Hiding in Plain Sight: Denial, Deception, and the Non-State Actor

Wirtz, James J.

http://hdl.handle.net/10945/43328
Hiding in Plain Sight: Denial, Deception, and the Non-State Actor

James J. Wirtz

History is replete with examples of militaries that have used denial and deception to gain victory on the battlefield. Denial withholds accurate information from an adversary, while deception puts forward misleading information that conforms to the expectations of an opponent. Recently, the advent of the information age has allowed small non-state actors, particularly terrorist organizations, to engage in denial and deception—with often devastating results. Unfortunately, states have been slow to adjust, which has allowed terrorist groups to carry out their attacks while hiding in plain sight of their targets.

Carl von Clausewitz, the famous military philosopher, never put much stock in denial and deception. “Denial,” in this case, refers to practices that are intended to prevent accurate information from reaching opponents. “Deception,” on the other hand, involves deliberate activities that are intended to provide opponents with misleading information, causing them to perceive reality according to the deceiver’s intentions. For Clausewitz, most attempts to deceive opponents were usually not worth the effort. In his day and age, such tactics were often too costly, and had the effect of diverting resources that were crucial to the main military attack. While much has changed since this Prussian philosopher offered his commentary on early nineteenth century European warfare, today it remains a matter of debate as to whether the information revolution has enhanced or has limited the prospects for contemporary denial and deception.

Among military historians and those who study security and intelligence affairs, there exists virtually unanimous agreement that the information revolution has empowered individuals at the expense of governments and bureaucracies, giving everyday people the communication, organizational, and analytical capabilities that were only possessed by national governments a few short decades ago. But there is less recognition of a new recent twist in the practice of denial and deception. Given that information about global events has become ubiquitous, it is becoming difficult for states, despite their enormous resources, to hide significant developments from the outside world. At the same time, it is becoming increasingly easy...
for individuals or small groups with limited resources and nefarious intentions simply to “hide in plain sight” from law enforcement and intelligence agencies. In other words, it might be possible that the information revolution has empowered the individual vis-à-vis the state when it comes to denial and deception, giving terrorists and criminal organizations new abilities to blend in with civil society. The practice of denial and deception has thus become the crucial enabler for contemporary terrorist cells, especially those operating within major urban areas.

To explore this important facet of denial and deception, this article will briefly describe what is meant by the terms “denial” and “deception” and why each term is important to both world politics and military combat. This article will then explain how terrorist cells and criminal organizations use denial and deception, while at the same time discussing the ways in which such organizations can be hampered in their use of such techniques. (For example, because terrorist organizations or spontaneous cells have limited resources, they tend to practice denial rather than deception when it comes to preventing their detection by state authorities.) The article will then briefly explore new ways in which the information revolution might, in the end, aid governments and other traditional state actors by making it increasingly difficult for terrorists to ‘hide in plain sight.’

Denial and Deception

Denial and deception are activities that work together to misdirect or mislead opponents about a deceiver’s presence, activities, or intentions. They create the possibility that one’s whole diplomatic or strategic outlook might be based on false assumptions or incomplete assessments of reality, and that these erroneous assessments are the product of a sustained campaign carried out by one’s opponents. If the developing situation is a bit too simple, or if potentially threatening events seem to be unfolding in a particularly benign way, or if innocent explanations for unusual events seem to clutter reports from the field, or even highly classified intelligence estimates, then prudent policymakers and intelligence analysts should begin to suspect that they are falling victim to denial and deception. When it comes to denial and deception, policymakers and analysts alike should operate on the principle of caveat emptor.

Denial is based on secrecy and a keen awareness of the signatures—observable phenomena related to planning, preparing, and undertaking an operation—that can tip off an opponent about what is actually about to happen. When these signatures are denied to an opponent—as they largely were by Japan in the weeks leading up to Pearl Harbor—the “noise” of innocuous events or alternative erroneous explanations can drown out the accurate “signals” that would otherwise indicate that an event is about to transpire. In other words, opponents cannot determine what is about to
Denial, Deception, and the Non-State Actor

Denial, Deception, anD the non-State actor
transpire because they do not possess the information needed to develop an accurate and timely estimate of what is happening. Of course, efforts at denial vary in quality. Nevertheless, denial is a common practice in international relations and military operations. Governments and militaries rarely make public their fundamental objectives, or even their own estimates of their strengths and weaknesses, in a political or military contest. Denial is a constant when it comes to diplomacy and strategy: policymakers, strategists, and intelligence analysts can safely assume that their opponent is withholding information.

Deception can take a myriad of forms and is limited only by the creativity and guile of the deception planner. Bogus stories published by legitimate media outlets, fake documents and plans, and false electronic signals or communications have all been used to give an opponent an inaccurate sense of what is about to transpire. In contrast to denial, which generally requires only security or self-awareness when it comes to the ‘signatures’ (observable electronic, seismic, social, or biometric evidence) generated by various activities, deception can be costly because it can require the expenditure of resources to create a convincing false front. For example, the Battle for Khe Sanh, which distracted U.S. commanders from the looming threat posed by the Viet Cong to the cities of South Vietnam on the eve of the 1968 Tet Offensive, involved several divisions of the People’s Army of Vietnam. In this case, deception involved activities that were so costly to the communist war effort that observers still debate which action was, in fact, the main avenue of attack and which initiative was the effort at deception.

Efforts at denial and deception rely on several factors for their success. Practitioners of denial and deception need accurate information not only about the way their opponents collect and analyze information, but also about their opponent’s beliefs, plans, and expectations. In other words, denial and deception require good intelligence about the opponent. Without this information, it might be impossible to control the flow of information to the opponent or provide information that will be perceived as credible or compelling. Technical virtuosity also plays a part in denial and deception, in the sense that the deceiver must employ artistry to attract the target’s attention to the misleading information without raising suspicion. Denial and deception work because they play off an opponent’s need for information, while heightening the opponent’s sensitivity to the information that the deceiver intends to provide, which often includes a message that the opponent also happens to want to hear. According to Donald Daniel, “denial plays against an adversary’s eagerness while deception plays to it. That is, while the denier conceals information from the opponent, the deceiver happily provides him with false clues.”

The opponent is desperate to learn about the deceiver’s intentions, but the opponent has to discover the planted information “naturally” if the deception is to take a firm hold within their intelligence community.
Although the practice of denial and deception in theory sounds highly demanding, in practice it can work splendidly, especially if the deceiver can channel the flow of information in a way that supports the target’s preferred conception of reality. In the early 1970s, for example, Israeli officials based their defense policy on three assumptions that came to be described as “the concept”: Egypt would be at the center of any Arab coalition against Israel, Egypt would not launch a significant attack without a strong prospect of victory, and, unless Egypt destroyed the Israeli Air Force, an Arab victory would not be possible. Israeli officials also believed that their intelligence agencies would provide a “war warning,” which would allow them to mobilize their reserves or even launch a pre-emptive attack—actions that would produce an Arab defeat. The “concept” held sway, despite some unusually compelling contradictory evidence and an Egyptian denial and deception campaign that was itself amateurish.

Even though Israel was equipped with an enormous amount of intelligence that should have raised flags—including actual Syrian and Egyptian war plans, reconnaissance photographs showing unprecedented force deployments along the Suez Canal and Golan Heights, a warning from a credible and trusted spy from the inner circle of Egyptian government, information that Soviet personnel and dependents were high-tailing it out of Cairo and Damascus, and signals intelligence suggesting that their opponents were about to strike—the Israelis never managed to act as if they were about to be hit by an all-out Arab assault. As a result, the outbreak of the 1973 Yom Kippur War was marked by one of the greatest intelligence-command failures in military history. Despite the availability of accurate, detailed, and compelling indications of what was about to transpire, Israeli analysts and officials could not overcome their existing conception of reality in order to act in time to head off disaster.

The practice of denial and deception is effective because it addresses the expectations of the target. Conventional wisdom, based on estimates made by Barton Whaley nearly forty years ago, continues to support the notion that denial and deception is effective about ninety per cent of the time it is attempted. Once the deceiver understands the target’s biases, it is very difficult for the target to escape the trap. In fact, John Ferris, a leading historian of twentieth century intelligence, has noted that only four qualities allow the target to escape effective denial and deception: “superior power and initiative; intelligence of outstanding quality or else so poor that it cannot pick up misleading signals, [and] an inability or unwillingness to act on any knowledge, true or false.” Ironically, two of the qualities identified by Ferris can be characterized as sheer incompetence, while superior performance is often in short supply. Given the fact that most governments fall somewhere in the middle of this range of capabilities, it is not surprising that efforts at denial and deception are often effective.

Hiding in Plain Sight

Most of the literature, history, and practice of denial and deception involve state actors or military organizations that possess the resources required to
(1) deny an opponent accurate information about their true intentions and
(2) create a second misleading “image” that largely conforms to the expecta-
tions of the opponent. This is no small task. It requires a large team of
analysts and operatives, as well as an effort to deny the opponent accurate
information and signatures related to one’s true intentions. It also requires
an understanding of the preferences and expectations of the target, and an
effective way to transmit information to the opponent in an attractive and
compelling manner. Traditional denial and deception uses denial to set
the stage for deception. In other words, denial is used to whet the target’s
appetite for information, while deception schemes are used to satisfy the
need for information with stories that fit the needs of the deceiver. For many
non-state actors—terror cells or even super-empowered individuals who
would like to use violence to achieve their own political objectives—engag-
ing in traditional denial and deception activities will likely be beyond their
capabilities. They simply lack the resources to generate and then offer an
alternative reality to feed to the target. Yet, other forms of denial and de-
ception are not beyond their reach—especially if they reverse the traditional
balance between denial and deception.

Unlike states or large military formations, small terrorist cells or individu-
als face a less daunting challenge when it comes to denial. In contrast to
an armored corps moving across the desert, for example, a terrorist cell does
not generate a dust, heat, electromagnetic, or radar signature that can be
detected from hundreds of miles away. The signature created by a terrorist
group preparing to launch an attack is relatively weak and diffuse, making
it difficult to detect against the noise generated by the normal everyday
activities of the communities in its midst. The challenge is more daunting
for deception, however, because small cells lack the human or material re-
sources needed to undertake significant deception activities. They cannot
launch duplicate, redundant efforts to mislead opponents. Furthermore,
increasing the size of their organizations or the scope of their operations is
unlikely to improve their prospects for success because it tends to increase
the risk of detection. The more people involved in an operation, the greater
the risk that someone will go to the police, speak to untrustworthy third
parties, or risk detection or arrest following some minor run-in with local
law enforcement.

Because of their weakness vis-à-vis the state, terrorist cells or individu-
als must incorporate denial as a fundamental principle of their operations. Terrorists rely on denial for their very existence. It becomes a strategic asset
for terrorists because without it, they cannot hope to exist, especially given
the large asymmetry between their resources and the resources of local law
enforcement and the state. Denial involves the tightest operational security,
coupled with a rudimentary strategy of deception. For terrorists, “decep-
tion” involves maintaining a normal routine to the greatest extent possible
as a cover for the nefarious plans and operations undertaken by the cell.
This technique can be referred to as “hiding in plain sight.” In fact, deception
is based on an understanding of what the target of deception believes
to be normal, and the degree to which the target of deception can assimilate
anomalies before responding. Deception is therefore not based on feeding the target erroneous information, but on making one’s actions comply with the expectations of the target.

Terrorists who hide in plain sight use their normalcy to appeal to the widely shared belief that what appears to be normal actually is normal in its entirety. In other words, because the image they present to the outside world fails to match a pre-existing notion of what (or who) constitutes a “threat,” terrorists are largely left alone, despite some anomalies in their behavior. Writing about the cell that bombed the World Trade Center in 1993, Bell notes, “no one in authority noticed the zealous sermons in the obscure storefront mosques or imagined that the wars of the Middle East might come to Manhattan. This lack of official concern persisted despite the visibility of militant Islam: the kidnappings and bombs of Beirut, the warnings in Algeria and Egypt and the threats of violence directed against the U.S. Homeland.” Although analysts and a few local authorities knew about Sheikh Omar Abdel Rahman and the message he was delivering to his followers, no one took the blind cleric seriously. “His cover,” according to Bell, “was that no American authority could imagine him as dangerous. He appeared to be an itinerant migrant who preached in seedy rented rooms.”

The persistent blindness of U.S. elected officials, law enforcement personnel, and intelligence analysts about the true nature of the al-Qaeda threat allowed members of the group to hide in plain sight in the months leading up to September 11, 2001. Despite the fact that Osama bin-Laden made little effort to hide his ambition of attacking U.S. citizens and interests wherever he could find them, or that al-Qaeda had established a track record of attacking U.S. interests across the Middle East and Africa, or that various law enforcement officials and intelligence analysts were sounding alarms about specific events, the terror cells in the United States operated virtually unimpeded prior to the September 11 tragedy. Given this track record, it is hard to escape the conclusion that a little denial can go a long way, especially in the information age.

**Toward Counterdeception**

Unlike most observers, Barton Whaley has expressed optimism about the possibility of counterdeception, the effort to detect and defeat the denial and deception strategies used by terrorist cells. He has devised a theory of counterdeception that is particularly well suited to detecting those who are hiding in plain sight. While counterdeception is relatively simple in theory, it is more difficult to put into practice. But counterdeception sometimes does occur and could be more common in the future, especially if law enforcement officers, intelligence analysts, and elected officials recognize the principles behind the effort to detect individuals who are hiding in plain sight.

Counterdeception is based on the idea that every type of human endeavor has a large but knowable set of characteristics that must be present if it is true to form. Imitations of real activity, or ‘false fronts,’ will lack
certain key characteristics, or will have extraneous characteristics added to a specific endeavor. The detection of these anomalies is the key element in discovering denial and deception because, according to Whaley, “every real thing is always, necessarily, completely congruent with all its characteristics.” Moreover, not all anomalies have to be detected before an analyst can uncover denial and deception. The detection of one anomaly is enough to raise the possibility that something is fundamentally amiss. Whaley is not alone in offering what amounts to a scientific method for uncovering denial and deception. Richards Heuer has developed a similar technique—an “analysis of competing hypotheses”—to validate the theoretical assumptions underlying intelligence estimates. Heuer suggests that analysts can overcome cognitive biases and organizational preferences by comparing competing hypotheses and rejecting explanations that fail to account for key elements in a developing situation. Anomalies are evidence that something is amiss; they are the Achilles heels of deception planners.

Two factors, however, complicate this simple observation about what is needed to detect denial and deception. The first is the problem of measurement error. In other words, not every observation of reality is accurate, and errors can be read as either false positives or false negatives. No simple solution is available to overcome the problem of measurement error, in the sense that it is difficult to define and detect significant social anomalies in the first place. An analytical or political decision must be made to assess what sort of thresholds should be used to trigger further investigation once an anomaly is detected. The second problem involves the decision to respond to an anomaly, which again is a matter of political or analytical judgment. As Bell notes, some officials recognized that Sheikh Omar Abdel Rahman and his followers did not appear to be typical residents of Jersey City, but this awareness was not translated into effective action. The decision to respond to anomalies might be made on the basis of the principles of risk management: anomalies involving certain type of groups or certain types of targets might be selected for additional investigation by police officers or intelligence analysts. In that sense, the detection of anomalies might not be the end of an investigation, but a signal to refocus information collection and analytical efforts.

The information revolution makes it easier to hide in plain sight by facilitating the movement of ideas, people, and resources across international boundaries because the movement of outsiders, as well as ideas and resources, are now an everyday occurrence. But the information revolution also might provide law enforcement officials and intelligence analysts with additional information needed to separate legitimate actors from those just masquerading as average people. Everyday life is increasingly digitized as people make full use of the services and resources made possible by the information revolution. This activity leaves a digital record in a myriad of unexpected ways and places. Templates and algorithms already exist that can detect anomalies in normal activities, such as the loss or theft of credit cards, unauthorized entry into secure facilities, or even increasingly routine airline baggage delays. There is no reason to subject anyone to this level
of scrutiny on a daily basis, but it might be possible to explore the digital reality behind individuals or groups that somehow manage to attract the attention of intelligence and law enforcement officials. The requirement to fashion a convincing “electronic history” might be beyond the ability of small groups or terrorist cells. The absence of this history—living off the grid—in some settings might be cause for suspicion itself. In fact, the U.S. intelligence community already has recognized the difficulty in manufacturing a credible electronic history to match the cover story supplied to its own clandestine operatives.19

Conclusion

Admittedly, if taken to their logical conclusions, the ideas presented here are downright Orwellian. But this is not a call to monitor people everywhere in real time to make sure that their “digital” lives roughly corresponds to some template based on their geographic location, employment and family history, or their socioeconomic status. Instead, the article offers a tool that law enforcement can use to evaluate terrorist suspects quickly. It describes why terrorists need to hide in plain sight while undertaking their operations, and how their modus operandi differs from the more traditional practice of denial and deception. It also identifies a critical weakness in their tradecraft that might be beyond their ability to remedy quickly with available resources. In other words, once individuals come to the attention of law enforcement officials in the course of some investigation, their electronic bona fides could be matched against their stories. Anomalies would not be evidence of guilt, but prudence would suggest that they might require further investigation.

Recent history has shown that terror cells have lived quietly in the United States, trying to give the appearance of normalcy until they can carry out their attacks. History also has shown that law enforcement and intelligence officials have not performed well in responding to anomalous behavior. Armed with rudimentary tradecraft, the September 11 hijackers were able to hide in plain sight while only attracting a modest amount of attention. They did reasonably well mimicking the behavior of average college students, who often lack visible means of support and have been known to spend more time lounging about or in bars than studying. But when cell members showed interest in learning how to take off and fly, but not land, commercial airliners, they were not acting as ‘normal’ student pilots. At that point they had blown their cover. The September 11 hijackers never tipped their hand in terms of their plans, but they did fail to preserve their image as run-of-the-mill student pilots. The detection of anomalies might not be the final solution when it comes to discovering denial and deception or detecting terrorists, but it is a good place to start.

Notes

1Because deception requires significant forces to be convincing, by definition it implies that these forces will not be available to support the main attack. Clausewitz judged that
efforts beyond simple operational security—the attempt to minimize the opponent’s ability to gather information about plans, troop movements, or the combat readiness of various units—were probably not worth the effort. Denial and deception might pay some dividends, but in all likelihood, these benefits would be modest compared to the resources required to create an effective diversion.


4 U.S. intelligence analysts, for example, became suspicious when they discovered large-hatched ships involved in the Baltic lumber trade moving from Soviet ports to Cuba in the late summer of 1962. The fact that these ships were riding high in the water and were being unloaded at night further raised the possibility that they were delivering something other than wood to Cuban ports. The fact that the ships’ cargo was not visible to U.S. intelligence analysts did little to allay their suspicions about what the Soviets were up to in Cuba.


8 Israeli intelligence determined that the “exercise” that the Egyptians apparently intended to use as a cover for their mobilization was, in fact, not taking place.


13 Ibid., 147.

14 Ibid.


17 Ibid.


19 According to Jose Rodriguez, the outgoing head of the U.S. National Clandestine Service, the widespread availability of public, real estate, and corporate data bases has made creating convincing cover stories for clandestine agents “hard as nails,” see Richard Willing “How U.S. Spies are Recruited, Trained is Morphing,” *USA Today* October, 1, 2007, p. 10A.