National Intelligence University

MST 664
Science and Technology Intelligence
Professor Rosin

A Review of Foundational Denial and Deception Topics

Submitted by

Alejandro F. Sosa

I verify that this submission is my own original work.
31 March 2024

Discuss the concepts of simulation and dissimulation as they relate to denial and deception. Provide examples in your response.

Simulation and dissimulation are concepts deeply entrenched in the realms of psychology, sociology, and military strategy. They represent mechanisms humans employ to navigate social interactions, particularly in contexts where concealment or manipulation of information is crucial, such as in statecraft, espionage, or military deception. Understanding these concepts can aid a planner or practitioner of denial and deception.

Simulation involves deliberately portraying a false appearance or behavior, often to convey a specific impression or achieve a desired outcome. Barton Whaley described simulation as showing a falsehood, which would be denying the adversary the ability to perceive reality[1]. It is a conscious act of presenting oneself or a situation in a manner that is different from reality. A classic World War 2 example of simulation would be the United States Army's use of a Ghost Army. The Army used a small force of around 1100 soldiers to deceive the Nazi senior leaders into believing that they were a force of over 30,000 soldiers.

The Ghost Army used visual deception by employing inflatable tanks, cannons, jeeps, trucks, and airplanes to simulate the vehicles that would be used by a much larger force. They used Sonic Deception by using recorded audio from actual infantry and armored units played through speakers to simulate the sounds of a much larger force[2]. These sounds could be heard over 15 miles away from their staging area[3]. Among many other techniques, Radio Deception was also used. The Ghost Army knew that the Nazis were intercepting Morse

---

[1] Barton Whaley, "Toward a General Theory of Deception," *Journal of Strategic Studies* 5, no. 1 (March 1, 1982): 178–92, https://doi.org/10.1080/01402398208437106.

[2] "When an Army of Artists Fooled Hitler | History & Archaeology | Smithsonian Magazine," accessed March 30, 2024, https://web.archive.org/web/20130523010707/http://www.smithsonianmag.com/history-archaeology/When-an-Army-of-Artists-Fooled-Hitler-208304561.html.

[3] "Ghost Army: The Combat Con Artists of World War II," The National WWII Museum | New Orleans, accessed March 30, 2024, https://www.nationalww2museum.org/visit/exhibits/traveling-exhibits/ghost-army-combat-con-artists-world-war-ii.

Traffic, so their signal operators would create false traffic networks and would simulate the Morse Code entry style of other operators who relayed real traffic. This traffic would include piecemeal information that indicated that their unit was preparing to mobilize for areas distinctly different from where the main Allied forces were massing, denying the nature of the true attack and getting the target to not believe something that was true.[4] The underlying motive behind this simulation is typically to influence others' perceptions or reactions. The Ghost Army's intent was to draw Nazi resources away from where the Allies were preparing to cross the Rhine River to head deeper into Germany.

Dissimulation, on the other hand, entails concealing one's true intentions, emotions, or capabilities. Unlike simulation, which involves actively projecting a false image, dissimulation revolves around masking genuine thoughts or feelings or deceiving the target into believing something untrue. It involves strategic concealment or distortion of information to mislead or manipulate others. Dissimulation often operates in tandem with simulation, as it provides the foundation for creating a convincing facade. Barton Whaley described dissimulation as hiding the real.

Dissimulation is often best employed in concert with simulation to most effectively deceive a target. For example, in a CIA report which analyzes deception maxims, the report suggests that it is most powerful to deceive someone in a way that reinforces what they already believe.[5] The report discusses World War II, in which Hitler believed that the main Allied invasion would occur at Calais rather than Normandy, France. Knowing Hitler's expectations for an invasion at Calais, the Allies developed a deception plan to reinforce the

[4] "Ghost Army."
[5] Deception Research Program Staff, "Deception Maxims: Fact and Folklore, April 1980" (Central Intelligence Agency, April 1980).

beliefs by simulating a falsehood. They went on to obfuscate or dissimulate their actual plans to land at Normandy.

> Discuss how cognitive processes relate to D&D and how they are exploited by the deception planner.

Denial and deception (D&D) are integral aspects of military strategy, aiming to mislead, confuse, or misdirect a specific target or small group of decision-makers. Understanding how cognitive processes operate is crucial for effective D&D planning. Cognitive processes encompass various mental activities involved in perception, attention, memory, decision-making, and belief formation, all of which influence how individuals interpret information and make sense of their environment. Military deception planners exploit these processes strategically to achieve their objectives by deliberating simulating false events and stimuli and by dissimulating real events and stimuli to lead the adversary to either make a specific choice or not make a specific choice that contributes to the accomplishment of the friendly mission[6].

Military Deception planning begins with detailed and accurate mission analysis and runs concurrently with the joint planning process. It is critical that all aspects of a military deception are tightly controlled and coordinated, and is, therefore, a top-down led initiative that is often coordinated at a higher headquarters element in coordination with other information operations plans and effects. Planners often utilize a "see, think, do" deception methodology, which intends to influence how the adversary sees the deceptive event, determines whether or not those

[6] Joint Chiefs of Staff, “Joint Publication 3-13.4 Military Deception” (Department of Defense, September 14, 2017).

observations are valid, and either takes or does not take specific action as the result of the conclusions of those observations.[7]

Military Deception planners take advantage of human cognition in order to create deceptive effects. Perception plays a fundamental role in D&D by shaping how individuals and groups interpret information from their surroundings. In the military, because the target does not directly perceive most information, the target of a deception campaign is not usually witnessing an event with their own eyes, ears, or other senses. Planners can create a plan that leverages an adversary's military capabilities in order to deceive them.

Planners can create a specific false narrative by employing public or private statements from government or military officials and leaks to journalists or double agents. This would give the adversary intelligence apparatus an anchoring bias by creating an overarching plan, which they can then create details later on that reinforce this initial belief. Friendly forces can use technical means or decoys to fool technical intelligence collection sensors into confirming details that corroborate that initial false plan.[8] By exploiting cognitive limitations in sensory processing, such as selective attention or confirmation bias, planners can direct attention away from critical information or reinforce preconceived beliefs in line with the deception narrative.

Belief formation and maintenance are central to the success of D&D efforts, as individuals' beliefs shape their interpretations of reality and guide subsequent actions. Deception planners employ various strategies to manipulate adversaries' beliefs, including propaganda, psychological operations, and false signaling, which utilize either the central route or peripheral routes to persuasion. By reinforcing existing beliefs, the planner must match the desired false message to the receiver's attitude. The target will carefully consider the persuasive message, so

---

[7] Joint Chiefs of Staff.
[8] Richards J. Heuer, "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly* 25, no. 2 (June 1981): 294, https://doi.org/10.2307/2600359.

the message must align with the target's expertise and experience. Alternatively, planners can focus on the peripheral route, which relies less on the message itself but rather on the source's credibility and style or format of the message to leverage the target's heuristics or simple decision rules, if x, then y[9]. Exploiting belief formation can be especially effective if it reinforces a preexisting adversary dogma or cultural belief.

In conclusion, cognitive processes play a crucial role in both the success and exploitation of military deception operations. Military deception planners leverage an understanding of perception, decision-making, and belief formation, which underlie the "see, think, do, methodology" to craft strategic narratives, manipulate information environments, and influence adversaries' interpretations and actions. By exploiting cognitive biases and limitations, planners can effectively deceive adversaries and achieve tactical or strategic objectives on the battlefield.

Select three technical collection capabilities, describe them, and identify the means by which each can be countered.

Optical Imaging and Radiometry[10]

i. Optical imaging systems are effectively advanced digital cameras. They work by converting an optical image into an electrical signal for transmission and storage, an update from older wet film technology, which was bulky and required retrieval and processing before it could be exploited. These sensors typically take images in the visible and infrared spectrums of light. Modern optical imaging systems take and process images that can be exploited near real-time only, accounting for the latency in which it takes for signals to transit through the requisite data

[9] Stephen W. Littlejohn and Steinfatt, “Elaboration Likelihood Theory,” in *Encyclopedia of Communication Theory* (Thousand Oaks (Calif.): Sage, 2009).
[10] Robert M. Clark, *The Technical Collection of Intelligence* (Washington (D.C.): CQ press, 2010).

architecture and then be exploited by either a human analyst or, increasingly, by advanced artificial intelligence for initial triage.

ii. These sensors can be utilized in a variety of ways, from human reconnaissance to being mounted on aircraft such as Intelligence Surveillance and Reconnaissance drones or manned aircraft, or increasingly mounted on satellites. These different form factors have different tradeoffs; putting a human in a position to take an image carries significant risks, and there are fewer risks, other than technological or financial, from putting an aircraft overhead. However, aircraft can typically only be utilized in an area where that force has air supremacy and is unchallenged by an adversary. In disputed or denied areas, the best option will be mounted on a satellite; however, satellite-mounted sensors tend to have limitations such as image resolution, how clearly an object can be distinguished from something else, and revisit rate, which is how often can an image be taken of a given target, and the requirement for clear weather to be effective. Aircraft can revisit a target within minutes if one is available; satellites, however, are subject to their orbital dynamics.

iii. These sensors can be countered in multiple ways. A mobile target can be challenging to track. A target can be camouflaged or concealed. Nations are increasingly creating sites and buildings with retractable roofs and deeply buried facilities, which can effectively deny remote imaging.

Active Sensing: RADAR C[11]

[11] Clark.

iv. Active Sensing is a term that is used to describe sensors that produce their own energy for the illumination of a target. RADAR is an acronym that stands for Radio Detection and Ranging and describes a system that uses radio waves or electromagnetic waves to determine the size, distance, direction, and speed of a given target. Advances in this technology have given rise to LiDAR or Light/Laser-based detection and ranging. Radar can typically operate in all-weather conditions and consist of one or multiple transmitter antenna, a receiver that detects the broadcast signal, a signal processor that interprets that collection, and a display that is typically in a command and control (C2) node.

v. Radar serves multiple purposes, both civil and military, and operates in multiple bands of the electromagnetic spectrum depending on their intended purpose. RADAR can have an extremely long range and act as an early warning system; some can even detect targets over the horizon by utilizing very low bandwidth waves that bounce off of the Earth's ionosphere; these tend to be relatively imprecise in how they detect targets and can have significant gaps in coverage. Higher bandwidth radar tends to give exact information at the expense of effective distance; the power of their illuminating signal weakens, or attenuates, rapidly and becomes ineffective at far distances.

vi. Adversaries have multiple ways of countering radar by interacting with the emitted energy. For example, many forms of stealth technology employ a combination of materials that absorb electromagnetic information, thus weakening the return signal, and a design that scatters the signal, thus

further degrading the return. Alternatively, an adversary could create a smaller decoy, such as an inflatable ship or a missile, which either gives an inordinately large return by the use of highly reflective and amplifying materials to artificially increase the size of the target, either making it appear realistic, or more attractive to the radar. Finally, electromagnetic warfare systems can jam radar by raising the baseline environment to mask an incoming signal or to present multiple false targets, thus obfuscating the real target.

Passive RF Collection[12]

vii. Passive RF collection, also referred to as Signals Intelligence or SIGINT, encompasses multiple subdisciplines, including communications intelligence, foreign instrumentation systems intelligence, electronic intelligence, and measurement and signature intelligence.

viii. Electronic intelligence often refers to the passive collection and categorization of RADAR signals. This is broken down into two subdisciplines: technical electronic intelligence, which focuses on the analysis of specific signal parameters such as power, phase, and polarization, and operational electronic intelligence, which focuses on taking technical intelligence and using it to categorize and track specific systems and their capabilities. It is often used to compile an adversary "order of battle," which indicates how many of certain systems there are, how often they are used, and where they are typically deployed.

[12] Clark.

ix. The systems used to collect electronic intelligence are typically either mounted or aircraft or spacecraft, and they have different strengths and weaknesses. The highest fidelity of collection typically comes from aircraft operating in the vicinity of a targeted system. However, in order for that aircraft to collect, the system must be operating. Therefore, an adversary could easily counter this either by not operating their most advanced systems when those aircraft are present and only operating legacy or civilian technology. Alternatively, they could develop and test their newest capabilities far inland, out of range of the aircraft, or underground where no radio signals could escape to be collected or observed. Spacecraft have the benefit of being able to cover a much larger area, potentially covering an entire country. However, because of their distance, they often have to deal with a "noisy" or dense signal environment where it can be difficult to differentiate between different signals on the spectrum. Adversaries are also experimenting with Low Probability of Intercept or Detection signals to protect themselves further. They do this either by physically masking some characteristics of the signal or through advanced signal processing capabilities.