Things Are Not What They Seem – Defining the Threats of Surprise, Denial and Deception

British writer Aldous Huxley may have unwittingly defined the fundamental challenge of national security when he said, "There are things known and there are things unknown, and in between are the doors of perception." The ability to distinguish between perception and reality is often the difference between being prepared and being a target. Likewise, the ability to distort perception can be a powerful offensive weapon. Could there ever be another 9/11? How far has Iran's nuclear program developed? Is North Korea launching a satellite rocket or testing a ballistic missile? The answers to questions like these begin with understanding how perception is altered itself.

Surprise is the perception that something is happening contrary to expectations. During World War II, military strategists had played out the possibility of a Japanese attack on American soil. The greater surprise about the Pearl Harbor attacks was that the U.S believed that Japan would attack the Philippines first and would also be incapable of mounting concurrent naval operations. By exploiting the perception between what is possible and what is probable, surprise leverages the effects of an adversary's unpreparedness and allows for success well out of proportion to the effort expended. "It is a powerful but temporary combat multiplier. It is not essential to take the adversary or enemy completely unaware; it is only necessary that he become aware too late to react effectively."[1]

A 2009 Defense Science Board study found that surprises that had occurred during the past century fell into two major categories. 'Known' surprises were "those few that the United States should have known were coming, but for which it did not adequately prepare," for which "the effects are potentially catastrophic; and dealing with them is difficult, costly, and sometimes counter-cultural." Included in this category were space, cyber, and nuclear surprises. The other category were 'surprising' surprises "that the nation might have known about or at least anticipated, but which were buried among hundreds or thousands of other possibilities," all of which the nation cannot afford to pursue.[2]

The effectiveness of surprises is inherently limited. First, the initiator must exploit the opportunity to fully benefit from it, but also understand that it does not determine the final outcome. Second, "strategic surprise is increasingly difficult in the information age when around-the-clock news on troop movements and the political process is available to anyone with a satellite dish or Internet connection."[3] Nevertheless, surprise remains a viable tactic because, "the possibility of such surprise at any time lies in the conditions of human perception and stems from uncertainties so basic that they are not likely to be eliminated, though they might be reduced."[4]

Denial prevents accessibility and accuracy of perception. In the United States, it was "Loose lips sink ships." In England, it was "Keep mum – she's not so dumb." These World War II slogans advised servicemen and citizens from carelessly talking about secure information that the enemy might find useful. If knowledge is power, then preventing an adversary's access to knowledge is paramount. "'Denial' refers to the attempt to block all information channels by which an adversary could learn some

[1] U.S. Army Field Manual No.1, June 2005, http://www.army.mil/fm1/PDF/FM%201.zip.
[2] "Report of the Defense Science Board 2008 Summer Study on Capability Surprise, Vol. 1 Main Report," September 2009, http://www.acq.osd.mil/dsb/reports/ADA506396.pdf.
[3] Lt. Cmdr. Christopher E. Van Avery, "12 New Principles of Warfare," *Armed Forces Journal*, July 2007, http://www.armedforcesjournal.com/2007/07/2807407.
[4] Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Palo Alto: Stanford University Press, 1962).

truth (e.g., about a military development program, a policy, a course of action, etc.) thus preventing him from reacting in a timely manner."[5]

Denial is proactive activity. In today's national security environment, it is achieved through operations security (OPSEC) processes that identify "the critical information of military plans, operations, and supporting activities and the indicators that can reveal it, and then develops measures to eliminate, reduce, or conceal those indicators."[6] The safeguarding of state secrets, classified information, and security programs, from foreign intelligence collection, has been made both easier and more challenging by the evolution of communications and information technology. As a result, cyber space has become the primary battlefield in the protection and retrieval of sensitive information from government networks as well as from their private sector partners. The effectiveness of securing information is now ironically dependent on the perception of information security itself.

Deception distorts the perception of reality. The success of the Greeks' Trojan horse ruse wasn't simply the soldiers hiding in the wooden structure; it was also making the Trojans believe they had sailed away in defeat, causing the Trojans to pull the horse into their city as a victory trophy. Deception "refers to the effort to cause an adversary to believe something that is not true, to believe a 'cover story' rather than the truth, with the goal of leading him to react in a way that serves one's own interests, rather than his."[7]

Unlike denial, deception is an intentional manipulation of information to gain advantage over an adversary. "The U.S. military community traditionally recognizes three levels of deception – based on the nature of the intent. *Strategic Deception* intends to 'disguise basic objectives, intentions, strategies and capabilities.' This contrasts with *operational deception*, which confuses an adversary regarding 'a specific operation or action you are preparing to conduct.' And, last, but not least, in the American doctrines, there is *tactical deception*. This is intended to mislead 'others while they are *actively involved* in competition with you, your interests, or your forces.'" [8] Another advantage of deception is that it doesn't necessitate the use of force and may deter the use of force altogether.

Within national security, deception is not only about the protection of power, but also the projection of power. For example, China's perspective on "strategic ambiguity - - including strategic denial and deception – is a mechanism to influence the policies of foreign governments and the opinions of the general public and elites in other countries."[9] When it comes to creating the perception of strength and authority, there may be no more effective force multiplier than deception.

Surprise, denial and deception are some of the oldest – and most successful – tricks in the book. They interfere with the accurate assessment of the capabilities and intentions of nation states and threat actors, which shape national security strategies and policies. This can leave an uncomfortable gap between what is known and unknown for perception to fill. Given that perception may not always be reality, it can make uncertainty a highly effective weapon.

---

[5] Abram Shulsky, "Elements in Strategic Deception and Denial," *Trends in Organized Crime,* Vol. 6, No. 1, pgs. 17-31, http://www.springerlink.com/content/31jkbk568agplat7/.
[6] U.S. Army, "Army Regulation 530-1, Operations and Signal Security," April 19, 2007, http://www.fas.org/irp/doddir/army/ar530-1.pdf.
[7] Shulsky, op.cit.
[8] Joseph W. Caddell, "Deception 101 – Primer on Deception," December 2004, http://www.fas.org/irp/eprint/deception.pdf.
[9] Dr. Mark B. Schneider, "Testimony Before the U.S.-China Economic and Security Review Commission, Hearing on "Developments in China's Cyber and Nuclear Capabilities," March 26, 2012, http://www.uscc.gov/hearings/2012hearings/written_testimonies/12_3_26/schneider.pdf.