



Page 2 Issued in lieu of N^o 09650 lost. Page 3 Navy Form 8, 1951

Surname **MARTIN**

Other Names **WILLIAM**

Rank (at time of issue) **CAPTAIN, R.M.
(ACTING MAJOR)**

Ship (at time of issue) **H Q
COMBINED OPERATIONS**

Place of Birth **CARDIFF**


Year of Birth **1907**

Issued by *A. Langens*

At **ADMIRALTY**

Date **2nd February 1943.**

NAVAL
IDENTITY CARD No. 148228



Signature of Bearer
W. Martin

Visible distinguishing marks
NIL.



Top left: The corpse of Glyndŵr Michael fully dressed and outfitted as Maj. William Martin, Royal Marines, in London, just before being sealed in his air-tight canister as the central piece of Operation Mincemeat. Top right: Identity card for Capt. (acting Maj.) William Martin, Royal Marines. One of the fictitious documents created. Bottom: Some of the effects included on "Maj. Martin's" person as part of the operation. (Photos courtesy of the Imperial War Museum, United Kingdom)

Perceptions Are Reality

Historical Case Studies of Information Operations in Large-Scale Combat Operations

Col. Mark D. Vertuli, U.S. Army

All war is inherently about changing human behavior, with each side trying to alter the behavior of the other by force of arms. Success requires the ability to outthink an opponent and ruthlessly exploit the opportunities that come from positions of relative advantage. The side that best understands an operational environment learns and adapts more rapidly and decides to act more quickly in conditions of uncertainty is most likely to win.

—ADRP 3-0, *Operations*

Arguably, information operations (IO) is one of the most misunderstood and misused terms in Army doctrine, to the point where it has largely become a ubiquitous term of reference that lacks the necessary clarity of purpose and application for the majority of the Army. I am sure that if several Army leaders and soldiers were asked to define information operations in their own words, one would receive several differing—and often conflicting—interpretations. Multiple changes to Army doctrine concerning information operations after it emerged as a concept from *Joint Doctrine for Command and Control Warfare (C2W)* over twenty-five years ago have contributed to this confusion.¹ The definition of IO has changed three times in the last eleven years alone: from C2W's focus on five core capabilities, to information engagement (2007), to inform-and-influence activities (2011), to its current incarnation focusing on information-related capabilities (2016). As the Army shifts its doctrinal focus to large-scale combat operations (LSCO) against peer and near-peer adversaries, the purpose of *Perceptions Are Reality* is to help leaders and soldiers visualize and understand IO through the lens of historical case studies.

In both joint and Army doctrine, IO is defined as “the integrated employment, during military

operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.”² In more general terms, IO supports the commander's ability to achieve a position of relative advantage through activities in the information environment (the physical, informational, and cognitive dimensions) to influence the adversary's will to fight; to disrupt, corrupt, or usurp its capabilities to collect, process, and disseminate information; and ultimately to manipulate (deceive) or disrupt an enemy decision-maker's understanding of the operational environment. Field Manual 3-0, *Operations*, does a very good job describing the broad scope of possible information-related capabilities and effects in the information environment. However, over the course of the last seventeen years of counterinsurgency and counterterrorism operations, IO has become synonymous, in many minds, with themes and messages, psychological operations (PSYOP)/military information support operations, or strategic communications/communications strategy, and its larger purpose has become lost.

Three lessons (dare I say themes) are interwoven throughout the book's historical case studies of information operations during large-scale combat operations: (1) the focus is the *information*, regardless of the capabilities employed to effect it; (2) successful information operations are operations—integrated, synchronized, resourced, and commander-led from inception to execution; and (3) information operations are, at their core, adversary/enemy-focused operations conducted to gain a relative advantage for friendly decision-makers.

“It Is All About the Information”

The title of this book in the LSCO box set is *Perceptions Are Reality*. Although this could be read as hackneyed phrase, its meaning has great significance to the application of IO in LSCO. Leaders visualize and understand the operational environment through information. As an element of combat power, information enables decision-making, and its transmission aids decisive operations. Today, modern technology has significantly increased the speed, volume, and access to information. Concurrently, technology has enabled significant means to disrupt, manipulate, distort, and

Previous page: Operation Mincemeat provides a classic example of how information operations can support a large-scale combat operation. The British operation in April 1943 involved creating a fictitious military officer using the body of a dead vagrant, planting false attack plans on it, and floating it off the Spanish coast, where it was picked up by Spanish fishermen. The Spanish government shared the false information found on “Cpt. William Martin” with German intelligence before returning him back to the British. The deception fooled the Germans, who reinforced Greece and Sardinia in the belief they were targeted for Allied invasion while leaving the actual invasion site, Sicily, relatively unprotected.



غداً سوف تضرب فرقة المشاة السادسة عشر وسيكون
القصف شديد، إذا أردت النجاة أترك مكانك ، ولا تسمح
لأحد ان يمنعك. أنقذ نفسك وتوجه الى الحدود
السعودية وسوف تجد من يستقبلك كأخ.

Close to five hundred thousand of these leaflets were dropped by U.S. Army Civil Affairs and Psychological Operations Command during Operation Desert Storm in 1991. The front of the leaflet (*above*) shows a B-52 bomber dropping bombs with the Arabic text that translates to "This is your first and last warning! The 16th Infantry Division will be bombed tomorrow! Flee this location now!" The back of the leaflet (*below*) translates to "The 16th Infantry Division will be bombed tomorrow. The bombing will be heavy. If you want to save yourself, leave your location and do not allow anyone to stop you. Save yourself and head toward the Saudi border, where you will be welcomed as a brother." The 16th Infantry Division was on the Kuwait-Saudi border and was smashed by Task Force Muthana of the Joint Arab Command. (Photos and information courtesy of www.psywar.org and www.psywarrior.com)

“During LSCO, maneuver in and through the information environment must be given the same attention as has been historically given to traditional maneuver on the land domain. Maneuver is maneuver, and whatever form of maneuver is employed, it is done through the operational process.”

LSCO

deny information; technology adversaries have already demonstrated a willingness to use with great effect.

In the book *Dark Territory*, author Fred Kaplan recounts an anecdote from then Rear Adm. Mike McConnell. While watching the movie *Sneakers* in 1992, the intelligence chief experienced the revelation that “it is all about the information”; that whoever controlled the information could dominate competition and conflict.³ In LSCO, this remains as true as ever. Leaders direct resources toward intelligence collection in order to develop the situation and gain the sufficient information required to make timely and informed decisions. Just as importantly, measures must be put into place to protect friendly information while simultaneously developing and executing means in all domains to attack the adversary’s ability to access, process, and disseminate information. In this way, IO enables an accurate understanding of the operational environment while disrupting or manipulating that of the adversary.

Through IO, the adversary/enemy decision-maker’s reality should be that which best supports achieving a position of relative advantage. The doctrinal definition change away from the rather limiting five core capabilities of C2W to the current more wide-ranging definition focused on effects is a move in the right direction. That said, more needs to be done to fully garner the true potential of information as an element of combat power in a LSCO context. Common sense dictates that information absent accompanying action does not resonate cognitively in the same way when both are present and complementary. However, the perception of IO as an enabler to maneuver or operations remains. The duality of relationship between action and information must become a constant theme of operations in the Information Age of the twenty-first century.

Information Operations are Operations

When addressing the idea of conflict in space, the commander of U.S. Strategic Command, Air Force Gen. John Hyten, said that there is no such thing as space war or cyber war, for that matter; just *war*. Similarly, I had a recent conversation with a senior leader who remarked that if IO planners had their way, everything would be considered information operations. I would like to flip that on its head. During LSCO, maneuver in and through the information environment must be given the same attention as has been historically given to traditional maneuver on the land domain. Maneuver is maneuver, and whatever form of maneuver is employed, it is done through the operational process.

Recent changes to joint doctrine are beginning to account for the recognition of information’s importance in conflict. Just last year, the secretary of defense and the chairman of the joint chiefs approved a rapid joint doctrine modification to make information a joint function. More recently, the joint staff issued a directive for operations in the information environment—titled as such to emphasize the activity as operations while avoiding the polarizing term information operations.⁴ This

Col. Mark Vertuli, U.S. Army, is chief of Operations Plans (J35) for U.S. Strategic Command. He holds master’s degrees in history from Vanderbilt University and in national resource strategy from the Eisenhower School, National Defense University. He has over twenty-three years of military experience and has planned information operations in Afghanistan and in the European Command and Pacific Command areas of responsibility. He served as commander of 1st Battalion, 1st Information Operations Command (Land) from 2012 to 2014.



emphasis comes after observing adversaries wielding information powerfully on and off the battlefield to achieve decisive tactical to strategic outcomes.

In Iraq and Afghanistan, the Taliban and al-Qaida staged countless engagements against the United States and its partners, less for the physical effects in the immediate operational environment, but rather to gain an informational advantage around the world. Videotaped improvised explosive device attacks, while devastating, worked well to promote an image of organizational credibility, bolster adherents' will to fight, radicalize vulnerable populations, and increase financial support.

More importantly with respect to LSCO, Russian information confrontation activity preceding, during, and following its illegal annexation of Crimea and invasion of eastern Ukraine demonstrates the power of integrated operations in the information environment, in this case more appropriately termed information warfare. Russia successfully sowed disinformation, causing the international community to distrust the information it was receiving while also crippling the Ukrainian

Sgt. 1st Class Richard Miller (left) and Chief Warrant Officer 2 Larry Elrod of the U.S. Army Cyber Protection Brigade discuss the response to a simulated cyber attack on the 1st Brigade Combat Team, 82nd Airborne Division, 6 November 2015 during the brigade's rotation at the Joint Readiness Training Center, Fort Polk, Louisiana. (Photo by Bill Roche)

response through cyberspace operations, electronic warfare, and psychological operations. The confusion and misdirection caused by Russian information warfare had a paralytic effect on Western decision-makers. So much so, that Russia was able to achieve its strategic and political objectives before Western leaders could mount a credible response.

Adversary Focused

There is one final lesson or theme that runs through the case studies of LSCO: IO is, at its core, adversary focused. The seventeen years of counterinsurgency and counterterrorism operations gave rise to

a population-centric focus for IO while almost completely subsuming the adversary command-and-control elements of the doctrine. Only recently, really as a result of adversary successes, has this begun to change. Unified land operations occur in an operational environment dominated by civilians; their presence cannot be ignored or bypassed. However, first, the adversary must be defeated.

Warfare is a human endeavor; it is a contest of wills. The focus of IO during LSCO must be on defeating the adversary's will. This can be accomplished directly, as during Operation Desert Storm where combined bombing and PSYOP dispirited thousands of Iraqi troops and caused their surrender. Or more indirectly, during Operation Iraqi Freedom, the United States and Allied application of deception, electronic warfare, physical destruction, and cyberspace operations disrupted Iraqi command and control, causing an absolute lack of situational understanding and inability to coordinate a defense by Iraqi leadership. As the quote at the beginning of this article states, "The side that best understands an operational environment learns and adapts more rapidly and decides to act more quickly in conditions of uncertainty is most likely to win."

The Book

Perceptions Are Reality is composed of eleven chapters. The first ten chapters explore historical case studies of IO during LSCO, and the final chapter considers the future implications of IO for LSCO. While many information-related capabilities are explored in the case studies, by no means do they present the definitive accounting. Some of the more technical or sensitive capabilities are not treated in as much depth as I would prefer due to considerations of security and classification. The case studies cover LSCO from World War II through recent conflicts in Georgia and Ukraine. While the United States is prominent in most of the



case studies, other nation's operations in the information environment are explored as well, particularly those of the Russian Federation.

In "The Logic of Information Operations in Large Scale Combat Operations," Col. Christopher Lowe explores the evolution of U.S. Army IO doctrine from its C2W roots to today's commonly held (mis)perception that IO is a means to influence civilian populations. Lowe attributes the origin of the United States IO to Cold War Soviet radio-electronic combat doctrine developments. The United States recognized that it needed similar doctrine, organization, training, material, leadership, personnel, and facilities solutions to counter the Soviet's development and an offset strategy to dominate on the modern battlefield through information. Over the course of several years of peacekeeping, counterinsurgency, and counterterrorism operations, the Army shifted focus from a command-and-control emphasis to a more population-centric, "hearts and minds" approach. The second chapter continues along a similar narrative.

While Lowe explores IO past, Maj. Justin Gorkowski reflects upon the current state of Army IO in "U.S. Information Operations in Large-Scale Combat Operations: Challenges and Implications for the Future Force." In his chapter, Gorkowski details internal, structural challenges to Army IO in doctrine, organization, and leadership in juxtaposition to adversarial advancements in the employment of information warfare in competition with the United States. While Gorkowski's assessment is not positive, it is not without hope for the future. He concludes his chapter with several recommendations to address the imbalance.

The third chapter provides a more in-depth analysis of Russian information warfare. United States Military Academy

Some of the patches of fictitious units that the U.S. Army used in a number of World War II deception operations. (Graphics created by various authors via Wikimedia Commons)

professors Dr. Lionel Beehner, Col. Liam Collins, and Dr. Robert Person combine first-hand accounts with secondary research to explore recent historical case studies of Russia's systemic, strategic use of information warfare, focusing on the evolution of its military doctrine from the Russia-Georgia War of 2008 to the ongoing Russia-backed campaign in Ukraine's Donbass region. This look at Russian strategy of information confrontation offers stark lessons for future large-scale combat operations and the integration of operations in the informational environment to achieve strategic effects.

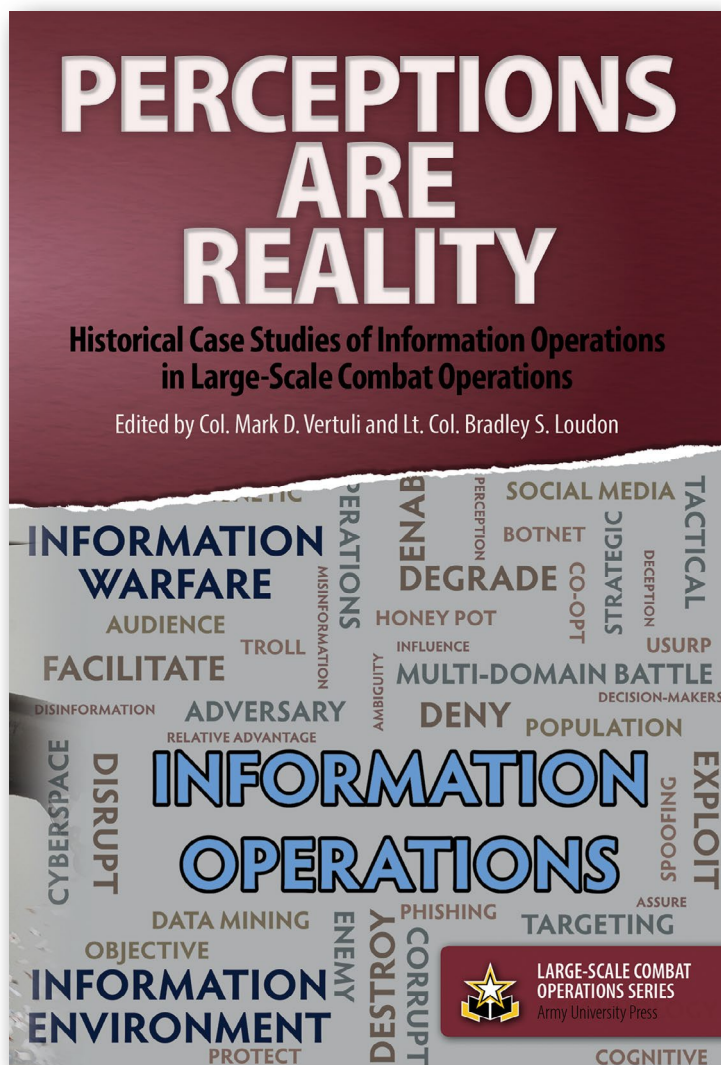
Taking the approach that one can learn as much from failure as from success, Michael Taylor analyzes one of the lesser-known Allied deception operations from World War II. In "Operation Starkey: The Invasion that Never Was," Taylor explores the reasons for the deception plan's failure to convince German leadership of Allied intentions to invade in 1943 in order to keep German forces in the west to relieve pressure on the allied Russian forces in the east. In the following chapter, Branden Riley, Michael Kitchens, and Matthew Yandura use the 1948 Arab-Israeli War to illuminate ways in which information was honed into a weapon by the belligerents and their supporters to achieve desired military, political, and social outcomes within the context of LSCO. In this war, the employment of strategic master narratives to guide

operational and tactical maneuver in the information environment proved decisive.

In chapter 6, Andrew Whiskeyman focuses on the use of PSYOP during the Vietnam War. After a brief exploration of the doctrinal, leadership, intelligence, and organization underpinnings of Military Assistance Command Vietnam, Whiskeyman details PSYOP employment during the largest ground (Operation Cedar Falls) and airborne (Operation Junction City) operations of the war. While PSYOP achieved some success during these operations, significant challenges impeded widespread support and operational integration. Many of these challenges continue to exist today.

Turning to more recent operations, the next two chapters examine IO during the Gulf War and Operation Iraqi Freedom. First, Dr. Robert Hill updates the first chapter of Dr.

Dorothy Denning's 1992 book, *Information Warfare and Security*. Using editorial comments throughout the text, Hill makes contemporary and relevant to today's operational environment Denning's exploration of what is considered the first true information war: Desert Storm. In the following chapter, Carmine Cicalese provides the only first-hand account in this volume. As the coalition forces land component commander (CFLCC) IO planner from April to July 2002, then Maj. Cicalese played an instrumental role in the design of information operations to support the CFLCC operational intent. This chapter offers tremendous insight



and lessons learned into planning and executing IO in LSCO at the highest operational levels.

The final two historical case studies explore elements of cyberspace operations during the recent conflicts in eastern Europe. While chapter 3 of this book examines Russian Federation information warfare from a strategic perspective, Wesley White documents Russian operational and tactical integration of cyberspace effects in Georgia, Estonia, and Ukraine. White argues that these conflicts served as test beds—cyber crucibles—for Russian forces to fully integrate cyberspace operations into multi-domain battle. In chapter 10, Rick Galeano, Katrin Galeano, Dr. Samer al-Khateeb, Dr. Nitin Agarwal, and James Turner focus on the employment of social botnets in support of military operations. Through detailed analysis of botnet use in Ukraine and the Baltics, they argue social botnet can be used to promote narratives, alter perceptions of viewpoint popularity, and ultimately trigger behavior supportive to military end states.

The book concludes with a look to the future. In the final chapter, Maj. Gen. James Mingus and Col. Christopher Reichart explore the implications of the

future information environment across the range of military operations during both competition and conflict. They offer several important recommendations that touch elements of Army training, organization, doctrine, and leadership in order to provide commanders the informational capability and capacity to gain and maintain a position of relative advantage in the future operational environment.

The intent of *Perceptions Are Reality* is to employ history to stimulate discussion and analysis of the implications of IO in future LSCO by exploring past actions, recognizing and understanding successes and failures, and offering some lessons learned from each author's perspective. I leave it you, the reader, to determine its success. ■

I want to thank all the authors for volunteering their time and research to support this effort. Brad Loudon provided tremendous advice and editorial support; I could not have completed this without his assistance. Finally, I want to offer my most heartfelt thanks to the leaders at the Army Combined Arms Center and Army University Press for entrusting me with this project.

Notes

Epigraph. Army Doctrine Reference Publication 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 6 October 2017), 1-4.

1. Joint Publication (JP) 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)* (Washington, DC: U.S. GPO, 7 February 1996 [obsolete]), II-1. The five elements of C2W are operations security, psychological operations, military deception, electronic warfare, and physical destruction.

2. JP 3-13, *Information Operations* (Washington, DC: U.S. GPO, 20 November 2014), GL-3; Field Manual 3-13, *Information Operations* (Washington, DC: U.S. GPO, 6 December 2016), 1-2.

3. Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon and Schuster, 2017), 31.

4. *Department of Defense Strategy for Operations in the Information Environment* (Washington, DC: U.S. Department of Defense, June 2016), accessed 25 June 2018, <https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf>.