How to Challenge Chinaâ??s Military Deception Tactics

Description

The United Statesâ?? pivot from counterinsurgency to peer conflict over the past decade has exposed a critical vulnerability: a diminished focus on detecting deception by operational and tactical level practitioners.

Throughout history, US military strategy has adapted to specific threats. During the Cold War, the AH-64 Apache helicopter was developed to counter a potential Soviet armored offensive through the Fulda Gap. Today, the threat posed by Chinaâ??s advanced deception tactics demands a similarly targeted response. Yet, while the US has spent two decades honing precision strikes against insurgents, China, the pacing threat, has been refining its doctrine of deception for over two millennia, building on principles dating back to 300 BCE.

To effectively counter Chinaâ??s deception-based approach, the US military must undergo a cultural shift that elevates deception detection to a core competency. This requires embedding deception awareness at every level of planning and execution. This article examines how Chinaâ??s deeply entrenched deception strategy creates an asymmetric advantage, contrasts it with the US approach, and presents steps for integrating deception detection into military planning frameworks such as the Intelligence Preparation of the Battlefield. By doing so, we can close this gap and bolster US strategic resilience against a threat that thrives on ambiguity and misdirection.

The Role of Deception Detection in American Military Strategy

For this analysis, *deception detection* refers to the process of identifying and countering adversariesâ?? deliberate efforts to mislead or misinform friendly forces. This can include activities such as concealing true intentions, operational feints, or presenting false narratives to disrupt decision-making and gain a strategic or tactical advantage.

Throughout American military history, both deception and deception detection have played critical roles in achieving strategic objectives. For example, during the 2003 invasion of Iraq, US Special Operations Forces executed a sophisticated deception campaign in northern Iraq. By coordinating with Kurdish Peshmerga forces and using false signals and communications, they created the illusion of a large-scale US attack. The Iraqi militaryâ??s inability to detect the deception tied down significant Iraqi forces in the north, diverting them from the main offensive coming from the south and west.

The Battle of Midway during World War II is another example, one which highlights the importance of detecting enemy deception. In the lead-up to the battle, Japanese forces feinted an attack on the Aleutian Islands to obscure their true objective. However, US Navy cryptanalysts had broken key Japanese codes, enabling them to monitor enemy plans. To confirm Japanâ??s real target, US forces transmitted a false message from Midway about a water shortage. When Japanese communications confirmed â??AFâ?• (the code for Midway) was experiencing a water shortage, analysts identified Midway as the target. Armed with this information, the US preempted the attack, turning the tide of the Pacific War and demonstrating the power of detecting deception at the onset.

After WWII, the focus of US deception detection efforts shifted with the introduction of nuclear weapons during the high-stakes environment of the Cold War. The Soviet Union relied heavily on â??maskirovkaâ??â??a comprehensive doctrine of military deception that included misinformation and concealment. Deception detection during this period was primarily focused on uncovering nuclear arsenals and geopolitical maneuvers rather than combat operations.

In contrast, countering Chinese deception today requires addressing a broader, multi-domain approach. Unlike the Soviet Unionâ??s centralized and doctrinally rigid methods during the Cold War era, Chinaâ??s strategy is far more pervasive, leveraging ambiguity across strategic narratives, tactical operations, and emerging domains like cyber and information warfare. This shift underscores the urgency for deception detection to evolve and become a core competency across all phases of modern conflict.

Today, much of the US emphasis on deception detection *in combat operations* appears to have diminished. Notably, US military doctrine does not formally define â??deception detection,â?? a gap that reflects the limited institutional emphasis on countering adversarial deception as a structured capability.

As General Charles Q. Brown Jr., now chairman of the Joint Chiefs of Staff, noted in 2019, the US militaryâ??s emphasis on deception has waned. Reflecting on past successes, such as those in World War II, he noted, â??Weâ??ve done some of these things in the past. [Deception]â??s not something that we think about as much anymore.â?• In the same discussion, General Brown underscored the critical need to revive deception efforts, particularly to create strategic and operational dilemmas for China in the Pacific. His call to action reflects the urgency of integrating deception into military training and doctrine to preserve a competitive edge in an era of intensifying great-power competition.

The Role of Deception in the Chinese Military

In contrast to the US, China has been refining deception tactics for centuries, dating back to the â??Warring States Periodâ?• (475â??221 BCE). It was against that backdrop that Sun Tsu famously wrote â??All warfare is based on deceptionâ?•â??a philosophy still deeply embedded in Chinese military thought today. This principle is not merely tactical; it is strategic, influencing Chinaâ??s long-term planning and operational art.

In Sun Tzuâ??s view, victory is achieved by outthinking the opponent, often by misleading them into making fatal errors. This aligns with the Daoist principle of wuwei (æ? ä¸º), or â??non-action,â?• where the most effective actions are those that go unnoticed or appear effortless. Modern Chinese theory echoes these principles, emphasizing misdirection. For example, the *Science of Military Strategy*, a core text from the Peopleâ??s Liberation Armyâ??s (PLAâ??s) Academy of Military Science, highlights the use of information warfare to shape enemy decisions through false narratives. Another example is the â??Three Warfaresâ?• (ä¸?æ??) doctrineâ??psychological, public opinion, and legal warfareâ??which highlights Chinaâ??s view of warfare as a broad spectrum with deception woven throughout every aspect of that continuum.

This enduring focus on deception in Chinese military thought is not confined to theory but is deeply embedded in modern doctrinal texts, which outline specific tactics designed to manipulate adversaries across various domains. A good example of this is Chinese joint doctrine, which promotes feints, false signals, and misinformation, ensuring adversaries remain uncertain about PLA intentions. Similarly, the PLA Air Force and Navy manuals stress camouflage, decoys, and false communications to mislead adversaries.

Moreover, Chinaâ??s recent actions illustrate its active application of these doctrines in real-world scenarios. In the South China Sea, for example, China has employed deceptive tactics by deploying maritime militia vessels disguised as fishing boats to assert territorial claims. These vessels, though ostensibly civilian, are coordinated by the Chinese government to support military objectivesâ??a strategy that warrants continued scrutiny.

The foundational texts above, along with Chinaâ??s active application of their principles, reveal a clear insight: China uses deception at all levels of conflictâ??tactical, operational, and strategicâ??to achieve its objectives. This underscores the urgent need to prepare, both to counter such tactics and to deter their use through proactive measures.

The Evolving Role of Deception Detection in LSCO: Lessons from the 2024 SOF-Only JRTC Rotation

The gaps in deception detection doctrine, training, and application have become increasingly evident as the US military refocuses on large-scale combat operations (LSCO) to prepare for peer conflict. This issue was underscored in March 2024 when the 7th Special Forces Group (Airborne) participated in the first SOF-only rotation at the Joint Readiness Training Center (JRTC). While the exercise marked a significant step in aligning SOF training with LSCO objectives, it also highlighted the persistent shortfalls in deception detection across doctrine, training, and practice.

During the rotation, Special Forces Operational Detachment Alphas (SFODAs) conducted missions designed to divert adversarial resources, facilitating joint force entryâ??a strategy reminiscent of SOF operations during the 2003 Iraq invasion. While the rotation demonstrated the offensive potential of deception in LSCO, it also highlighted a critical vulnerability: the lack of emphasis on detecting and countering adversarial deception in military planning.

During the exercise, the simulated enemy employed tactics mirroring the Russian invasion of Ukraine. After a rapid invasion of a neighboring ally, the adversary established a defensive front and claimed the occupied territory as their own. As NATO and conventional forces mobilized, US Army Special Forces teams infiltrated behind enemy lines. Exploiting their knowledge of US doctrine, the enemy devised a sophisticated deception plan: they left a seemingly unguarded helicopter landing zone large enough for a battalion air assault while repositioning air defense assets to suggest a frontal attack was their primary concern.

From conventional intelligence sourcesâ??such as aerial reconnaissanceâ??the air assault seemed the optimal course of action. However, US Special Forces teams identified the trap, determining that the enemyâ??s true intent was to ambush US troops in transport. This analysis, provided by SFODAs, averted a potentially disastrous outcome for the joint force entry. Yet, this success revealed a significant gap: detecting the enemyâ??s deception relied solely on the ingenuity of the SFODAs rather than on a structured, institutionalized deception detection process.

The Necessity of Integrating Deception Detection in US Planning

The above analysis of Chinese doctrine and observations from recent events make it clear that deception is a fundamental element of todayâ??s threat environment. Despite this, US military planning frameworks, such as the Military Decision-Making Process (MDMP) and the Joint Planning Process, lack structured mechanisms for integrating deception detection into operational planning and decision-making. Integrating deception detection as a core competency across the broader force is essential for maintaining strategic advantage in multi-domain conflicts.

While US military intelligence and reconnaissance efforts include elements of deception detection, large portions of the joint planning process lack the structure and prioritization required to counter sophisticated and culturally ingrained tactics employed by adversaries like China. Integrating deception detection doesnâ??t abandon other priorities but rather *enhances existing capabilities*, making the force more resilient and adaptable. By embedding it within established processes like the intelligence preparation of the battlefield (IPB), the US can improve decision-making efficiency, ensuring commanders are better informed without added complexity.

IPB is a systematic process that identifies and analyzes the operational environment to support decision-making. The process consists of four steps: defining the operational environment, describing environmental effects, evaluating the adversary, and determining adversary courses of action. Throughout this process, practitioners should systematically assess potential adversarial deception indicators, such as inconsistencies in intelligence reporting or anomalies in adversary behavior, which are then turned into intelligence collection requirements to later confirm or deny if deception is occurring.

In the first step of the IPB, defining the operational environment, planners can inject counter-deception measures by identifying areas or domains where adversarial deception is most likely to occur such as cyber networks or contested maritime regions. Planners should also asses the adversaryâ??s historical use of deception to anticipate potential strategies. While evaluating environmental effects, planners can assess how adversaries might manipulate terrain, weather, and infrastructure to obscure their intent, such as using complex terrain for ambushes or electronic warfare to disrupt communications.

Evaluating the adversaryâ??s tactics and doctrine allows for identifying deception patterns or vulnerabilities. Planners can employ analytical tools to detect inconsistencies in intelligence reports, such as sudden changes in enemy force dispositions that donâ??t align with known capabilities or logistics constraints. Determining adversary courses of action should include analyzing which actions might serve as deceptive feints versus genuine threats. Techniques like red-teaming and war-gaming can simulate adversary deception tactics, helping to validate or challenge assumptions.

Lastly, deception detection should be incorporated into existing education and training frameworks. For example, exercises should include scenarios where planners identify adversarial deception indicators, such as conflicting intelligence patterns or falsified communications. Moreover, professional military educators should train future leaders in identifying deception tactics, with specific modules on adversaries like China, similar to how Russian tactics were previously taught during the Cold War Era.

Conclusion: Adapting to the New Age of Deception

The US faces an adversary that prioritizes ambiguity and manipulation in every domain of warfare. While the US has historically excelled in projecting overt strength, this approach must evolve to counter deception-focused adversaries like China. Integrating deception detection into IPB, exercises, professional education, and joint planning processes is critical to addressing this asymmetry. By institutionalizing deception detection, US forces can not only counter adversarial misdirection but also ensure more informed operations across allied and joint domains. Such integration would enhance strategic resilience and provide a competitive edge in multi-domain operations. Failure to adapt to this new age of deception risks ceding advantage to adversaries who exploit our blind spots.

Cole Herring is a seasoned professional with 19 years of experience, including a distinguished career in the United States Army Special Forces. With a Master of Science from Kingâ??s College London and a Master of Business Administration from Anglia Ruskin University, Cole combines academic excellence with extensive practical experience.

The views expressed are those of the author(s) and do not reflect the official position of the Irregular Warfare Initiative, Princeton Universityâ??s Empirical Studies of Conflict Project, the Modern War Institute at West Point, or the United States Government.

Main Image: Chinese vessels moored at Whitsun Reef. (Photo by Philippine Coast Guard via Wikimedia)

If you value reading the Irregular Warfare Initiative, please consider supporting our work. And for the best gear, check out the IWI store for mugs, coasters, apparel, and other items.

Date Created
2024/12/19