, DC: co-author of "Intelligence Analysis, Does NSA Have What it Takes," *Cryptologic Quarterly,* 20, nos. 1/2 (Summer/Fall 2001); "Core Competencies for Intelligence Analysis at the National Security Agency," in *Bringing Intelligence About: Practitioners Reflect on Best Practices,* Russell Swenson, ed. (2004); "Evaluating Intelligence: A Competency-Based Approach," in the *International Journal of Intelligence and CounterIntelligence*, 19, no. 2 (Summer 2005); and author of "Species of Competencies for Intelligence Analysis," *Defense Intelligence Journal,* 11, no. 2 (Summer 2002), and *American Intelligence Journal*, 23 (2005) (expanded version of original article). Over two decades of intelligence assignments, both in the Washington DC area and abroad have provided Mr. Moore expertise in the areas of intelligence analysis competencies, methods, and standards. This paper builds on six years of advocacy for, and mentoring of, best practices in intelligence.

WILLIAM N. REYNOLDS is President and Chief Science Officer of Least Squares Software Inc. Dr. Reynolds holds a Ph.D. in theoretical physics from the University of California, San Diego. Dr. Reynolds has been working in complex systems research for over 15 years and studying intelligence problems for the past five years. His research focuses on the implications complexity science brings to real-world decision-making and analysis. His studies have included topics as diverse as the behavior of slime mold colonies and the complex dynamics of stock markets and battlefields. He is the designer and lead developer of Landscape/Decision, a tool for supporting analysts trying to understand complex decision processes and Policrash, a general-purpose system for agent-based modeling.