U.S. Army photo by Markus Rauchenberger

U.S. Soldiers with the 75th Ranger Regiment scale the cliffs at Omaha Beach, Pointe du Hoc, Normandy, France, June 5, 2019, to commemorate the 75th anniversary of Operation Overlord, the World War II Allied invasion of Normandy, commonly known as D-Day. The lessons of World War II still provide valuable insights into how the Army needs to operate now and in future large-scale combat operations.

Deceivingly Decisive: U.S. Army Military Deception and Counterintelligence

by First Lieutenant Will Rector

Introduction

After almost two decades of conducting counterinsurgency operations, the U.S. Army is shifting its focus to prepare for large-scale combat operations. Historical experience suggests that one staff function that will likely play a significant part in such potential conflicts is military deception (MILDEC). For example, the U.S. Army engaged in several MILDEC operations against Axis forces in the European theater of operations during World War II. The success of those operations was due in large part to the support they received from U.S. counterintelligence (CI). Given this historical precedent, this article seeks to answer the question of what support CI can provide to MILDEC in future large-scale combat operations. The findings suggest that CI capabilities can enable opportunities for MILDEC by denying the adversary knowledge of essential elements of friendly information (EEFI) from both U.S. and multinational partners. Primarily, this includes friendly actions, intentions, and capabilities.[1] Additionally, it suggests CI can provide conduits for MILDEC and feedback indicators for assessing its effectiveness.

To demonstrate this argument, this article will rely largely on the Army's experience in the European theater of operations during World War II. While a limited number of

examples of CI and MILDEC coordination can be found in more contemporary large-scale combat operations, World War II is the optimal case to examine for this purpose. This is mainly because the scale and duration of the conflict provided more opportunities for CI and MILDEC coordination relative to the Army's other historical large-scale combat operations.[2]

The organization of this article consists of four parts. The first part provides a general overview of MILDEC and CI. The second part discusses CI functions that can support aspects of MILDEC that emphasize denying the adversary true information pertaining to friendly forces. This contrasts with the third part, which discusses CI functions that can support aspects of MILDEC in providing untruths to adversaries about friendly forces. Lastly, the final part provides a summary of the article's findings, recommendations, and implications for the future.

Defining the Concepts

MILDEC is a type of information-related capability that consists of activities designed to mislead adversary decision makers, with the goal of influencing the adversary to take actions that are advantageous to the friendly mission.[3] These operations consist of more than a cover plan to conceal the actual friendly plan. Rather, they are actions that influence adversary decision makers by either increasing or decreasing ambiguity about the strength, disposition, intentions, or other information pertaining to friendly forces.[4] While both goals are acceptable, operations designed to decrease an adversary's ambiguity (i.e., making the adversary think they are certain about the friendly plan) are the optimal of the two because it decreases the adversary's perceived need to collect additional intelligence on friendly forces.[5] In addition, a MILDEC activity that seeks to confuse or make friendly forces' intentions harder to interpret for the adversary, but does not focus on generating a specific adversary action or inaction, is known as deception in support of operations security (OPSEC).[6] MILDEC accomplishes these goals by controlling the flow of information or disinformation through intelligence gateways known as conduits. These conduits act as pathways to the adversary for introducing a deception story.[7]

The success of MILDEC relies on two factors: 1) denying the adversary knowledge of the true friendly operation and 2) identifying and leveraging suitable conduits that are likely to influence adversary decision makers. Moreover, success is more likely when the deception story is mixed with true information and tailored to mesh with the enemy's existing assumptions or interpretations of friendly forces.[8] If successful, MILDEC has the potential to greatly influence operations on the battlefield. Perhaps the most notable example of successful MILDEC is found in Allied deception activities before the invasion of Western Europe as part of Operation Overlord during World War II. Through MILDEC, the Allies were able to convince the Germans to divert crucial reinforcements to Calais and away from the true objective, Normandy.[9] As such, these operations are typically highly sophisticated and rely on coordination with multiple staff elements.

In addition to staff elements and liaison officers, MILDEC planners must coordinate with the supporting CI elements. CI is an intelligence discipline that seeks to detect, identify, neutralize, or exploit the activities of foreign intelligence entities (FIE). FIE activities include acquiring U.S. information, blocking or impairing U.S. intelligence collection, influencing U.S. policy, or disrupting U.S. systems and programs.[10] In terms of scope, this article focuses specifically on FIE activities of state actors that target U.S. Army and Department of Defense interests. To execute this mission, Army CI conducts operations, investigations of national security crimes, collection, analysis and production, technical services, and support activities. In a large-scale combat operations context, doctrine and historical experience suggest that

Courtesy of the U.S. Army Intelligence and Security Command Historical Collection

A U.S. Army Counterintelligence Corps agent takes a report from a local French national following the withdrawal of German forces from the area.

during defensive and offensive operations Army CI will be primarily tasked with establishing checkpoints to screen internally displaced persons.[11] In addition to internally displaced persons, Army CI will likely screen enemy prisoners of war for any information they might have pertaining to FIE activities. Doctrine and history also suggest that when the Army transitions to stability operations in an area of operations, Army CI will likely conduct investigations and collection activities to counter FIE activities.[12] Like MILDEC, the success of CI activities has major implications for the security of Army operations. For example, the Army counterespionage operation against Clyde Conrad stopped the further compromise of sensitive Army war plans to the Soviet bloc during the late Cold War era.[13]

Outside the four CI mission areas—counterespionage, CI support to force protection, CI support to research and development, and cyber—one aspect of CI that is often overlooked is CI support to MILDEC. To emphasize this role, the following sections discuss how CI can contribute to the success of MILDEC operations.

Denying the Adversary

The first service CI can provide to MILDEC operations is denying the adversary knowledge of friendly forces' EEFI. CI can achieve this by promoting OPSEC as well as conducting CI operations and investigations that exploit and/or neutralize FIE activities. OPSEC is crucial to the success of MILDEC operations because it limits FIE ability to accurately identify actual friendly intentions and protects operations from being compromised. Effective OPSEC ensures security measures are in place to limit the amount of mission-critical information that the adversary can observe and collect on that is contradictory to the deception story.[14] To support this effort, Army CI conducts Covering Agent Program activities. These activities mitigate threat collection efforts by promoting OPSEC and increase vigilance by providing CI Threat Awareness and Reporting Program briefings to Army personnel. These briefs are essential for educating Soldiers on how to identify indicators of FIE and insider threat activities to protect critical EEFI pertaining to friendly actions, intentions, and capabilities.[15] In addition, CI capabilities briefs inform local commanders, security managers, and other leadership in the area of operations about what support CI can provide them. Furthermore, an effective Covering Agent Program can advise supported units of the FIE threat and assist them in developing threat reporting awareness and relationships.[16]

Despite efforts to enhance Threat Awareness and Reporting Program measures, widespread accessibility to smartphones and wireless internet access poses challenges to maintaining adequate OPSEC in the contemporary operational environment. In 2018, several media outlets identified the location of United States forces operating in Afghanistan by leveraging a popular running app.[17] Similarly, open-source analysis leveraged social media to identify Russian soldiers deployed in eastern Ukraine in 2015.[18] Such examples demonstrate that the Army will likely face considerable difficulties in maintaining OPSEC in future large-scale combat operations. Because FIE can easily take advantage of such situations, adequate CI assets are essential for investigating any potentially damaging lapses in OPSEC. To this end, CI can support MILDEC in large-scale combat operations by neutralizing FIE human intelligence efforts to collect on friendly forces. By investigating espionage and other related national security crimes, CI can deny the adversary knowledge of EEFI and thereby protect the deception story.

Deceiving the Adversary

A second service that CI can provide to MILDEC operations in large-scale combat operations is identifying and leveraging suitable conduits for the deception story. Allied deception conduits in World War II included using technical means such as false signal communications and decoy or "dummy" units, in addition to human means such as controlled enemy agents (CEA).[19] While technical means were highly successful in the execution of MILDEC in World War II, adversary capabilities may limit their effectiveness in future large-scale combat operations. For instance, adversaries such as Russia have heavily invested in electronic warfare capabilities to counter the United States Army's superior technical-communications infrastructure.[20] If the Army is unable to emit signals for real communications, it is unlikely it will be able to do so for false communications. As a result, these systems have the potential to disrupt not only U.S. maneuver operations but also MILDEC operations. The implication of such adversary capabilities is that MILDEC conduits that rely on technical means such as false communications may not be available to the Army in a large-scale combat operations environment. In such a scenario, the Army may need to rely on low-technology means, such as CEAs, for establishing MILDEC conduits.

In World War II, the Army was successful in establishing low-technology conduits for MILDEC by using CEAs.[21] CEAs were FIE-tasked human sources that Allied CI leveraged to operate on behalf of friendly forces via the following process. FIE typically tasked human sources to operate in friendly controlled areas as "stay-behind" agents. Once in place, these enemy agents would collect on friendly forces and send their reports back to FIE via radio transmission. Upon detecting and arresting enemy agents for espionage

Courtesy of the U.S. Army Military Intelligence Corps Historical Collection

U.S. Army military deception units position dummy tanks as part of Operation Fortitude in preparation for the invasion of Normandy.

or sabotage, local Army CI detachments screened them to determine whether they possessed the potential for use as a CEA.[22] If they identified an individual with such potential, the CI detachment transferred the enemy agent to the custody of the Special Counterintelligence detachment.[23] These units consisted of a team of officers from the X-2 (not to be confused with the Army 2X staff position) section of the Office of Strategic Services that were attached to an Army Group headquarters.[24] If the Special Counterintelligence detachment determined that the enemy agent was suitable, it would task him or her with feeding the adversary disinformation to FIE as a CEA.[25] Such operations were particularly aggressive in nature relative to deception in support of OPSEC in that they sought to influence the adversary's actions. As X-2 historian Timothy Naftali explains:

> ***With [CEAs] under your control you could supply your enemy with information of your own choosing. Assuming you could prevent him from forming a word-picture from uncontrolled sources—air reconnaissance, signals interception, etc.—then manipulation of his assessments of the military, political and diplomatic situation lay within your grasp. Moreover, under these conditions, there was the opportunity to compel him to take steps that would materially improve your own situation, by weakening his.[26]***

Naftali's assessment suggests FIE can be a useful conduit for passing disinformation as part of a deception story. This is largely because they constitute the adversary's primary means of obtaining knowledge of the true friendly plan.[27] Therefore, CEA operations are more likely to be successful when CI can prevent or neutralize FIE recruitment of non-CEA (i.e., uncontrolled) penetrations among Army personnel that could result in the adversary's collection of EEFI.[28]

An example of the use of CEAs in World War II MILDEC operations is Operation Jessica. This MILDEC operation from late 1944 to early 1945 intended to deceive German decision makers into retaining a substantial force along the Franco-Italian border rather than commit them as reinforcements to other fronts.[29] To support this operation, Special Counterintelligence detachments leveraged CEAs within the network they had developed in France. Two specific CEAs, Paul Jeannin and a source codenamed FOREST, provided false reports to German intelligence pertaining to troop movements and other information that would indicate preparations for an Allied offensive in northern Italy.[30] Through these efforts, at least two German divisions badly needed elsewhere were held on the Italian front.[31] Thus, in this capacity, Army Group Special Counterintelligence detachments successfully exploited CEAs to support MILDEC operations during World War II.[32]

Since effective deception stories typically use multiple conduits, relying on a single conduit is not optimal but nonetheless may be the most practical choice depending on the difficulty of penetrating the target.[33] When the operational environment negatively impacts the number of available conduits for MILDEC, CI can provide a low-cost and low-technology method of providing the adversary decision makers with disinformation through the use of sources similar to the World War II–era CEAs.[34] Furthermore, these types of sources provide CI the ability to assess whether the adversary has accepted the MILDEC disinformation as truth, as well as other critical information about friendly forces of which the adversary is aware.[35] Based on this assessment, CI can also analyze and assess what information the FIE

tasked the CEA to collect. This in turn provides a feedback indicator for MILDEC planners to determine if the deception story is effectively influencing the adversary's perception of friendly forces.

Conclusion and Recommendations

MILDEC faces several challenges as the Army shifts from fighting counterinsurgencies to large-scale combat operations in the contemporary operational environment. Historical experience suggests active and aggressive CI support to MILDEC can help resolve some of these challenges. Particularly, this article has devoted much of its discussion to how FIE can influence MILDEC operations. Since engaging FIE is primarily a CI mission, it is essential that MILDEC planners leverage and coordinate with Army CI.

As one of the initial steps to increase coordination between these disciplines, this article recommends that CI support to MILDEC be designated as an additional/fifth CI mission area. The support CI can provide MILDEC includes denying FIE the ability to collect intelligence on friendly forces while simultaneously providing FIE disinformation to propagate a deception story. As this article discussed, CI support significantly contributed to the success of MILDEC operations in World War II. If the Army can learn from such lessons and implement them in how it plans to fight in future conflicts, it will be better prepared to operate in complex large-scale combat operations.

Courtesy of the U.S. Army Intelligence and Security Command Historical Collection

Army Counterintelligence Corps agents searching for items of intelligence value among captured German documents.

Endnotes

1. Department of the Army, Field Manual (FM) 3-13.4, *Army Support to Military Deception* (Washington DC: U.S. Government Publishing Office [GPO], 26 February 2019), 1-5.

2. For a limited discussion of U.S. Army counterintelligence support to military deception in the Gulf War, see Douglas L. Tystad, *The Role of the Media in the Operational Deception Plan for Operation Desert Storm* (Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, 3 April 1992), 20, https://apps.dtic.mil/dtic/tr/fulltext/u2/a258285.pdf.

3. Department of the Army, FM 3-13.4, *Army Support to Military Deception,* 1-1.

4. Donald C. Daniel and Katherine L. Herbig, eds., *Strategic Military Deception* (New York: Pergamon Press, 1981), 5.

5. Robert M. Clark and William L. Mitchell, *Deception: Counterdeception and Counterintelligence* (London: Sage Publications, 2019), 13.

6. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 3-13.4, *Military Deception* (Washington, DC: The Joint Staff, 26 January 2012), I-2.

7. Ibid., viii.

8. Daniel and Herbig, *Strategic Military Deception,* 42.

9. Jonathan Gawne, *Ghosts of the ETO: American Tactical Deception Units in the European Theater, 1944-1945* (Havertown, PA: Casemate, 2014), 12.

10. Department of the Army, Army Techniques Publication (ATP) 2-22.2-1, *Counterintelligence Volume I: Investigations, Analysis and Production, and Technical Services and Support Activities (U)* (Washington, DC: U.S. GPO, 11 December 2015), Glossary-4 (common access card login required).

11. U.S. Army Intelligence Center, *History of the Counter Intelligence Corps: Volume XV* (Fort Holabird, MD: U.S. Army Intelligence Center, 1959), 22.

12. John Schwartzwalder, *We Caught Spies: A History of the U.S. Army's Counterintelligence Corps* (New York: Duell, Sloan and Pearce, 1946), 108.

13. For an exceptional account of the Conrad case from the U.S. Army's perspective, see Stuart Herrington, *Traitors Among Us: Inside the Spy Catcher's World* (Novato, CA: Presidio Press, 1999).

14. Office of the Chairman of the Joint Chiefs of Staff, JP 3-13, *Information Operations* (Washington, DC: The Joint Staff, 27 November 2012), II-12. Change 1 was issued on 20 November 2014.

15. Department of the Army, Army Regulation 381-12, *Threat Awareness and Reporting Program* (Washington, DC: U.S. GPO, 1 June 2016).

16. Department of the Army, ATP 2-22.2-1, *Counterintelligence Volume I,* 2-2.

17. Alex Hern, "Fitness tracking app Strava gives away location of secret US army bases," *Guardian,* January 28, 2018, https://www.theguardian.com/

world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

18. Dmitry Volchek and Claire Bigg, "Ukrainian bloggers use social media to track Russian soldiers fighting in east," *Guardian,* June 3, 2015, https://www.theguardian.com/world/2015/jun/03/bloggers-social-media-russian-soldiers-fighting-in-ukraine.

19. Donald J. Bacon, "Second World War Deception" (master's thesis, Air Command and Staff College, 1998), 20.

20. Asymmetric Warfare Group, *Russian New Generation Warfare Handbook* (Washington, DC: U.S. GPO, 2017), 17.

21. Robert Cowden, "OSS Double-Agent Operations in World War II," *Studies in Intelligence* 58, no. 2 (2014): 65.

22. U.S. Army Intelligence Center, *History of the Counter Intelligence Corps: Volume XVIII* (Fort Holabird, MD: U.S. Army Intelligence Center, 1959), 85.

23. Ibid.

24. George C. Chalou, *The Counter Intelligence Corps in Action* (New York: Garland, 1989), 290.

25. U.S. Army Intelligence Center, *History of the Counter Intelligence Corps: Volume XVI* (Fort Holabird, MD: U.S. Army Intelligence Center, 1959), 8.

26. Timothy Naftali, "X-2 and the Apprenticeship of American Counterespionage 1942-1944" (PhD diss., Harvard University, 1993), 3.

27. Clark and Mitchell, *Deception,* 13.

28. Abram Shulsky, "Elements of Strategic Denial and Deception," *Trends in Organized Crime* 6, no. 1 (2000): 22.

29. Thaddeus Holt, *The Deceivers: Allied Military Deception in the Second World War* (New York: Skyhorse Publishing, 2007), 650.

30. Cowden, "OSS Double-Agent Operations," 70.

31. Ibid., 71.

32. William Hood, "Angleton's World: Lessons for U.S. Counterintelligence," in *U.S. Intelligence at the Crossroads,* ed. Ernest May, Roy Godson, and Gary Schmitt (New York: Potomac Books, 1995), 74.

33. Department of the Army, FM 3-13.4, *Army Support to Military Deception,* 2-10.

34. Robert W. Stephan, *Stalin's Secret War: Soviet Counterintelligence against the Nazis, 1941-1945* (Lawrence, KS: University Press of Kansas, 2003), 13–14.

35. Michael I. Handel, "Intelligence and Deception," *Journal of Strategic Studies* 5, no. 1 (1982): 126.

1LT Will Rector is the executive officer of Charlie Company, 301st Military Intelligence Battalion, where he was previously the counterintelligence platoon leader. He is a Ph.D. candidate in political science at Arizona State University. He holds a master's degree in security studies and a bachelor's degree in international relations and German.