The Scholar

Texas National Security Review: Volume 6, Issue 1 (Winter 2022/2023)
Print: ISSN 2576-1021 Online: ISSN 2576-1153

The Organizational Determinants of Military Doctrine: A History of Army Information Operations

Sarah P. White

For the past four decades, the U.S. Army has made repeated attempts to create an enduring doctrinal framework that describes the role of information in conflict, yet these attempts have been largely unsuccessful. What accounts for this struggle? More broadly, why do militaries choose one doctrinal concept over others, and what determines whether a new doctrine will succeed or fail? Building upon classic scholarship in military innovation, this paper traces the evolution of Army information doctrine to highlight the unique role of military sub-communities in determining whether changes to doctrine endure or are ultimately rejected. The structural reforms that were necessary to modify and elevate the role of information within Army doctrine ultimately came to handicap the Army's ability to transform that role when the strategic environment demanded it. While strategic and technological conditions can create the necessary pretext for doctrinal change, there are important organizational determinants of doctrine that may operate independently of the demands of the overarching strategic environment and that can force difficult and suboptimal compromises with respect to the final product.

In the spring of 2019, Lt. Gen. Stephen Fogarty announced his intention to transition U.S. Army Cyber Command into an information warfare command. The announcement reflected Fogarty's conviction of the increased importance of information to cyberspace operations. "The power we are going to project globally," he stated, "is information."[1] Discussion for the next year focused on expanding cyberspace operations to encompass information warfare and included proposals to rename subordinate cyber units and to shift the curriculums at Army training centers.[2]

Eighteen months later, in the fall of 2020, U.S. Army Cyber Command announced that information warfare had given way to the concept of information advantage. Designed to achieve "decision dominance," information advantage was settled upon as a more appropriate description of the expanded Army mission in the information space — described as an environment of "unprecedented information warfare."[3] Organizations ranging from U.S. Army Cyber Command to the U.S. Army Combined Arms Center began to wrestle with the concept of information advantage even as they continued to use, at times interchangeably, the terms "information warfare" and "information operations."

The arrival of the term "information advantage" to the doctrinal lexicon has marked the seventh shift in Army information operations terminology in under four decades. Beginning with "command,

[1] Kimberly Underwood, "Army Cyber to Become Information Warfare Command," *Signal Magazine*, March 14, 2019, https://www.afcea.org/signal-media/technet-augusta-22-coverage/army-cyber-become-information-warfare-command.

[2] Sydney Freedberg Jr., "Army to Build New Info War Force — Fast," *Breaking Defense*, Aug. 22, 2019, https://breakingdefense.com/2019/08/the-armys-information-warfare-build-up/; Mark Pomerleau, "U.S. Army Cyber Chief Outlines Ten Year Plan for Information Warfare," *C4ISRnet*, July 28, 2020, https://www.c4isrnet.com/smr/information-warfare/2020/07/28/us-army-cyber-chief-outlines-ten-year-plan-for-information-warfare/; Mark Pomerleau, "When Should the Army's Cyber School Teach Information Warfare?"*C4ISRnet*, Aug. 5, 2019, https://www.c4isrnet.com/information-warfare/2019/08/05/when-should-the-armys-cyber-school-teach-information-warfare/; Mark Pomerleau, "A New Name — and Focus — for Army Cyber Command?" *C4ISRnet*, Aug. 21, 2019, https://www.c4isrnet.com/show-reporter/technet-augusta/2019/08/21/a-new-name-and-focus-for-army-cyber-command/; and Mark Pomerleau, "A New Company Level Unit to Support Information Warfare," *C4ISRnet*, July 8, 2020, https://www.c4isrnet.com/information-warfare/2020/07/08/heres-what-tactical-army-cyber-units-will-use-to-conduct-operations/.

[3] Mark Pomerleau, "Out: 'Information Warfare.' In: 'Information Advantage,'" *C4ISRnet*, Sept. 29, 2020, https://www.c4isrnet.com/information-warfare/2020/09/29/out-information-warfare-in-information-advantage/.

control, and communications countermeasures" (C3CM)[4] in 1981 and transitioning through "command and control warfare," "information warfare," "information operations," "inform and influence activities," and "information advantage," the Army has spent the greater part of the past 40 years trying to determine what information is and what it means for warfighting. The service has cycled and recycled through numerous attempts at doctrinal codification, and yet it seems to be in much the same place in 2023 as it was in the early 1990s: aware that the information revolution means something for warfare, yet unsure of what that something is, what it should be called, and what is the appropriate doctrinal response.

Why has the Army struggled to create an enduring doctrinal framework to describe the role of information in conflict? More broadly, why do militaries choose one doctrinal concept over other viable alternatives, and what determines whether a new doctrine will succeed or fail? This paper attempts to answer these questions by tracing the history of Army information doctrine from the late 1960s to the present. In so doing, it will offer a new perspective on the process of doctrinal reform that focuses on the role of intra-organizational competition between service sub-communities.

While external strategic conditions were decisive to doctrinal outcomes in the earliest phases of the information operations concept, over time, strategic conditions became less important than the preferences and interests of organizational actors when it came to influencing the process of doctrinal change. By the middle of the Global War on Terror, competing perspectives within the Army's relevant organizational sub-communities had produced irreconcilable disagreements that stalled the process of doctrinal reform and prevented the Army from adequately responding to a new strategic reality. The history of Army information operations therefore suggests that there are important organizational determinants of doctrine that may operate independently of the demands of the overarching strategic environment. While theories of war may dominate the conceptual phase of doctrine development, underlying organizational and fiscal realities often force difficult and suboptimal compromises with respect to the final product.

This paper proceeds in three parts. First, it reviews relevant scholarship on military innovation to explore existing explanations for how and why militaries develop new doctrines. This discussion of the existing explanations for doctrinal change is then followed by the introduction of a new, sub-organizational theoretical perspective. Second, this paper briefly summarizes the historical context from which Army information doctrine emerged, concluding with a series of service structural reforms in the mid-1990s.[5] Third, it examines the intra-organizational dynamics that were born of these structural reforms and that ultimately impeded efforts to change the Army's information doctrine during the Global War on Terror. The paper concludes with a discussion of relevant lessons that may inform how to approach current operational and strategic problems.

The Sources of Doctrine and the Causes of Military Change

What is military doctrine, and how and why is it created? Doctrine consists of the fundamental principles that guide the employment of military force.[6] It is important in that it "constitutes an organization's formal articulation of its understanding as to how it will fight the next war."[7] Doctrine is more than a set of written military manuals — it serves as the central principle around which a service mans, trains, equips, and organizes itself, and it provides a common language for members of a military organization.[8]

Doctrine is created in response to a given set of strategic conditions. Its purpose is to generate the most effective military response to the most likely range of security threats that a nation will face. When strategic conditions change — or when new technologies arrive that may alter the way in

[4] For a full list of terminology and abbreviations, see Appendix 1 in the online version of this article, which can be accessed here: https://tnsr.org/2023/01/the-organizational-determinants-of-military-doctrine-a-history-of-army-information-operations/

[5] For the purposes of space and theoretical exposition, this paper focuses the bulk of its historical analysis on information operations doctrine during the Global War on Terror. A more comprehensive historical account of the early years of Army information doctrine, to include the broader strategic and technological trends to which the doctrine was designed to respond, may be found in Sarah P. White, "The Origins and History of U.S. Army Information Doctrine," (Master's Thesis, U.S. Army Command and General Staff College, 2022).

[6] *Doctrine for the Armed Forces of the United States*, Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 1-0, March 25, 2013, incorporating Change 1 July 12, 2017, VI-3, https://irp.fas.org/doddir/dod/jp1.pdf.

[7] Suzanne C. Nielsen, *An Army Transformed: The U.S. Army's Post-Vietnam Recovery and the Dynamics of Change in Military Organizations*, The Strategic Studies Institute, 2010, 18, https://press.armywarcollege.edu/monographs/343/.

[8] Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars* (Ithaca, NY: Cornell University Press, 1985), 13; and John A. Nagl, *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Chicago: The University of Chicago Press, 2002), 7.

which a military can navigate these strategic conditions — it is expected that doctrine will change in response, and with it, certain key aspects of the military organization.[9]

However, doctrine is not a purely rationalist reaction to external circumstances. In addition to being constrained by resources,[10] doctrinal outcomes are filtered through and shaped by various non-rational influences whose effects on the development of new doctrines have been well documented by military innovation scholars.[11] These influences can be broadly categorized as political, organizational, and cultural schools of thought.[12]

The political school of thought tends to focus on the role of civilian leaders, who can direct the military to make doctrinal changes in response to new strategic conditions.[13] Those who fall within this school frame doctrinal change as primarily a principal-agent problem,[14] in which naturally stagnant military bureaucracies must be directed by civilian leaders to modify existing ways of doing things. Different political structures can result in unique patterns of military change,[15] while different civilian perspectives can result in directives that are more or less optimally suited to prevailing balance-of-power dynamics.[16] The doctrine that results represents an articulated solution to the challenges of a given strategic setting, as interpreted by a nation's political leadership.

However, the political argument for doctrinal change suffers from numerous shortcomings, not least of which is a failure to take into account the natural limitations — in expertise, confidence, and/or will — of the political "principal" as well as the unique organizational characteristics of the military "agent."[17] Various organizational explanations for military change have arisen to address these shortcomings. Drawing from organization theory and bureaucratic politics, these arguments emphasize both inter- and intra-service dynamics to explain when, why, and under what conditions militaries embrace change, as well as why those changes might succeed or fail. Critical to these perspectives is the role of competition, whether between services or within a service, in driving both how threats are interpreted and how those interpretations are used to gain advantage over bureaucratic adversaries.[18]

Complementing the organizational perspective, a third collection of arguments has focused on the

[9] In contrast to the early military innovation theorizers, it has become an empirically accepted fact that militaries can and do change regularly. These changes can range in their significance from ordinary or trivial to radical and sweeping. See Williamson Murray and Allan R. Millett, eds., *Military Innovation in the Interwar Period*, (Cambridge, UK: Cambridge University Press, 1996), who argue on page 5 that, "Innovation is natural and the result of a dynamic environment in which organizations must accept change if they are to survive."

[10] Andrew Bacevich in *The Pentomic Era* provides an excellent example of doctrine development as a result of resource constraints, similar to the Army's embrace of network-centric warfare as a foundational principle of force transformation in the mid-1990s. A.J. Bacevich, *The Pentomic Era: The U.S. Army Between Korea and Vietnam* (Washington, DC: National Defense University Press, 1986).

[11] This paper avoids the discussion of what does or does not comprise "military innovation." It instead concerns itself with those processes of doctrinal change that have implications for organizational strategy or structure. Military innovation literature provides the most comprehensive assessment of the drivers of military change, and so is seen as the most appropriate literature to review in this section. For more on the discussion of what constitutes military change, see Theo Farrell and Terry Terriff, eds., *The Sources of Military Change: Culture, Politics, Technology* (Boulder, CO: Lynne Reiner Publishers, 2002), 4–7.

[12] For different methods of categorization, see Nielsen, *An Army Transformed*; Janine Davidson, *Lifting the Fog of Peace: How Americans Learned to Fight Modern War* (Ann Arbor: The University of Michigan Press, 2010); Stuart Griffin, "Military Innovation Studies: Multidisciplinary or Lacking Discipline?" *Journal of Strategic Studies* 40, no. 1–2 (2017): 196–224, https://doi.org/10.1080/01402390.2016.1196358; and Adam Grissom, "The Future of Military Innovation Studies," *Journal of Strategic Studies* 25, no. 9 (2006): 905–34, https://doi.org/10.1080/01402390600901067.

[13] Posen, *Sources of Military Doctrine*; and Jack Snyder, *The Ideology of the Offensive* (Ithaca, NY: Cornell University Press, 1984).

[14] Nielsen, *An Army Transformed*, 20.

[15] Deborah D. Avant, *Political Institutions and Military Change* (Ithaca, NY: Cornell University Press, 1994), 9–18; and Peter Feaver, "Crisis as Shirking: An Agency Theory Explanation of the Souring of American Civil-Military Relations," *Armed Forces and Society* 24, no. 3 (1998): 421, https://doi.org/10.1177/0095327X9802400305.

[16] Avant, *Political Institutions*; and Elizabeth Kier, *Imagining War: French and British Doctrine Between the Wars* (Princeton, NJ: Princeton University Press, 1997), 21–24.

[17] Nielsen, *An Army Transformed*, 21–22.

[18] For perspectives on competition between services, see Bacevich, *The Pentomic Era*; Harvey M. Sapolsky, *Polaris System and Development: Bureaucratic and Programmatic Success in Government* (Cambridge, MA: Harvard University Press, 1972); Owen R. Cote, "The Politics of Innovative Military Doctrine: The U.S. Navy and Fleet Ballistic Missiles" (Ph.D. Dissertation, Massachusetts Institute of Technology, 1996). For perspectives on competition within a service, see Stephen P. Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991); B. Hayes and D. Smith, eds., *The Politics of Naval Innovation* (Newport, RI: U.S. Naval War College, 1994); Susan L. Marquis, *Unconventional Warfare: Rebuilding U.S. Special Operations Forces* (Washington, DC: Brookings Institute Press, 1997); Suzanne C. Nielsen, "Preparing for War: The Dynamics of Peacetime Military Reform," (Ph.D. Dissertation, Harvard University, 2003). On the interpretation of threats, see Thomas G. Mahnken, *Uncovering Ways of War: U.S. Intelligence and Foreign Military Innovation*, 1918–1941 (Ithaca, NY: Cornell University Press, 2002). On gaining bureaucratic advantage, see Sarah P. White, "Subcultural Influence on Military Innovation: The Development of U.S. Cyber Doctrine," (Ph.D. Dissertation, Harvard University, 2019), http://nrs.harvard.edu/urn-3:HUL.InstRepos:42013038.

role of culture in driving, preventing, or shaping change processes.[19] Culture consists of a set of shared beliefs, values, and assumptions that create persistent patterns of thinking among a group's members and shape expectations about standards of appropriate behavior. These beliefs, values, and assumptions form the scaffolding of a group's epistemic infrastructure: They not only influence how to interpret new information or events, but they also drive a shared understanding of what information or events are worth paying attention to. Cultural effects can work at the national, organizational, and sub-organizational level to influence both the fact of military change and the process by which it occurs.[20]

In addition to improving our understanding of when, why, and how militaries may adopt a new doctrinal concept, the cultural and organizational arguments offer an additional explanation as to why a new doctrinal concept might succeed or fail by highlighting the factors *internal* to a military organization that may affect the doctrine's reception. In particular, the cultural and organizational perspectives can help us to understand why a new doctrine might be rejected despite it being ordered by civilian or military leadership, and despite its evident appropriateness for a given strategic context.[21]

Adopting a Sub-Organizational Perspective

The political, organizational, and cultural arguments outlined above offer different answers to two questions that are fundamental to the process of doctrinal evolution: first, what influences how militaries interpret their strategic environments, and second, what influences how militaries respond to the challenges that are identified as a result of this interpretation. However, with few exceptions, most scholars continue to treat military organizations as monolithic entities that lack significant structural and cultural variation at the sub-organizational level.[22] This disregard for intra-organizational diversity risks undervaluing the critical role played by organizational sub-communities in shaping the processes by which doctrine develops.[23] Where organizational diversity is acknowledged, it is over-simplified as pure bureaucratic politics, which risks misunderstanding the nature of the actual mechanisms of competition that are at play.[24]

The history of Army information doctrine simultaneously affirms elements of the existing theoretical explanations of doctrinal reform while offering a new perspective on the critical role of organizational sub-communities as drivers — or inhibitors — of change. Specifically, it shows how the structural reforms that were necessary to modify and elevate the role of information within Army doctrine ultimately came to handicap the Army's ability to further transform that role when the strategic environment demanded it.[25] It did this by creating a cadre of information professionals who not only came to possess a bureaucratic self-interest in the preservation of their career field, but whose upbringing in that career field resulted in a unique and specific conceptual orientation toward the role of information in war. This perspective influenced

[19] Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford, CA: Stanford University Press, 2010); Andrew F. Krepinevich Jr., *The Army and Vietnam* (Baltimore: Johns Hopkins University Press, 1986); Farrell and Terriff, *The Sources of Military Change*; Theo Farrell, *Norms of War: Cultural Beliefs and Modern Conflict* (Boulder, CO: Lynne Rienner, 2005); Terry Terriff, "Innovate or Die: Organizational Culture and the Origins of Maneuver Warfare in the U.S. Marine Corps," *Journal of Strategic Studies* 29, no. 3 (2006): 475–503, https://doi.org/10.1080/01402390600765892; Theo Farrell, "The Dynamics of British Military Transformation," *International Affairs* 84, no. 4 (2008): 777–807, https://doi.org/10.1111/j.1468-2346.2008.00737.x; Kier, *Imagining War*; and White, *Subcultural Influence*.

[20] Adamsky, *The Culture of Military Innovation*; Austin Long, *The Soul of Armies: Counterinsurgency Doctrine and Military Culture in the U.S. and U.K.* (Ithaca, NY: Cornell University Press, 2016); Kier, *Imagining War*; Krepinevich, *The Army and Vietnam*; Farrell and Terriff, "Innovate or Die;" and White, *Subcultural Influence*.

[21] The Vietnam era produced numerous examples of failed or highly difficult civilian-directed organizational change, such as the presidentially directed creation of Army Special Forces and the Army's execution of strategy in Vietnam.

[22] The diversity of military organizations is typically acknowledged only as it concerns choices of bureaucratic self-preservation, rather than with respect to driving differences in conceptual orientation to warfare. Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd ed. (New York: Longman, 1999); Sapolsky, *Polaris System and Development*; and Owen R. Cote, "The Politics of Innovative Military Doctrine.

[23] Raphael D. Marcus briefly alludes to the role of intra-organizational competition as a trigger for military change in his study of the Israeli Defense Forces, but does not discuss the underlying processes or mechanisms in detail. See Raphael D. Marcus, *Israel's Long War with Hezbollah* (Washington, DC: Georgetown University Press), 8–9.

[24] Just as differences in individual leader backgrounds can influence foreign policy choices with respect to the use of force, so do differences in operational backgrounds influence the decisions that military leaders make with respect to the doctrines that guide force employment. For examples of the former phenomenon, see Michael C. Horowitz and Allan C. Stam, "How Prior Military Experience Influences the Future Militarized Behavior of Leaders," *International Organization* 68, no. 3 (2014): 527–59, https://doi.org/10.1017/S0020818314000046; Keren Yarhi-Milo, Joshua D. Kertzer, and Jonathan Renshon, "Tying Hands, Sinking Costs, and Leader Attributes," *Journal of Conflict Resolution* 62, no. 10 (2018): 2150–79, https://doi.org/10.1177/0022002718785693; and Cathy Xuanxuan Wu and Scott Wolford, "Leaders, States, and Reputations," *Journal of Conflict Resolution* 62, no. 10 (2018): 2087–117, https://doi.org/10.1177/0022002718786001.

[25] The case study of Army information doctrine thus presents a useful addendum to Stephen Rosen's explanation of both peacetime and wartime military reform.

how the Army's information professionals interpreted the strategic environment, as well as the range of doctrinal changes that they were willing to accept, in a way that acted independently of their need for bureaucratic self-preservation.

The information career field, in addition to implicitly shaping the conceptual orientations of personnel, eventually came to suffer from a *quality* problem that would have lasting consequences for future doctrine. Specifically, the mediocre quality of the field's recruited personnel limited their ability to either demonstrate information's new relevance on the battlefield or to advocate for a specific doctrinal perspective in a way that was institutionally resonant.[26] This struggle suggests that structural reform, in and of itself, is not enough to ensure that doctrinal change will succeed. If the organizations and individuals created to instantiate a new doctrine fail to convincingly demonstrate their worth to the broader institution, whether due to inadequate resourcing or to poor personnel quality, then their ability to advocate for new ways of war will be limited.[27] In this sense, both the quality of individuals selected into a new career field and how those individuals are resourced matter as much to the success of doctrinal reform as the creation of the career field itself.

The Army's information doctrine case study therefore offers a number of important conclusions for our understanding of doctrinal change processes. First, it suggests that intra-organizational competition over conceptual frameworks can be decisive to outcomes of doctrinal change. This competition results as much from intrinsic differences in conceptual orientations toward warfare as it does from the bureaucratic need for self-preservation. Differences in conceptual orientation can affect the process of doctrinal reform in two important ways: They can influence how a given strategic or technological context is interpreted, and, based on that interpretation, they can influence how well a new doctrine is received within the force. Both effects can work to produce a doctrine that is sub-optimally matched to the overarching strategic conditions or to the central operational problem that a military might face.

However, a doctrine that *is* optimally suitable to a given set of strategic conditions may still be rejected by different sub-communities within the institution, and thus may ultimately fail. This phenomenon, evident during the Global War on Terror era of Army information doctrine, suggests that the primary determinant of a doctrine's success at any given point in history may not necessarily be its level of strategic appropriateness, but the extent to which it fits with the prevailing institutional culture and meets the dominant organizational interests. The implication of this finding is that there are significant differences between what is conceptually possible and what is organizationally acceptable for any given doctrinal framework. Finally, the Army information doctrine case study suggests that the structural reforms that are necessary for an initial doctrinal change to succeed can have second- and third-order effects that may preclude further doctrinal refinement as conditions evolve.

The Historical Context of Army Information Doctrine

1968–1991: Waging War on the Electronic Battlefield

By the late 1960s, advances in technology had led to the proliferation of electronic devices on the battlefield.[28] The Army's experience in Vietnam revealed the potential of these devices and their underlying information technologies, from networked sensors and electronic intelligence to computerized information processing and advancements in radio encryption.[29] In 1969, Army Chief of Staff Gen. William Westmoreland referenced the existence of an "electronic battlefield" and argued that future wars would be defined by "data links, computer assisted intelligence evaluation, and automated fire control."[30]

Throughout the 1970s and into the early 1980s, the Army saw in this advanced information technology what they had embraced in tactical nuclear

[26] A similar phenomenon was evident in the Air Force's decision to nominally create a cyber career field by relabeling its communicators. Their early struggle to demonstrate an appropriate level of technical competence or cyber-specific expertise caused the career field — and thus the service's overall investment in cyberspace operations — to struggle.

[27] As Nielsen states, "In order to have political power in the military … innovators must have the credibility that comes with traditional service credentials." Nielsen, *An Army Transformed*, 14.

[28] William C. Westmoreland, *Addresses by General W. C. Westmoreland, Chief of Staff, United States Army,* Volume IV, July 3, 1969 – December 16, 1969 (Washington, DC: Government Printing Office, 1973), 93.

[29] Christopher W. Lowe, *From 'Battle' to the 'Battle of Ideas': The Meaning and Misunderstanding of Information Operations*, School of Advanced Military Studies, 2010, https://apps.dtic.mil/sti/pdfs/ADA536456.pdf. Concurrently, the experience of other armies also suggested the potential of electronics and electronic warfare, such as that of the Israelis in the Six Day War of 1967. See David G. Chizum, *Soviet Radioelectronic Combat* (Boulder, CO: Westview Press, 1985), 47.

[30] Lowe, *From 'Battle' to the 'Battle of Ideas'*, 5–6.

weapons two decades prior: a way to offset the Soviet Union's numerical advantage in a conventional war in Europe.[31] However, the integration of these advanced technologies into doctrine required a full reimagining of the Army operating concept. The result was AirLand Battle, which prioritized advanced information technology and automated command-and-control systems as a way to optimize the application of scarce assets against a numerically superior foe.[32] AirLand Battle depended upon a constellation of advanced technologies that could locate forces deep in the enemy rear and then electronically pass that information to units that were capable of attacking them.[33] The doctrine put a high premium on advanced electronic technology and survivable command-and-control systems that preserved the ability to synchronize combat forces and concentrate combat power at the decisive time and place.[34]

However, command-and-control systems had to meet two criteria in order to be effective under the AirLand Battle construct. First, they had to function more quickly than enemy systems, and, second, they had to be resilient and survivable in the face of enemy electronic warfare.[35] These twin criteria led to an embrace of computer automation as a way to increase the speed with which information could be acquired, processed, and distributed.[36] The turn toward computer automation caused a subtle shift in how the Army viewed information itself as well as its relation to other Army functions.[37] Whereas historically, information had been seen as a tool to achieve surprise over the enemy and to facilitate the aggregation of combat power, the incorporation of automation into command-and-control platforms and weapons systems solidified a new interpretation of information as the fuel required to feed and maintain the overarching command-and-control system, which itself was the central "essential" requirement of AirLand Battle.[38] Accordingly, the term "information" began to take on a technological intonation due to its growing affiliation with computers and automation.

The importance of command and control to the Army's operating concept, along with the dependence of command and control on computer technology, led to the development of the earliest recognizable precursor to information operations: command, control, and communications countermeasures.[39] Formally codified in Army doctrine

[31] For more on tactical nuclear weapons, see Bacevich, *The Pentomic Era*.

[32] Department of the Army, *Operations*, Field Manual (FM) 100-5, (Washington, DC: Army Publishing Directorate, 1982). Of note, AirLand Battle was based upon the concept of "deep attack" or "deep battle" first developed by Soviet military thinkers in the 1930s. See Earl F. Ziemke, "The Soviet Theory of Deep Operations," *Parameters* 13, no. 1 (1983): 23–33, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1339&context=parameters. See also Richard Simpkin, "From Broad Front to Deep Battle," in *Deep Battle: The Brainchild of Marshal Tukhachevskii* (London: Brassey's Defence Publishers, 1987), 33–52.

[33] Walter E. Kretchik, *U.S. Army Doctrine: From the American Revolution to the War on Terror* (Lawrence: University of Kansas Press, 2011), 204.

[34] Joe Halleran, "Command and Control Interoperability," *Military Review* 66, no. 10 (October 1986): 38–49, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/259/rec/7. On synchronization, see John B. Rogers, "Synchronizing the AirLand Battle," *Military Review* 66, no. 4 (April 1986): 65–71, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/254/rec/10; Dennis H. Long, "Command and Control: Restoring the Focus," *Military Review* 61, no. 11 (November 1981): 44–48, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/342/rec/12. On command and control, see Starry, "Command and Control."

[35] Robert W. Zawilski, "Computers: An Aid to Command and Control," *Military Review* 61, no. 12 (December 1981): 51–56, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/343/rec/3. Field Manual 100-5 (1986) states that "The ultimate measure of command and control effectiveness is whether the force functions more effectively and more quickly than the enemy." See page 22. Walter Kretchik affirms this emphasis on speed and agility as a way to exploit enemy weaknesses and frustrate enemy plans. Walter E. Kretchik, *U.S. Army Doctrine: From the American Revolution to the War on Terror* (Lawrence: University of Kansas Press, 2011), 206.

[36] Zawilski, "Computers;" Clayton R. Newell, "Fog and Friction: Challenges to Command and Control," *Military Review* 67, no. 8 (August 1987): 18–26, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/521/rec/9; Forrest G. Clark, "The Commander and Battlefield Automation," *Military Review* 64, no. 5 (May 1984): 68–71, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/276/rec/9; Dean R. Anderson, "Modernizing Army Command and Control," *Military Review* 70, no. 7 (July 1990): 2–10, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/538/rec/10; and Wayne Knudson, "The Future of C2," *Military Review* 70, no. 7 (July 1990): 18–24, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/538/rec/10.

[37] Newell, "Fog and Friction;" and Thomas B. Giboney, "Commander's Control from Information Chaos," *Military Review* 71, no. 11 (November 1991): 34–38, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/494/rec/1.

[38] On historic views of information, see David V. Boslego, *The Relationship of Information to the Relative Combat Power Model in Force XXI Engagements*, School of Advanced Military Studies, 1995, https://apps.dtic.mil/sti/pdfs/ADA309699.pdf. On the new interpretation of information, see Newell, "Fog and Friction." On the centrality of command and control to AirLand Battle, then-commander of U.S. Army Training and Doctrine Command, Gen. Don Starry, highlighted this point in 1981, arguing, "No element of [the AirLand Battle] concept is more essential to the development of a credible warfighting capability than command and control." Starry, "Command and Control."

[39] Command, control, and communications countermeasures (C3CM) was preceded by the doctrinal concept of C3, or command, control, and communications. The 1976 edition of Field Manual 100-5, titled *Operations*, established the twin abilities to conduct command, control, and communications and to disrupt the enemy's ability to conduct command, control, and communications as essential to the successful execution of Army operations. Command, control, and communications countermeasures evolved after a series of Defense Department studies that ran from 1975 to 1978 and were designed to explore the implications of command, control, and communications for a fight against the Soviet Union. Department of the Army, *Operations*, Field Manual (FM) 100-5 (Washington, DC: Army Publishing Directorate, July 1, 1976).

in 1981, it was designed to protect the critical function of command and control by hardening the technologies it depended upon and to deny adversaries the same ability through "the integrated use of operations security, military deception, jamming, and physical destruction, supported by intelligence."[40] Command, control, and communications countermeasures envisioned a warfighting approach that focused on disrupting the enemy's ability to command its forces as a way to offset a numerical disadvantage.[41]

The impact of advanced information technology on the outcome of Desert Storm led to a period of intense theorizing about the extent to which the information age had changed the character of warfare.

In 1991,[42] Operation Desert Storm offered a resounding proof of concept for what had become the central thesis of Army doctrine development: that attacking adversary command-and-control systems would be the key to success in future combat.[43] Called a "knowledge war" by the Army chief of staff and an "information war" by policy commentators, Desert Storm featured the unprecedented integration of advanced technologies — ranging from networked intelligence sensors, communications systems, electronic warfare platforms, space-based capabilities, and the mass media — to achieve decisive victory over the larger Iraqi forces.[44] These technologies were deliberately leveraged as part of a broader information warfare campaign designed to decapitate the Iraqi army's command, control, and communications;[45] deceive Iraqi forces;[46] and ultimately prevent the Iraqi army from massing its numerically superior land forces at the point of the main attack.[47]

The impact of advanced information technology on the outcome of Desert Storm led to a period of intense theorizing about the extent to which the information age had changed the character of warfare.[48] While scholars disagreed on terminology — with references to "information-age warfare," "information warfare," "cyber war," "sixth-generation warfare," "third-wave war," and a "revolution in military affairs" presented with equal abandon in scholarly discourse — they generally agreed that technological improvements

[40] W. Graham Claytor, *Command, Control, and Communications (C3) Countermeasures*, Department of Defense Directive 4600.4, Aug. 27, 1979, enclosure 1. The Army released a classified pamphlet on command, control, and communications countermeasures in 1981 called *Joint Operational Concept for Command, Control, and Communications Countermeasures*, TRADOC Pamphlet 525–7.

[41] Charles F. Smith, "Command, Control, and Communications Countermeasures," *Military Review* 63, no. 1 (January 1983): 67–74, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/290/rec/12. Of note, the fact that Army command, control, and communications countermeasures doctrine in the 1980s was classified did little to encourage the concept's realization across the broader force. The decade of the 1980s was marked by confusion as to what command, control, and communications countermeasures was and how it fit within the Army way of war. See Smith, "Command, Control, and Communications Countermeasures."

[42] 1991 also featured the Army's release of an unclassified field manual on command, control, and communications countermeasures. Department of the Army, *Multi-Service Procedures for Command, Control, and Communications Countermeasures*, Field Manual (FM) 90-24 (Washington, DC: Government Printing Office, 1991), https://cdm16040.contentdm.oclc.org/digital/collection/p4013coll9/id/620/rec/11.

[43] Department of the Army, *Information Operations*, Field Manual (FM) 100-6 (Washington, DC: Government Printing Office, August 1996), chap. 3, https://irp.fas.org/doddir/army/fm100-6/index.html. See also Edward Mann, "Desert Storm: The First Information War," *Air Power* 8, no. 4 (1994): 4–14, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-08_Issue-1-Se/1994_Vol8_No4.pdf.

[44] Alan Campen, ed., *The First Information War* (Fairfax, VA: AFCEA International Press, 1992).

[45] Mann, "Desert Storm," 8; and George J. Franz, *Information: The Fifth Element of Combat Power*, School of Advanced Military Studies, 1996, 19, 25, https://apps.dtic.mil/sti/pdfs/ADA314297.pdf.

[46] On public affairs, see Richard F. Machamer Jr., "Avoiding a Military-Media War in the Next Armed Conflict," *Military Review* 73, no. 4 (April 1993): 43–54, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/463/rec/11. On psychological operations, see Franz, *Information*, 24, 9.

[47] Franz, *Information*, 17.

[48] For examples of theorizing within the Army, see Gordon R. Sullivan and James M. Dubik, *War in the Information Age,* Strategic Studies Institute, 1994, https://apps.dtic.mil/sti/pdfs/ADA281097.pdf; Randall G. Bowdish, "The Revolution in Military Affairs: The Sixth Generation," *Military Review* 75, no. 6, (Nov-Dec 1995): 26–33, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/447/rec/1; and Gordon R. Sullivan, "A Vision for the Future," *Military Review* 75, no. 3 (May–June 1995): 5–14, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/444/rec/2; Richard F. Ricciarelli, "The Information and Intelligence Revolution," *Military Review* 75, no. 5 (Sept–Oct 1995): 82–87; Kerry A. Blout and Lauren D. Kohn, "C2 Warfare in FM 100-6," *Military Review* 75, no. 4 (July–Aug. 1995): 66–69, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/446/rec/6; Wallace C. Arnold and Thomas H. Killion, "MANPRINT Battle Command and Digitization," *Military Review* 75, no. 3 (May–June 1995): 48–57, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/444/rec/2; Antulio J. Echevarria II and John M. Shaw, "The New Military Revolution: Post-Industrial Change," *Parameters* 22, no. 1 (1992), https://apps.dtic.mil/sti/pdfs/ADA528178.pdf. For examples of theorizing outside the Army, see Eliot A. Cohen, "A Revolution in Warfare," *Foreign Affairs* 75, no. 2 (March–April 1996): 37–54, https://doi.org/10.2307/20047487; David Jablonsky, "U.S. Military Doctrine and the Revolution in Military Affairs," *Parameters* 24, no. 1 (1994), https://doi.org/10.55540/0031-1723.1711; Kenneth F. McKenzie Jr., "Elegant Irrelevance: Fourth Generation Warfare," *Parameters* 23, no. 1 (1993), https://apps.dtic.mil/sti/pdfs/ADA515609.pdf; James R. Fitzsimonds, "The Coming Military Revolution: Opportunities and Risks," *Parameters* 25, no. 1 (1995), https://apps.dtic.mil/sti/pdfs/ADA528503.pdf; and Michael J. Mazarr, "The Revolution in Military Affairs: A Framework for Defense Planning," Strategic Studies Institute, June 10, 1994, https://apps.dtic.mil/sti/pdfs/ADA281758.pdf.

had accelerated the importance of information to war in at least four ways.[49]

First, intelligence, surveillance, and reconnaissance technology extended the *range* of the battlefield by expanding the distance from which adversaries could be observed and targeted. Second, computation and communications technology accelerated the *tempo* and *synchronization* of operations by increasing the rate at which information reached commanders.[50] Third, the integration of advanced technology into weapons systems increased the *precision* of their delivery and their effective lethality. Success in an information-age war would therefore go to the side that could acquire, process, distribute, and act upon information faster than its opponent. Finally, Desert Storm also demonstrated the operational relevance of the global mass *media* through a public relations campaign that was heralded as the "greatest hands-on application of media relations ever."[51]

The combined effect of these conclusions ushered in a new theory of technological warfare in which knowledge and information were as important to success as weapons and tactics. Information became not simply something that would offer one side an advantage over the other, but a critical commodity that was necessary for the entire system of war to function.[52] As such, its maintenance would require the same level of command attention as traditional combat resources.[53] Just as the industrial age required a new focus on degrading the enemy's war-making capacity, so the information age required a new focus on disrupting the adversary's ability to receive, process, and disseminate information.[54] Army information doctrine arose in response to these challenges and opportunities.

1991–2001: Warfare in the Information Age

The Army's efforts to craft an information doctrine began in earnest in 1991. Two major events transpired that year that would come to have a significant effect on this process. First, the overwhelming coalition success in the Gulf War affirmed the effectiveness of command, control, and communications countermeasures. In so doing, it cemented the status of information and information technology as the critical enablers of future war. Second, the collapse of the Soviet Union reshaped the global order into an American-led unipolar system, which deprived the Army of its primary peer competitor and led to an immediate reduction in defense spending.[55] As a result, the Army had to reimagine its operating concept for a world in which it would not know when or where the next fight would take place or against whom it would be fought, and it had to do so with fewer resources. The ability to use its forces efficiently became vital.

"Information warfare" emerged in the early 1990s as a central component of the Army's vision for how it would fight in this new strategic context.[56] Information warfare concerned the provision of timely and accurate information to friendly forces while corrupting or denying adversary information systems.[57] It required a force that was capable of leveraging information to economize the application of combat power; operate at a higher tempo than the enemy; and achieve victory quickly, decisively, and at minimal cost.[58] Gaining and maintaining access to information would thus become the main imperative for future operations.[59]

Initially driven by Gen. Gordon R. Sullivan, who

[49] Edward Waltz, *Information Warfare: Principles and Operations* (MA: Artech House, 1998), 10.

[50] Campen, ed., *The First Information War*, ix.

[51] Machamer, "Avoiding a Military-Media War."

[52] Campen, ed., *The First Information War*, xi.

[53] W.B. Cunningham and M.M. Taylor, "Information for Battle Command," *Military Review* 74, no. 11 (1994): 81, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/459/rec/5.

[54] Sullivan and Dubik, *War in the Information Age*. See also Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston, MA: Little and Brown, 1993).

[55] Numerous sources from internal Army discussions in 1991 and 1992 discuss downsizing and budget cuts as a critical factor in determining how Army doctrine should change. For example, see U.S. Army Training and Doctrine Command, "The Army in Transition: The Evolution of AirLand Battle for a Strategic Army," Presentation, Fort Monroe, VA, 1991, slide 8, 29, which places its discussion of doctrinal change in the context of Army downsizing from 1990 to 1995. See also, Combined Arms Command, "FM 100-5: Evolution or Dynamic Change?" Information brief, 1992, slide 29, which lists "Army downsizing principles" as a consideration for Field Manual 100-5.

[56] U.S. Army Training and Doctrine Command, "Strategic Vision for Winning the Information War," Jan. 10, 1994.

[57] U.S. Army Training and Doctrine Command, "Strategic Vision for Winning the Information War," 6. The service formally defined information warfare in 1994 as "actions taken to preserve the integrity of one's own information system from exploitation, to corrupt or destroy an adversary's information system, and, in the process, to achieve an information advantage in the application of force." U.S. Army Training and Doctrine Command, *Force XXI, Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century*, TRADOC Pamphlet 525-5 (Fort Monroe, VA: U.S. Army Training and Doctrine Command, Aug. 1, 1994), Glossary-5, https://apps.dtic.mil/sti/citations/ADA402580.

[58] U.S. Army Training and Doctrine Command, *Force XXI Operations*.

[59] U.S. Army Training and Doctrine Command, *Force XXI Operations*, 3-2.

began his tenure as the future-focused Army chief of staff in 1991, the Army spent the 1990s pursuing this vision of information-age warfare through a series of doctrinal, organizational, and personnel changes that would come to define the service's approach to information for the next three decades. In 1993, the Army identified "winning the information war" as one of its top modernization priorities.[60] In 1994, an initiative called "Force XXI" pursued this priority through a force digitization initiative that brought digital communication networks and new "internetted" systems to lower tactical levels.[61] Force XXI envisioned a smaller, lighter, faster force that could use information technology to substitute the efficient application of precise firepower for the industrial-era practice of massing forces.[62] However, it also produced new dependencies on information technology, introduced new vulnerabilities as a result of those dependencies, and reinforced the technological orientation of the service's nascent information doctrine.

In 1996, the Army produced its first information warfare field manual, Field Manual 100-6, *Information Operations*.[63] In a noteworthy departure from the joint force, the manual abandoned the term "information warfare," which it saw as too narrowly focused on the impact of information during conflict and therefore insufficient for the multiple roles and missions that were expected of the post-Cold War Army. Instead, the Army adopted the term "information operations," which it defined as those activities that "enable, enhance, and protect, the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations."[64] Functionally, information operations encompassed the five elements that had previously comprised command, control, and communications countermeasures — operations security, military deception, electronic warfare, psychological operations, and physical destruction — along with civil affairs and public affairs.[65]

Field Manual 100-6 built upon several years of conceptual work that sought to integrate lessons learned from Desert Storm with the service's growing vision for information-age warfare.[66] It advanced the Army's thinking on information in several important ways. First, it presented information operations not as a new capability, but as a new approach to military operations that focused on controlling and exploiting information to gain an operational advantage. This approach would synchronize several information-based military functions that had been previously stove-piped and independent from one another.[67] The integrating role of information operations spoke to one of the primary lessons learned from Desert Storm, which was the need for a mechanism to coordinate competing methods of information dissemination and avoid information fratricide.[68]

Meanwhile, the purpose of information operations as something that would create an operational advantage affirmed information as an essential enabler of combat power, rather than as something

[60] Arnold and Killion, "MANPRINT Battle Command."

[61] U.S. Army Training and Doctrine Command, *Force XXI Operations*, 3-2, 3-4. See also Morris J. Boyd and Michael Woodgerd, "Force XXI Operations," *Military Review* 74, no. 11 (1994): 17–28, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/459/rec/5.

[62] The Army spent much of the latter 1990s pursuing a series of force modernization efforts that were based upon the initial Force XXI vision of a small, agile, networked force. Thomas K. Adams, *The Army After Next: The First Postindustrial Army* (Westport, CT: Praeger Security International, 2006), 8. Beginning with Sullivan in 1994 and ending with Gen. Peter Schoomaker in 2003, four consecutive Army chiefs of staff worked to advance the vision of a smaller, lighter, faster force that could leverage information technology to substitute the efficient application of precise firepower for industrial-era mass. The names of each initiative were: Sullivan's "Force XXI," Gen. Dennis J. Reimer's "Army After Next," Gen. Eric Shinseki's "Objective Force," and Schoomaker's "modular brigade combat teams."

[63] Department of the Army, *Information Operations*, Field Manual (FM) 100-6.

[64] Department of the Army, *Information Operations*, FM 100-6, 2–3. Of note, "information operations" was first introduced and defined in 1994. See U.S. Army Training and Doctrine Command, *Force XXI Operations*, Glossary-4.a

[65] Center for Army Lessons Learned, "Task Force Eagle Information Operations: IO in a Peace Enforcement Environment," *CALL Newsletter*, no. 99-2 (January 1999), 2. By the time Field Manual 100-6 was published, command, control, and communications countermeasures had been replaced in joint doctrine by "command and control warfare," or C2W. See Donald J. Atwood, *Electronic Warfare (EW) and Command and Control Warfare (C2W) Countermeasures*, Department of Defense Directive 3222.4, July 31, 1992, incorporating change 2, Jan. 28, 1994, https://biotech.law.lsu.edu/blaw/dodd/corres/pdf/d32224wch2_073192/d32224p.pdf.

[66] U.S. Army Training and Doctrine Command, "Information Brief to LTG Holder on FM 100-6, Information Operations," PowerPoint Presentation, Fort Leavenworth, KS, October 1995. This document describes Field Manual 100-6 as the "linchpin from today's operations to future operations." "Information Operations: The Plan" from March 1995 describes information operations as fulfilling the vision of third-wave warfare. U.S. Army Command and General Staff College, "Information Operations: The Plan," PowerPoint Presentation, Fort Leavenworth, KS, March 1995.

[67] Center for Army Lessons Learned, "Task Force Eagle Information Operations," 1.

[68] White, "Subcultural Influence," 72. Information fratricide refers to instances in which different sources of information contradict one another, such as operations security efforts conflicting with military deception campaigns or public affairs messages unintentionally countering those put forth by psychological operations.

that could be leveraged independently of military operations.[69] Both organizationally and conceptually, information operations would be integrated with the Army's targeting process as a way to affect the enemy via non-lethal means.[70] In this, the Army resolved several of the key debates that had defined the initial drafting phase: whether information operations should be a separate or an integrated concept,[71] its relation to more traditional elements of combat power such as maneuver and fires,[72] and the extent to which information operations should focus at the strategic versus the tactical or operational levels of war.[73]

The Army's new information operations doctrine and organizations were put to the test in Bosnia, where the Army provided support to NATO in enforcing the Dayton Peace Accords.

In addition, Field Manual 100-6 established information operations as, fundamentally, operations. This was an important, if nuanced, distinction that spoke to concerns about the intelligence community having been designated as the stewards of information operations.[74] When the vice chief of staff first tasked U.S. Army Training and Doctrine Command with developing a concept for information warfare in November of 1993, it in turn gave this job to Fort Huachuca and the Army's intelligence community. This decision was due to the latter's combination of technical and targeting skills, its history with electronic warfare, and its preexisting organizational structures and relationships within the joint command-and-control warfare world.[75]

However, the technical skills derived from the intelligence community's role in signals intelligence and electronic warfare reinforced the development of an information warfare doctrine that favored technology and technological solutions over cognitive or psychological ones. The practical challenges of non-combat operations in the Balkans in the late 1990s would continue to encourage this technological favoritism: Even while the supported units valued information operations as a tool to shape perceptions and win popular influence, the information operations field support teams tended to focus on technical solutions to the challenges of information management, network connectivity, and the ability to access state-side intelligence assets from forward-deployed positions.[76]

The intelligence community's ownership of information warfare also resulted in the creation of organizational relationships that reinforced these preexisting technological instincts and excluded outside perspectives. On May 8, 1995, the Army created the Land Information Warfare Activity, a new organization that would serve as a focal point for land-based information operations.[77] Administratively subordinate to the U.S. Army Intelligence and Security Command,[78] the Land Information

[69] Michael D. Starry and Charles W. Arneson Jr., "FM 100-6: Information Operations," *Military Review* 76, no. 6 (1996): 3–15, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/439/rec/2; U.S. Army Intelligence Center, "Information Operations: Defining the Concept," PowerPoint Presentation, Fort Huachuca, AZ, 1995, states that information operations "is more than cyberwar weaponry and C2 attack."

[70] Department of the Army, *Information Operations*, FM 100-6, Appendix D Staff Organization and Training.

[71] U.S. Army Command and General Staff College, "FM 100-6, 'Information Operations, Proposed Issues for the DRAG," PowerPoint Presentation, Fort Leavenworth, KS, Oct. 23, 1995.

[72] U.S. Army Intelligence Center, "Information Operations: Defining the Concept." Field Manual 100-6 states the following about information operations as firepower: "The MIE [military information environment] equivalent of firepower, already included in doctrine, is the employment of lethal and nonlethal, direct and indirect capabilities through C2W [command and control warfare]. C2W uses deception, PSYOP [psychological operations], EW [electronic warfare], OPSEC [operations security], and destruction to attack an adversary's capabilities. … US Armed forces have always employed these capabilities, but they were recently integrated into operations under C2W." Department of the Army, *Information Operations*, FM 100-6, 1-12.

[73] U.S. Army Training and Doctrine Command, "Information Brief to LTG Holder," slide 61, defined the Army's perspective on information operations as "more focused at operational and tactical level" and focused on "supporting, enabling, enhancing."

[74] U.S. Army Intelligence Center, "Information Operations: Defining the Concept."

[75] Command and General Staff College, "Information Operations: The Plan." See also Department of the Army, *Division Intelligence and Electronic Warfare Operations*, Field Manual (FM) 34-10 (Washington, DC: Army Publishing Directorate, November 1986); and Department of the Army, *Echelons Above Corps (EAC) Intelligence and Electronic Warfare Operations*, Field Manual (FM) 34-37 (Washington, DC: Army Publishing Directorate, January 1991).

[76] White, "Subcultural Influence," 78.

[77] "Activation of US Army Land Information Warfare Activity," Memorandum from Department of the Army, Washington, DC, to ARSTAF, May 8, 1995; Paul E. Blackwell et al., "The U.S. Army Intelligence and Security Command's Land Information Warfare Activity," Memorandum of Understanding Among Deputy Chief of Staff for Operations and Plans and Deputy Chief of Staff for Intelligence and Director of Information Systems for Command, Control, Communications, and Computers and Commander, U.S. Army Intelligence and Securities Command, March 24, 1995.

[78] Of note, the Army's command, control, and communications countermeasures organization that had been created in the mid-1980s — the Studies and Analysis Activity — reported directly to the Army staff.

Warfare Activity was comprised primarily of intelligence and communications personnel who received extensive technical training both in government and industry.[79] They were organized into a combination of field support teams that provided intelligence operations planning support to deployed units and vulnerability assessment teams that secured information networks and systems.[80]

Over time, the Land Information Warfare Activity — which in 2002 became 1st Information Operations Command — would come to favor the pursuit of network security, network effects, and technical solutions to achieve information dominance over the more cognitive aspects of information warfare, such as psychological operations and deception. This preference would become so pronounced that, in 2002, the information operations community struggled to convince the Army that its scope went beyond computer network operations.[81] These intelligence community relationships and their technical consequences would continue after the transfer of information operations ownership from U.S. Army Training and Doctrine Command to the Combined Arms Center in 1996, a move that effectively shifted responsibility for doctrine development from the intelligence community to the maneuver community.[82] Given the historic relationship between information operations and intelligence, Field Manual 100-6's assertion of information operations as *operations*, rather than something that supported operations, was intended to reinforce the notion of information operations as both conceptually and operationally different from intelligence.

The Army's new information operations doctrine and organizations were put to the test in Bosnia, where the Army provided support to NATO in enforcing the Dayton Peace Accords. Subsequent experimentation with the application of information operations to non-combat operations introduced a subtle, yet pivotal, shift in the information operations concept.[83] On the one hand, the experience of Task Force Eagle legitimized information operations as an essential component of military operations and the main effort of stability operations.[84] The information campaign in Bosnia, waged jointly by psychological operations and public affairs "24 hours a day," was considered the main effort of division operations and the most effective method of non-lethal influence available.[85]

On the other hand, however, the very importance of information operations to peacekeeping activities caused the army to expand its sense of how information ought to be used and applied in future conflict. The success of Task Force Eagle depended less on military force than on convincing participants to accept the legitimacy of a political settlement. Information transitioned from a critical enabler of combat operations and a potential method of disrupting enemy command and control to a mechanism for the non-lethal engagement of populations and key decision-makers. The Army's experience in the Balkans thus had the twofold effect of reinforcing the necessity of information operations while modifying the breadth of the doctrine's application.

The total effect of information operations in Bosnia led to an increased appetite for information operations across the force. In 1997, the Army created the FA30 information operations career field to meet the new demand.[86] However, the creation of this career field had several consequences that would come to affect intra-organizational competition over the next decade. First, because the career field was a functional area, rather than a traditional branch, it lacked general officer representation, which made it increasingly difficult for the community to advocate for itself amid competing

[79] White, "Subcultural Influence," 76.

[80] White, "Subcultural Influence," 77.

[81] "Information Operation Requirements Review Council (RCC)," PowerPoint Presentation, Fort Leavenworth, KS, November 2002.

[82] Joe N. Ballard, "Information Operations Proponency," Memorandum for Commander, U.S. Army Combined Arms Center and Fort Leavenworth, U.S. Army Training and Doctrine Command, Fort Monroe, VA, June 19, 1996.

[83] Center for Army Lessons Learned, "Operation Joint Endeavor, Bosnia-Herzegovina, Task Force Eagle Continuing Operations," Initial Impressions Report, September 1996, 29; Center for Army Lessons Learned, "Operation Joint Guard, Bosnia-Herzegovina, Task Force Eagle Operations," Initial Impressions Report, March 1998; Center for Army Lessons Learned, "Operation Joint Guard, Bosnia-Herzegovina, MND(N) and SFOR: Information, Infantry, Engineer, and Medical Operations," Initial Impressions Report, April 1998; and Stephen W. Shanahan and Garry J. Beavers, "Information Operations in Bosnia," *Military Review* 77, no. 6 (1997): 53–62, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/430/rec/2.

[84] White, "Subcultural Influence," 79–80. Information operations integration also became a core criterion for passing the Army's large-scale warfighter exercises, which served as validation tests for the proficiency of division and corps commanders.

[85] Center for Army Lessons Learned, "Operation Joint Endeavor, Bosnia-Herzegovina, Task Force Eagle Continuing Operations," Initial Impressions Report, March 1997, 13; Center for Army Lessons Learned, "Operation Joint Guard," April 1998, 8; and Center for Army Lessons Learned, "Operation Joint Guard," March 1998, 15.

[86] Command and General Staff College, "Functional Area 30 (Information Operations) 'Smart' Book," PowerPoint Presentation Fort Leavenworth, KS, Feb. 5, 1999.

doctrinal perspectives.[87] Second, by the early 2000s, the career field had developed a tendency to attract mediocre officers who lacked the professional attributes required to integrate into maneuver staffs or to sell the concept of information operations to a maneuver audience.[88] Third, the creation of this career field resulted in the eventual replacement of the community's previous training model — which was informal, unstructured, and requirements-driven — with a single, standardized 12-week training program that emphasized staff processes at the expense of technical expertise or creative thinking.[89] The information operations officers who emerged from this program were more beholden to the staff processes in which they had been trained than to the type of independent critical thinking, intellectual ingenuity, and technical expertise that had marked information operations as a field in the late 1990s. The result was a career field that lacked institutional credibility and struggled to sell its vision.

Competing Conceptual Frameworks

2001–2016: An Era of Persistent Conflict

The period from 2001 to 2016 was one of the most operationally intense periods in U.S. Army history. It began with the successive toppling of authoritarian governments in Afghanistan and Iraq. The campaigns that resulted in these victories — defined by the use of smaller, agile forces empowered by information technology and precision firepower — were seen by senior defense officials as a resounding vindication of the information-age warfare ideas that had defined the Defense Department's transformation over the previous decade.[90]

By 2004, however, the limitations of this military transformation had become evident as the situations in both Iraq and Afghanistan deteriorated into messy sectarian conflict and violent insurgency.[91] The Army responded to this challenge by launching an ambitious overhaul of its force design that, it was hoped, would enable the service to more efficiently maximize its limited combat power across multiple theaters of war.[92] Called "modularity," this reorganization replaced divisions as the Army's central unit of action with modular brigade combat teams, whose comparatively reduced size and fighting power were augmented by advanced information technology and digitization.[93] Information technology would enhance the combat power of modular brigade combat teams by creating improved situational awareness that expanded the combat effectiveness of smaller, networked formations.[94]

However, while the Army doubled down on information technology in its force design, its information operations doctrine began to evolve in the opposite direction. In 2001, the *Quadrennial Defense Review* listed information operations as one of six operational goals for the Defense Department's 21st-century transformation and required the services to treat information operations as a core competency of future forces.[95] In 2002, the Army initiated a wholesale reexamination of its information operations doctrine in response to this

[87] White, "Subcultural Influence," 67.

[88] White, "Subcultural Influence," 91.

[89] White, "Subcultural Influence," 92. The 12-week course was finalized around 2008, which meant that there was no formalized information operations training for FA30s for the first several years of their existence.

[90] Adams, *Army After Next*, 157. The Taliban was ousted from power in roughly five weeks after the start of combat operations, while U.S. forces captured Baghdad in 21 days — less than half the time of the 1991 Gulf War with fewer than one-third the number of strikes and one-tenth the number of bombs. It should be noted that, as with Desert Storm, things were not so neat on the ground as they appeared in the official narrative. Units often suffered poor connectivity as they outran the range of high-bandwidth communications systems and relays. On more than one occasion, units were attacked while they stopped to wait for slow downloads. As a general rule, situational awareness was excellent at division level and above but very poor among frontline commanders. Adams, *Army After Next*, 177. Combined with the invasion's regression into sectarian conflict, many in the Army mocked the Defense Department's "victory" narrative.

[91] The failure of the military to achieve relevant dominance or to otherwise coerce the adversary into a certain set of behaviors, despite overwhelming conventional and technological superiority, called into question the idea of "Rapid Decisive Operations," which served as the conceptual underpinning of Donald Rumsfeld's transformation strategy. Huba Wass de Czege, "Rethinking IO: Complex Operations in the Information Age," *Military Review* (November-December 2008): 14–26, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/241/rec/8.

[92] Joseph L. Cox, *Information Operations in Operation Enduring Freedom: What Went Wrong?*, School of Advanced Military Studies, 2006, https://apps.dtic.mil/sti/pdfs/ADA449922.pdf.

[93] Johnson, et al., "A Review of the Army's Modular Force Structure," 11. Of note, although the term "modularity" is often exclusively associated with Schoomaker's creation of brigade combat teams, the idea of modularity was first introduced in 1994 as one of five characteristics that described the Army's Force XXI. Johnson, et al. "Review of the Army's Modular Force Structure," 8.

[94] Adams, *Army After Next*, 185, 209. This principle was in keeping with the vision of network-centric warfare that had served as the central organizing principle of the Defense Department transformation since 1996. See John Shalikashvili, "Joint Vision 2010" (Washington, DC: Government Printing Office, 1996); Chairman of the Joint Chiefs of Staff, "Joint Vision 2020" (Washington, DC: Government Printing Office, 2000).

[95] Donald H. Rumsfeld, *Quadrennial Defense Review Report*, Department of Defense, 2001, 30, 38, 43, https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/qdr2001.pdf.

requirement.[96] By that point, early in the Global War on Terror, Army information operations had developed a reputation that was indistinguishable from the technology that it relied upon. This reputation created three interrelated challenges that the Army would have to address if it was going to successfully meet Defense Department guidance to develop information operations as a core capability.[97]

First, the Army would have to alter the prevailing service mindset that viewed information operations as synonymous with technology.[98] Doing so would entail meeting a second challenge: untangling the complicated relationship between information operations, computer network operations, and space. The complexity of this relationship was as much organizational as it was conceptual. 1st Information Operations Command, the organizational successor to Land Information Warfare Activity, had to answer to U.S. Army Intelligence and Security Command, U.S. Army Network Command, and U.S. Army Space Command in a series of support relationships that not only reinforced the notion of information operations as a technological discipline, but that also made it increasingly difficult for the information operations community to fulfill its purpose of integrating different capabilities.[99] Finally, the Army would have to address the first two challenges while simultaneously building out its capability across the five information operations components that the Defense Department's 2003 *Information Operations Roadmap* had identified as authoritative.[100] This meant not only improving its information operations organizations, career force, and training, but also doing the same for information operations' subordinate capabilities — most notably electronic warfare and computer network operations, which had gained favor in the still-persistent vision of network-centric warfare.

To further complicate matters, the Army had to fulfill joint guidance on information operations without fully agreeing on the joint information operations concept that motivated that guidance. While the Army information operations community generally accepted the five-capability structure and the paradigm of core, supporting, and related capabilities espoused in joint doctrine, they perceived the joint concept as too stove-piped in its approach to integration: Capabilities were discretely employed by information operations planners rather than fully integrated into planning and operations.[101] In addition, the joint definition of information operations did not allow for the possibility of influencing non-adversary audiences, which the Army assessed as a critical requirement for fighting among local populations on land.[102]

Despite this disagreement, the Army's 2003 update to Field Manual 100-6 — now called Field Manual 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures* — did not substantially deviate from the joint definition of information operations. Rather, the manual updated the Army's definition to fall in line with the joint characterization of information operations as comprising five core capabilities:

> Information operations is the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decision-making.[103]

Whereas Field Manual 100-6 had focused largely

[96] Senior Information Operations Review Council, "Synchronizing Army Information Operations," PowerPoint Presentation, Fort Leavenworth, KS, July 8, 2002.

[97] These guidelines were most explicitly outlined in Rumsfeld, *Quadrennial Defense Review Report*, 30, 38, 43, and Donald H. Rumsfeld, "Information Operations Roadmap," Department of Defense, Oct. 30, 2003, https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/Information_Operations_Roadmap_30_October_2003.pdf.

[98] Information Operation Requirements Review Council, "Information Operation Requirements Review Council (RCC)," PowerPoint Presentation, Fort Leavenworth, KS, November 2002, slide 18.

[99] Senior Information Operations Review Council, "Synchronizing Army Information Operations," slides 11–14, 21.

[100] Rumsfeld, "Information Operations Roadmap."

[101] Information Operations Requirements Review Council, "Information Operations Requirements Review Council," slide 11.

[102] Joint Publication 3-13 published in 1998 defined information operations as "actions taken to affect *adversary* [emphasis mine] information and information systems while defending one's own information and information systems." Office of the Chairman of the Joint Chiefs of Staff, *Information Operations,* Joint Publication (JP) 3-13 (Washington, DC: Joint Chiefs of Staff, Oct. 9, 1998), Glossary-7. Joint Publication 3-13 published in 2006 defined information operations as "The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp *adversarial* [emphasis mine] human and automated decision making while protecting our own." Office of the Chairman of the Joint Chiefs of Staff, *Information Operations,* Joint Publication (JP) 3-13 (Washington, DC: Joint Chiefs of Staff, Feb. 13, 2006), Glossary-9, https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf.

[103] Department of the Army, *Information Operations: Doctrine, Tactics, Techniques, and Procedures,* Field Manual (FM) 3-13 (Washington, DC: Government Printing Office, 2003), Glossary-12, https://www.bits.de/NRANEU/others/amd-us-archive/fm3-13%2803%29.pdf.

on theory, this manual focused heavily on the practical implementation of information operations based on lessons learned in Bosnia and Kosovo.

However, the deterioration of Iraq into sectarian violence and insurgency in 2004 caused the practical application of information operations to take on two different, and contradictory, meanings. Doctrinally, it remained an activity of staff integration whose purpose was to affect enemy decision-making in accordance with the 2003 edition of Field Manual 3-13. Tactically, however, the unique demands of counter-insurgency operations had caused information operations to become conflated with psychological operations, strategic communication, and public affairs.[104]

This confusion over the proper definition and function of information operations resulted from a number of structural, organizational, and doctrinal factors. From the standpoint of doctrine, neither Field Manual 3-13 nor Field Manual 3-0 contained sufficient guidance on how to integrate information operations into staff operations writ large or into counter-insurgency operations specifically.[105] Commanders either developed their own unique methods of integrating information operations or ignored it entirely in favor of the more lethal elements of counter-insurgency, which were easier to understand and easier to measure.[106]

A shortage of qualified information operations personnel exacerbated these doctrinal deficiencies. Beginning in 2004, the twin engines of modularity and ongoing combat operations caused a jump in FA30 manpower requirements that far exceeded the field's original growth model.[107] Faced with

[104] Lowe, "From Battle to Battle of Ideas," 41; Fredric W. Rohm Jr., "Merging Information Operations and Psychological Operations," *Military Review* 88, no. 1 (2008): 108–11, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/236/rec/7; Curtis D. Boyd, "Army IO *Is* PSYOP: Influencing More with Less," *Military Review* 87, no. 3 (2007): 67–75, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/162/rec/6; Norman Emery, "Information Operations in Iraq," *Military Review* 84, no. 3 (2004): 11–14, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/192/rec/1; Norman Emery, et al., "Fighting Terrorism and Insurgency: Shaping the Information Environment." *Military Review* 85, no. 1 (2005): 32–38, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/168/rec/7; and Garry J. Beavers, "Defining the Information Campaign," *Military Review* 85, no. 6 (2005): 80–82, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/172/rec/3.

[105] Collin T. Hunton, *The War of Ideas and the Role of Information Operations in Counterinsurgency*, School of Advanced Military Studies, 2007, https://apps.dtic.mil/sti/pdfs/ADA494409.pdf.

[106] Cox, "Information Operations in Operation Enduring Freedom;" and Hunton, "The War of Ideas."

[107] Cox, "Information Operations in Operation Enduring Freedom," 25. The information operations FA30 smart book shows the FA30 growth model, which predicted neither the increase in demand due to overseas combat operations nor the addition of FA30 billets into brigade combat teams.

limited resources and high operational demand, 1st Information Operations Command prioritized lending its support to the special operations and strategic communities, while the conventional Army received poorly trained and inexperienced teams of national guard and reserve personnel.[108] Inadequacies in the FA30 training model combined with the generally poor quality of officers presented additional challenges to effectively integrating or implementing information operations.[109]

The growth of the field of cyber and electromagnetic activities further tested the traditional information operations construct.[110] Though originally one of the five subcomponents of information operations, in the mid-2000s both cyberspace operations and electronic warfare experienced rapid growth that complicated the organizational dynamics and conceptual models of information operations.[111] The role that digital information played in counter-terrorism and counter-insurgency — that of enabling an unprecedented level of precision intelligence and targeting — encouraged the growth of cyberspace as the medium through which to achieve the economy of force that the Department of Defense's 21st-century transformation had originally pursued on the physical battlefield.[112] By the late 2000s, cyberspace operations had attracted much of the information revolution-style attention that would have formerly gone to command-and-control warfare or to an earlier construct of information operations, while information operations had devolved into a spin-off of psychological warfare.

The field of information operations thus faced a paradox. On the one hand, there was unanimous consensus that information and the information environment were vital to the successful conduct of military operations in Iraq and Afghanistan.[113] On the other hand, there was widespread confusion as to what information operations was or how it ought to be leveraged.[114] In the midst of this confusion, a few influential maneuver commanders began to develop their own understanding of what information operations was and how it should apply to a counter-insurgency. This began a process of top-down, directed change that threatened to disrupt existing organizational structures and ran counter to the preferences of the FA30 community.

A New Information Paradigm for Stability Operations

When then-Lt. Gen. David Petraeus took over command of the Combined Arms Center at Fort Leavenworth in October 2005, one of his priorities was to fix the Army's information operations construct.[115] To enact the desired changes, he had to overcome entrenched resistance from the information operations community itself, most of which did not want to change the five-capability model or break from its origins in the technical world of command-and-control warfare.

In 2006, Petraeus asked intellectual heavyweight Brig. Gen. (ret.) Huba Wass de Czege to serve as his special assistant for information operations. From October 2006 to September 2007, Wass de Czege conducted a comprehensive review of information operations to inform the development

[108] White, "Subcultural Influence," 91; and Bradley Bloom, "Information Operations in Support of Special Operations," *Military Review* 84, no. 1 (2004): 45–49, https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/174/rec/6.

[109] On training, Dean A. Burbridge, "U.S. Army Functional Area Qualification Course Inputs," Letter to U.S. Army Information Operations Proponent, Combined Arms Center, Fort Leavenworth, KS, Headquarters, Combined/Joint Task Force (CJTF)-101, Bagram Airfield, Afghanistan, Oct. 19, 2008. On quality, see White, "Subcultural Influence," 91–92.

[110] U.S. Army Combined Arms Center, "FM 3-13, *Information*, Update to Army Science Board, 02 February 2009," PowerPoint Presentation, Fort Leavenworth, KS, Feb. 2, 2009.

[111] U.S. Army Combined Arms Center, "FM 3-13, *Information*, Update to Army Science Board," slide 5.

[112] Both Donald Rumsfeld and George W. Bush were influenced by Andrew Marshall's work on Revolutions in Military Affairs (RMAs), which was based upon the ideas of an information-dependent precision-strike complex and network-centric warfare. Rumsfeld appointed Arthur Cebrowski to lead his force transformation initiative based on the theory of network-centric warfare, in which smaller, lighter, more agile units would leverage information technology to fight as "networked systems" and "distributed formations" using newly developed sensors and a dense computer-enabled communications network.

[113] Lowe, "From Battle to Battle of Ideas," 43; Paul B. Olsen, ed., *An Engine of Change: The Collected Works of LTG Petraeus 2005-2007* (Leavenworth, KS: Combined Arms Center, 2008), 27.

[114] U.S. Army Combined Arms Center, "FM 3-13, *Information*, Update to Army Science Board,"; James C. Riley, "Establishing an ACofC, G7 as the Coordinating Staff Officer for Information Operations," Memorandum for Director, Combined Arms Doctrine Directorate, U.S. Army Combined Arms Center, Fort Leavenworth, KS, May 30, 2003. Information operations articles in *Military Review* during the mid-2000s included subjects as wide-ranging as network operations, marketing, and detainee health, in addition to discussions of more standard information operations fare.

[115] William O. Robertson and Kelvin Crow, "Interview with Lieutenant General David H. Petraeus," Combined Arms Center History Office, April 17, 2004. William O. Robertson and Kelvin Crow, "End of Tour Interview with Lieutenant General David Petraeus," Combined Arms Center History Office, Jan. 27, 2007. The other priorities included the revamp of Field Manual 3-0 for full-spectrum operations, and the drafting of an Army counter-insurgency manual.

of new doctrine.[116] He argued that both the Army and joint information operations paradigms were ill suited to the complexities of 21st-century warfare. Developed in the 1990s to solve the central problem of how to rapidly defeat a modern, information-age military, information operations doctrine adopted an overly simplified causal logic that was heavily biased toward physical effects; pursued a purpose — information superiority — that was ultimately unattainable; and tended to overlook the psychological or moral dimensions of conflict.[117] In order to be effective in modern conflict, Wass de Czege argued, information operations doctrine would have to be redesigned according to a new logic, in pursuit of a new purpose, and using different methods.

To replace the current information operations paradigm, Wass de Czege identified three dimensions common to all 21st-century military problems.[118] The first was the psychological contest of wills, in which adversaries leverage words, actions, and images to influence decisions in the moral domain. The second was the realm of military public relations, which concerned gaining and keeping the trust of relevant populations both at home and abroad. The third and final dimension was the contest between different applications of information technology, which Wass de Czege called "netwar." The purpose of information operations was not to attain information superiority, but to achieve an advantage in each of these three areas.

Several organizational consequences followed from Wass de Czege's new paradigm. First, the differences between the dimensions were such that it was untenable to group them under the purview of a single staff officer. Wass de Czege instead recommended reorganizing information operations capabilities into staff groupings that shared a common functional purpose — moving deception into plans, for example, operations security into protection, and electronic warfare into fires.[119] Second, the need for coherence between words and actions meant that information operations capabilities were necessary but not sufficient for achieving success across the three dimensions.[120] Information operations would have to be combined with capabilities outside of the information operations umbrella to be effective. This meant that information operations could not be treated as a separate line of effort, but had to be fully integrated with the multiple lines of operation that were present in a combined arms campaign — a fact that further supported the distribution of information operations responsibilities across the staff.[121] Third, having eliminated the need for a central staff integrator, the role of the FA30 shifted to that of a "strategic communicator," who was primarily responsible for managing the second dimension: public communications. The end result was the disaggregation of information operations as a distinct staff function and its wholesale elimination as a term.[122]

Wass de Czege's recommendations were nearly unanimously rejected by the FA30 community due to their disruptive effect on existing structures and paradigms. However, they heavily influenced Petraeus, his successor at the Combined Arms Center, Lt. Gen. William Caldwell, and Gen. William Wallace, who commanded U.S. Army Training and Doctrine Command from October 2005 to December 2008. Each of these men viewed Wass de Czege's concept as more in line with their experiences in Iraq and Afghanistan than the current model. Wallace used the 2008 edition of Field Manual 3-0 to implement the first major doctrinal changes to the Army's information operations construct.

As the first revision of the Army's capstone manual since 9/11, this manual replaced the term "information operations" with five information tasks: command-and-control warfare, information protection, operations security, military deception, and information engagement.[123] Information engagement consisted of

> the integrated employment of public affairs to inform U.S. and friendly audiences; psychological operations, combat camera, U.S. Government strategic communication and defense support to public diplomacy, and other means necessary to influence foreign

[116] Huba Wass de Czege, "Information Operations Study," PowerPoint Presentation, U.S. Army Combined Arms Center, Fort Leavenworth, KS, Oct. 12, 2007; Huba Wass de Czege, "Information Operations Study (Synopsis)," U.S. Army Combined Arms Center, Fort Leavenworth, KS, Dec. 6, 2007; Huba Wass de Czege, "From 'IO' to Complex Operations in the Information Age: Synopsis of a Comprehensive Review of Information Operations (IO) in the 21st Century for the US Army Information Proponent," Fort Leavenworth, KS, August 2009.

[117] Wass de Czege, "Rethinking IO."

[118] Wass de Czege, "Information Operations Study."

[119] Wass de Czege, "Rethinking IO."

[120] Wass de Czege, "Rethinking IO."

[121] Wass de Czege, "Rethinking IO."

[122] Wass de Czege, "Information Operations Study."

[123] Department of the Army, *Operations*, Field Manual (FM) 3-0 (Washington, DC: Government Printing Office, 2008), 7–3.

> audiences; and, leader and Soldier engagements to support both efforts.[124]

In other words, information engagement was seen as the way to develop a unit's public affairs officer into a true subject-matter expert in the one area that did not have a name in the joint information operations construct: coordinating to get messages out and ensuring that those messages are consistent with a unit's actions.[125]

The stated reasons for these changes were twofold. The first was a need to rectify a critical deficiency in joint doctrine to make information operations more applicable to land forces.[126] As stated, the joint definition of information operations was narrowly focused on adversaries and did not make allowances for the need to influence friendly or neutral audiences — a complaint the army had harbored about joint doctrine since the introduction of Field Manual 100-6 in 1996.[127] The second, and far more important reason, was the feedback that came from commanders in Iraq and Afghanistan about the difficulties they faced in implementing information operations under current Army doctrine.[128] These challenges were multifaceted and built upon the manpower problems already mentioned.

Conceptually, the information operations construct was too broad for Army commanders and staffs to either understand or apply.[129] Information operations consisted of a collection of loosely related capabilities that ranged from the technically specific realm of electronic warfare and computer network operations to the more cerebral activities of psychological operations and public affairs. This range was more than any single staff officer could handle, yet the lack of subject-matter expertise *within* staffs made it difficult to distribute responsibility for the capabilities more widely.[130] The transition to modular brigade combat teams created further confusion with respect to staff responsibilities, since existing information operations doctrine had been developed for use at division and corps levels.[131] Moreover, there was an evident need for greater specialization within the technical capabilities, particularly that of electronic warfare, as the Army began to place stronger emphasis on these capabilities at the expense of a unified information operations construct.[132] Practically, despite the breadth of the information operations construct, it did not address the critical task of how to communicate with wide audiences or to engage with different populations.[133]

Despite widespread recognition of the underlying need for change, the replacement of information operations with five information tasks was widely considered a controversial move.[134] Equally as controversial was the subsequent effort to revise Field Manual 3-13 based on the information task model. Called simply, *Information*, the new draft was meant to further specify the logic of the Army's new information construct, to refine its integration into Army planning and operations, and to resolve outstanding issues with Field Manual 3-0.[135] However, the manual never made it past draft form due to entrenched disagreement over both its underlying conceptual framework and its organizational implications.

The draft revision of Field Manual 3-13 began from Wass de Czege's premise that the historic core of the Army information operations model — command-and-control warfare[136] — was no longer

[124] Department of the Army, *Operations*, FM 3-0, (2008), 7-3.

[125] U.S. Army Combined Arms Center, "Operations and Information Update GORB," PowerPoint Presentation, Fort Leavenworth, KS, July 7, 2009.

[126] U.S. Army Combined Arms Doctrine Directorate, "FM 3-0 Issue Paper: Information Operations," Fort Leavenworth, KS, 2008, 2. In 2006, the update to Joint Publication 3-13 defined information operations as "the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."

[127] Wass de Czege, "Rethinking IO."

[128] U.S. Army Combined Arms Doctrine Directorate, "FM 3-0 Issue Paper," 2.

[129] U.S. Army Combined Arms Doctrine Directorate, "FM 3-0 Issue Paper," 2.

[130] U.S. Army Combined Arms Doctrine Directorate, "FM 3-0 Issue Paper." Also see Riley, "Establishing the ACofS, G7," which states that "Army forces [in Operation Iraqi Freedom] failed to leverage information as an element of combat power to its greatest potential."

[131] U.S. Army Combined Arms Doctrine Directorate, "FM 3-0 Issue Paper," 2.

[132] U.S. Army Combined Arms Doctrine Directorate, "FM 3-0 Issue Paper," 2. Robertson and Crow, "End of Tour Interview with Lieutenant General David Petraeus," 2007.

[133] U.S. Army Combined Arms Center, "FM 3-13, *Information*, Update to Army Science Board."

[134] U.S. Army Combined Arms Doctrine Directorate, "Issue Paper – Chapter 7, FM 3-0, Information Superiority," Fort Leavenworth, KS, 2009.

[135] Department of the Army, *Information*, Field Manual (FM) 3-13, Initial Draft (Washington, DC: Government Printing Office, Feb. 27, 2009).

[136] Command and control warfare replaced command, control, and communications countermeasures in 1992. See Deputy Secretary of Defense, *Electronic Warfare (EW) and Command and Control Warfare (C2W) Countermeasures*, Department of Defense Directive 3222.4, Department of Defense, July 31, 1992, Incorporating Change 2 through Jan. 28 1994.

adequate for the complex and unstructured nature of the Army's 21st-century operational demands, nor did it capture the implications of a globally interconnected and information saturated operating environment.[137] Its doctrinal emphasis on the pursuit of information superiority, which the manual called an "inconclusive operational objective and an elusive goal," had caused the Army to neglect the importance of influencing the emotions, attitudes, behaviors, and beliefs of the various populations involved in a conflict.[138] The ability to win this contest of influence would "determine the outcome of military missions in the 21st century."[139]

The 2009 draft Field Manual 3-13 reorganized the five information tasks from 2008 into Wass de Czege's three dimensions of information conflict, thereby expanding the ways in which commanders could use information to influence the operational environment.[140] However, the practical implementation of the draft's framework would have led to the same significant reorganization of staff responsibilities for information tasks that Wass de Czege's original recommendations did in 2007. Under the old construct, the FA30 retained responsibility for integrating all five components of information operations into the planning process. The new construct distributed the information tasks across the staff and relied on the operations process to synchronize and integrate them.[141] The FA30, acting as the staff G7, would be solely responsible for the task of information engagement, rather than for information operations integration.

Differing Organizational Perspectives

Responses to the draft Field Manual 3-13 were highly contentious and varied along three different organizational perspectives. Each of these perspectives differed in how it defined the fundamental relationship between information and operations, which, in turn, affected how information ought to be treated and where on the staff it belonged.[142]

The first of these perspectives was that of the maneuver community, represented not only by commanders in the field but by the leadership at the Combined Arms Center. Broadly speaking, this community argued that "information" was inherent to all operations. "Influence" over enemy decision-making was the cumulative result of all of a unit's interactions with the operational environment, such that the physical actions of a unit created more consequential messaging than did words or images.[143] Planning this type of influence was a fundamental aspect of campaign design that could not be delegated to a secondary staff integrator. Instead, decisions about who to influence, why, and how were the responsibility of the commander and G3, while assessment of influence success was the responsibility of the G2.[144] This community argued that the skillful use of words and images for operational purposes served as an adjunct tool of influence, but it nevertheless needed to rise to the level of a warfighting function in order to develop real competence, capacity, and capability across the Army.[145]

The second perspective was that of the fires community, for whom information was a quantifiable, non-lethal munition that commanders could fire at targets to achieve specific and predictable effects.[146] Information, thus conceived, was fundamentally a part of the targeting process, which meant that decisions about whom to influence and how were the responsibility of the fires support coordinator working in conjunction with the commander.[147]

[137] Department of the Army, *Information*, FM 3-13, initial draft (2009), 1-3; and U.S. Army Combined Arms Center, "FM 3-13, *Information*, Update to Army Science Board."

[138] Department of the Army, *Information*, FM 3-13, initial draft (2009), 1-2 to 1-3.

[139] Department of the Army, *Information*, FM 3-13, initial draft (2009), 1-1.

[140] This field manual featured a chapter dedicated to each of the three dimensions, which served as the central organizing principle for the information doctrine. See chapters 2, 3, and 4.

[141] U.S. Army Combined Arms Center, "FM 3-13, *Information*, Update to Army Science Board."

[142] U.S. Army Combined Arms Center, "FM 3-13 Update," PowerPoint Presentation, Fort Leavenworth, KS, May 14, 2009; U.S. Army Combined Arms Center, "Operations and Information Council of Colonels 28 July 2009 Read Ahead Packet," PowerPoint Presentation, Fort Leavenworth, KS, July 28, 2009; and U.S. Army Combined Arms Doctrine Directorate, "Comments on IO GORB," PowerPoint Presentation, Fort Leavenworth, KS, Aug. 31, 2009.

[143] U.S. Army Combined Arms Center, "Operations and Information General Officer Review Board, Update to DtCG, 12 June 2009," PowerPoint Presentation, Fort Leavenworth, KS, June 12, 2009.

[144] U.S. Army Combined Arms Center, "Operations and Information General Officer Review Board."

[145] U.S. Army Combined Arms Doctrine Directorate, "Decision Briefing: DOTMLPF Way Ahead for 'Information' and 'Non-Lethal Effects,'" PowerPoint Presentation, Fort Leavenworth, KS, April 21, 2009.

[146] U.S. Army Combined Arms Center, "Operations and Information General Officer Review Board."

[147] U.S. Army Combined Arms Center, "Operations and Information General Officer Review Board."

Information and its various sub-tasks logically fell underneath the fires warfighting function.[148]

The third perspective came from the FA30 community. This community argued that "information" comprised a special category of operations used by the commander to affect adversary decision-making while protecting the commander's own decision-making. Decisions about how to use this category of operations belonged under the purview of a dedicated G3 information operations officer, whose primary focus was on the process of integrating different information capabilities to achieve a specific effect on a target population.[149] Assessing the impact of those capabilities required intelligence specialists who were trained in applying intelligence to information operations.[150] The broad majority advocated for information operations as a warfighting function, though some senior FA30s disagreed.[151]

These differences in perspective shaped each community's reaction to the Field Manual 3-13 draft, with the FA30 community reacting with the most hostility. Conceptually, this community argued that the entire premise of Field Manual 3-13 was false because the existing construct was not inadequate.[152] Instead, it was under-manned and under-resourced.[153] Any perceived deficiencies in the construct stemmed from these challenges, combined with the lack of a central U.S. plan for strategic communications. While this community largely acknowledged a need for better information engagement, they argued that it should fall to public affairs and psychological operations rather than serve as the central task of the FA30.[154] Moreover, they argued that the draft Field Manual 3-13 model was too focused on the unique conditions of the Global War on Terror and would have limited applicability to large-scale conventional conflicts.[155]

Practically, the FA30 community objected to the decentralization of staff responsibility for information tasks. They argued that, although information tasks may possess certain functional similarities to other warfighting functions, they would lose visibility if assigned outside of the purview of a central integrator.[156] This much was evident in Desert Storm, when the lack of a central integrator resulted in information fratricide and the inefficient use of information capabilities.[157] In addition, the manual broke from joint doctrine without acknowledging the fact that information operations was still a viable term in the joint community.

Finally, the new paradigm created unpalatable bureaucratic and financial consequences for the FA30 community. In addition to threatening the existence of the FA30 career field itself, the new paradigm would jeopardize the existence of the programs and capabilities that were tied to the old construct.[158] In total, the release of draft Field Manual 3-13 for review in late 2009 revealed a significant difference of opinion within the Army about how information operations should be organized, who on staff should be responsible for it, and what its relation is to the growing fields of cyber and electronic warfare.[159] In late 2009, Army Chief of Staff Gen. George Casey killed the draft Field Manual 3-13 project due to the intractability of these differences.[160]

[148] U.S. Army Combined Arms Center, "Operations and Information General Officer Review Board"; and U.S. Army Combined Arms Doctrine Directorate, "Decision Briefing: DOTMLPF Way Ahead."

[149] U.S. Army Combined Arms Doctrine Directorate, "Decision Briefing: DOTMLPF Way Ahead."

[150] U.S. Army Combined Arms Center, "Operations and Information General Officer Review Board."

[151] U.S. Army Combined Arms Center, "Operations and Information General Officer Review Board."

[152] Pat Manners, et al., "A Common Sense Approach to U.S. Army Information Operations," PowerPoint Presentation, Headquarters, U.S. Army Pacific and U.S. PACOM, Fort Shafter, HI, 2009.

[153] Manners, et al., "A Common Sense Approach."

[154] Manners, et al., "A Common Sense Approach"; and U.S. Army Combined Arms Doctrine Directorate, "FM 3-13 Feedback," PowerPoint Presentation, Fort Leavenworth, KS, March 26, 2009.

[155] U.S. Army Combined Arms Center, "Operations and Information Council of Colonels 28 July 2009 Read Ahead Packet."

[156] U.S. Army Combined Arms Doctrine Directorate, "FM 3-13 Feedback."

[157] U.S. Army Combined Arms Doctrine Directorate, "FM 3-13 Feedback"; and Manners, et al., "A Common Sense Approach."

[158] U.S. Army Combined Arms Doctrine Directorate, "FM 3-13 Feedback;" and U.S. Army Combined Arms Doctrine Directorate, "Decision Briefing: DOTMLPF Way Ahead."

[159] Martin E. Dempsey, "Posturing the Army for Cyber, EW, and IO as Dimensions of Full Spectrum Operations," Memorandum for Gen. Peter W. Chiarelli, Vice Chief of Staff, Headquarters, U.S. Army Training and Doctrine Command, Fort Monroe, VA, Oct. 16, 2009. Slides from the 1995 U.S. Army Intelligence Center briefing, "Information Operations: Defining the Concept," which was associated with the Fort Huachuca information operations war games that took place in October and November of that year, indicate that these questions of relationships and staff management were present from the earliest days of information operations. Proposed discussion topics for the information operations war game included: "Is C2W equivalent to maneuver, fires, M/C/S?"; "Is there a difference between information operations and intel?"; and "Where should C2W be on Corps staff and who should serve as C2W officer?" This debate grew more complex with the 2003 transfer of certain information operations responsibilities to the mission command function.

[160] Department of the Army, G-3/5/7, "CSA Tasker: Army Information Operations (IO) Information Briefing," PowerPoint Presentation, Washington, DC, March 25, 2015, slide 10.

The Arrival of "Inform and Influence"

In February 2011, a change to Field Manual 3-0 offered a new way forward for information operations when it replaced the five information tasks with two task categories: inform and influence activities and cyber and electromagnetic activities. Inform and influence activities took over the short-lived role of information engagement, with a definition of "integrating activities within the mission command warfighting function which ensure themes and messages … are synchronized with actions to support full spectrum operations."[161] The stated reason for the change was to rectify a deficiency in the joint construct, which lacked reference to activities related to synchronized messaging.[162] Change 1 also eliminated the chapter on information superiority and instead moved information activities into a chapter on staff processes entitled "The Science of Control."

The transformation of information operations doctrine reached its zenith in January 2013, with the release of a new version of Field Manual 3-13.[163] Now called *Inform and Influence Activities*, this manual formally eliminated information operations as an Army term and replaced it with "inform and influence activities." The manual also removed cyber and electromagnetic activities from underneath the purview of what used to be called information operations and treated it instead as its own unique function — albeit one that the Army would use in conjunction with inform and influence activities to support the joint construct of information operations.[164]

Field Manual 3-13 defined "inform and influence activities" as "the integration of designated information-related capabilities in order to synchronize themes, messages, and actions with operations to inform United States and global audiences, influence foreign audiences, and affect adversary and enemy decision-making."[165] Information-related capabilities, in turn, included the traditional information operations components of psychological operations — now called "military information support operations" — military deception, and operations security, along with public affairs, combat camera, civil affairs, and "soldier and leader engagement."[166] The overall purpose of inform and influence activities was to inform domestic and global audiences, influence foreign audiences, and affect enemy decision-making. It retained the strong focus on synchronizing messages and actions that was present in the 2008 Field Manual 3-0.

The 2013 edition of Field Manual 3-13 was highly controversial. While the majority of the Army organizations that were involved with the drafting process concurred with the radical changes, members of the information operations community had several significant criticisms…

The 2013 edition of Field Manual 3-13 was highly controversial. While the majority of the Army organizations that were involved with the drafting process concurred with the radical changes, members of the information operations community had several significant criticisms, many of which echoed their critiques of both the 2008 edition of Field Manual 3-0 and the 2009 Army Doctrinal Publication 3-13 draft.[167] The first of these criticisms was the unclear relationship between inform and influence activities and the joint information operations construct. Although inform and influence activities served as a substitute for information operations within the Army context, it was unclear whether it was intended to be a subset of joint information operations or a replacement for it.[168] As a result of this unclear relationship, Army FA30s were asked to perform double duty, serving in a staff public affairs role for inform and influence activities integration while fulfilling joint and Defense Department

[161] Department of the Army, *Operations, Change 1*, Field Manual (FM) 3-0 (Washington, DC: Government Printing Office, 2011), Glossary-7.

[162] Department of the Army, *Operations, Change 1*, FM 3-0, D-8.

[163] Department of the Army, *Inform and Influence Activities*, Field Manual (FM) 3-13 (Washington, DC: Army Publishing Directorate, January 2013), https://www.bits.de/NRANEU/others/amd-us-archive/FM3-13%2813%29.pdf.

[164] U.S. Army Training and Doctrine Command G2, "IIA/IO/MISO Overview G-3/5/7 Staff Estimate," PowerPoint Presentation, August 2012, slide 4.

[165] Department of the Army, *Inform and Influence Activities*, FM 3-13 (2013), 1-1.

[166] Department of the Army, *Inform and Influence Activities*, FM 3-13 (2013), 1-1.

[167] Wayne Grigsby, "General Officer Steering Committee Meeting, FM 3-13: Inform and Influence Activities," PowerPoint Presentation, U.S. Army Combined Arms Center, Fort Leavenworth, KS, March 27, 2012; and Mike Dominique, "General Officer Steering Committee Meeting, FM 3-13: Inform and Influence Activities," PowerPoint Presentation, Information Proponent Office, Fort Leavenworth, KS, Feb. 23, 2012.

[168] Army Cyber Command, "Summary of ARCC Non-Concur with FM 3-13," Power Point Presentation, Fort Belvoir, VA, Feb. 22, 2022.

requirements to serve as information officers.[169]

A second, and related, issue concerned staff synchronization and organization. Whereas information operations integrated all information-related capabilities, inform and influence activities did not present a single synchronization process, but distributed responsibility for various information-related activities across the staff. The gaps within the concept placed an unrealistic burden on the G3 to ensure consistency in integration.[170] Moreover, the exclusive centralization of certain inform and influence activities tasks within the G7/S7 construct did not adequately address units that lacked that critical staff position.[171] If the function was as critical as the manual said it was, then it ought to be allocated to a position that existed within all units at all echelons. It was also unclear how units were to evaluate the effectiveness of their inform and influence activities, given the difficulty of measuring things like "influence" or the impacts of messaging on target audience psychology.

The 2013 edition of Field Manual 3-13 also presented unclear roles and responsibilities with respect to the Army's major information operations organizations, specifically 1st Information Operations Command and the National Guard's four Theater Information Operations Groups.[172] These organizations were organized, staffed, equipped, and trained to support the joint information operations standards. The radical changes to the Army's doctrinal concept that Field Manual 3-13 contained would inevitably risk personnel, funding, and mission support for these organizations.

Finally, the construct also focused on low-intensity conflict at the expense of future full-spectrum operations, did not sufficiently address levels above the battalion, and did not articulate how to integrate inform and influence activities with cyber and electromagnetic activities in support of mission command.[173] There was also the nagging sense that if information operations was simply about influence, then it would be a redundant — and ultimately unnecessary — form of psychological operations.[174]

In addition to these organizational and cultural frictions, feedback from the field between 2009 and 2013 suggested that the inform and influence activities concept was no more effective than its predecessors in solving the Army's operational challenges.[175] Army leaders remained dissatisfied with the results of information-related capabilities on the battlefield despite the creation of an ostensibly more suitable information doctrine.[176] While the 2013 edition of Field Manual 3-13 presented the strongest doctrinal version of Wass de Czege's 2007 information logic, its poor reception suggested that this logic was fundamentally incompatible with the Army's organizational and cultural realities.

On Dec. 4, 2013, Army Chief of Staff Gen. Raymond Odierno, who had disagreed with Change 1 to Field Manual 3-0 in 2011, issued a directive to disaggregate inform and influence activities.[177] In December 2016, the Army responded to this directive with the release of Field Manual 3-13, *Information Operations*. The stated purpose of this field manual was by now a familiar refrain: to better align Army doctrine with joint doctrine while recognizing the unique requirements of information operations in support of land forces. The manual rescinded the term "inform and influence activities" and returned to "information operations" under the joint definition: "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."[178] In addition, the FA30 returned to being the central staff focal point for the synchronization and integration of information operations.[179]

[169] U.S. Army Information Proponent Office, "FM 3-13 IPR," PowerPoint Presentation, Fort Leavenworth, KS, 2011.

[170] Army Cyber Command, "Summary of ARCC Non-Concur with FM 3-13."

[171] Jeffrey E. Pounding, "Draft FM 3-13," Memorandum for Director, Training and Doctrine Command, Fort Leavenworth, KS, Feb. 1, 2012.

[172] Army Cyber Command, "Summary of ARCC Non-Concur with FM 3-13"; and Pounding, "Draft FM 3-13."

[173] Grigsby, "General Officer Steering Committee Meeting."

[174] Department of the Army, G-3/5/7, "CSA Tasker." This redundancy presented a threat to the FA30 community but an opportunity to psychological operations, which used it to launch an ultimately unsuccessful effort to acquire information operations wholesale.

[175] Steven D. Santa Maria, *Improving Influence Operations by Defining Influence and Influence Operations*, School of Advanced Military Studies, 2013, https://apps.dtic.mil/sti/pdfs/ADA606282.pdf.

[176] Scott K. Thompson, *Theoretical Implications for Inform and Influence Activities*, School of Advanced Military Studies, 2013, https://apps.dtic.mil/sti/pdfs/ADA589562.pdf.

[177] John E. Bircher IV, "Review of the Program Directive for FM 3-13, *Information Operations*," Memorandum for Distribution, Information Operations Proponent, Fort Leavenworth, KS, July 10, 2014.

[178] Department of the Army, *Information Operations*, Field Manual (FM) 3-13 (Washington, DC: Government Printing Office, December 2016), 1-2, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/FM%203-13%20FINAL%20WEB.pdf.

[179] Department of the Army, *Information Operations*, FM 3-13 (2016), 3-4.

The idea of information superiority, which had historically motivated both the Army and joint information operations constructs, was absent from the manual. Instead, the 2016 version of Field Manual 3-13 described a twofold purpose for information operations that attempted to reconcile the joint understanding of information operations with lessons learned from 15 years of persistent conflict. The first purpose, recalling the traditional information operations paradigm, held that Army units employ information operations to create effects in and through the information environment. These effects provide commanders with a decisive advantage over "adversaries, threats, and enemies" in order to defeat the opponent's will to fight.[180]

The second purpose recalled the Army's decade-long attempt to bend information operations toward a better accommodation of the human dimension of conflict. It argued that Army units engage with and influence other relevant foreign audiences to gain their support for friendly objectives.[181] While the manual maintained that the central focus of information operations was to affect adversary decision-making, the balance of emphasis throughout was on this second purpose of influence. This was a product of the recognition — which emerged from the Global War on Terror — that commanders and staffs must do more than alter the enemy's decision-making processes if they are to accomplish their mission: They must know how to conduct information operations "left of bang" on the spectrum of conflict.[182] The manual featured robust discussion of the importance of narrative alignment, audience engagement, and the protection of friendly messaging as components of successful information operations.[183] This emphasis aside, from both a definitional and a doctrinal standpoint, the 2016 edition of Field Manual 3-13 marked a clear return to the classical understanding of information: as a collection of capabilities that create effects to alter adversary decision-making.

Emerging Doctrine: Information Advantage

In November of 2021, the Army released a draft of its new manual on information operations, Army Doctrinal Publication 3-13. Called simply *Information*, this publication is organized around the central concept of "information advantage," or the condition when a force holds the initiative in terms of the use, protection, denial, or manipulation of information. Information advantage goes to the side that possesses better information and uses that information more effectively.[184] The publication adopts a broad definition of information that encompasses its different technical and psychological meanings: Information is "data in context to which a receiver assigns meaning."[185] Data — whose collection and processing can have specific technological requirements — is ultimately meaningless without human interpretation. This definition admits that information can mean different things in different contexts, and that information doctrine must be capable of accommodating this full range of meanings.

According to this manual, the purpose of information is to contribute to decision dominance, or a state in which commanders can act more quickly and effectively than their adversary. One achieves decision dominance by engaging in information advantage activities along five lines of effort: enabling decision-making, protecting friendly information, informing domestic and international audiences, influencing foreign audiences, and conducting information warfare.[186] While all military activities can contribute to information advantage, the core information capabilities of cyberspace operations, electronic warfare, military information support operations, and public affairs have information advantage as their principal purpose.[187]

In total, draft Army Doctrinal Publication 3-13 has attempted to adapt elements of the previous seven information operations frameworks to the unique strategic and technological conditions of the present age. Its description of information in terms of relative advantage has a coherence that was lacking

[180] Department of the Army, *Information Operations*, FM 3-13 (2016), vi.

[181] Department of the Army, *Information Operations*, FM 3-13 (2016), vi.

[182] John E. Bircher IV, "Proponent Adjudication of Final Draft FM 3-13, *Information Operations*, Comment Review Matrix (CRM) Critical and Major Comments," Memorandum for Headquarters, Department of the Army DCS G-3/5/7 DAMO-ODCI, Information Proponent Office, Fort Leavenworth, KS, April 8, 2016.

[183] Bircher, "Proponent Adjudication of Final Draft FM 3-13."

[184] Department of the Army, *Information Advantage*, Army Doctrinal Publication (ADP) 3-13, Initial Draft (Washington, DC: Government Printing Office, November 2021), 1-13.

[185] Department of the Army, *Information Advantage*, ADP 3-13, Initial Draft, 1-2.

[186] Department of the Army, *Information Advantage*, ADP 3-13, Initial Draft, 1-13.

[187] Department of the Army, *Information Advantage*, ADP 3-13, Initial Draft, 1-18.

in previous publications, while its treatment of the five information advantage lines of effort imperfectly reflects the three dimensions of conflict that served as the central organizing principle for the 2009 draft version of Field Manual 3-13. It remains to be seen, however, whether this new information framework will resonate with the broader force or, more importantly, whether it will resolve the organizational and cultural differences that doomed its 2009 and 2013 predecessors.

Discussion

Why has the Army struggled to create an enduring doctrinal framework to describe the role of information in conflict? More broadly, why do militaries choose one doctrinal concept over other viable alternatives, and what determines whether a new doctrine will succeed or fail? This section will offer several possible answers to these questions that are informed by the history described above.

The Organizational Determinants of Doctrine Development

The history of Army information operations offers an opportunity to assess the prevailing schools of thought on military innovation and doctrinal change, while suggesting a new argument for the process by which intra-organizational competition can affect doctrinal change outcomes. First, the salience of the 2001 *Quadrennial Defense Review* and the 2003 *Information Operations Roadmap* to the Army's internal process of doctrinal change would appear to support the argument that military change can be directed by civilian leadership outside the military. However, at least within the Army, this direction was less the originating impulse of reform than it was the validation of a pre-existing service-wide push toward information warfare that had been underway for over a decade. Moreover, while the *Information Operations Roadmap* clarified the Defense Department's vision for information operations, it did not preclude the Army from redefining information operations to its own liking in the late 2000s. The civilian-directed innovation argument is thus insufficient to fully explain the evolution of Army information doctrine.[188]

The counter-argument — that innovation can be directed by prescient leadership from within a military service — also serves as only a partial explanation of how the information doctrine story unfolded. Beginning with Westmoreland's observations in 1969 and continuing through four consecutive chiefs of staff from 1991 to 2003, senior Army leadership repeatedly demonstrated the ability to recognize changes in the character of war and the willingness to radically transform the service in pursuit of a new theory of victory.[189] However, while the Army readily embraced the premise of information-age warfare — that a technologically enabled force could leverage more and better information to substitute precision for volume in the application of combat power — the support of Army three- and four-star leadership proved incapable of successfully extending information operations into the realm of inform and influence roughly a decade later. The military-directed innovation argument is thus also insufficient to fully explain the history of Army doctrine presented above.

Similarly, inter-service dynamics fail to offer an adequate explanation for the information doctrine case study. Inter-service dynamics were evident in the Army's embrace of information warfare throughout the 1990s. Specifically, the inter-service fiscal competition of the post-Cold War environment provided a compelling incentive for the Army to adopt information operations and information technology as a way to maximize the combat power and deployability of a smaller force, counter the growing claims that land power had become obsolete,[190] and maintain its share of a defense budget that was heavily skewed toward the Air Force and

[188] Future research would do well to look at how information doctrine fared in the Navy and Air Force, particularly in response to these civilian directives. My past research into Navy and Air Force cyber doctrine suggests that these services remained steadfastly fixated on technological interpretations of information operations and suffered no internal controversy over the proper role of cognitive or psychological influence within this doctrine. This pattern makes sense, as both the Navy and Air Force are technologically oriented, platform-based services.

[189] Sullivan was admittedly heavily influenced by the writings of Alvin and Heidi Toffler, war futurists whose 1993 book, *War and Anti-War*, inspired numerous military leaders to the view that industrial-age warfare was over. However, the Tofflers did not *direct* military change, nor did they have the capacity to. The military leadership took these ideas and recognized the need for change without a need for external civilian direction. See Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (England: Little, Brown, 1993).

[190] The post-Cold War strategic environment demanded an Army that could respond quickly to a variety of scenarios in unpredictable locations, yet the Army's ponderous deployment requirements and large logistical tail often prevented it from doing so. The 1999 success of Operation Allied Force in Yugoslavia — a pure air campaign that led to the capitulation of Slobodan Milosevic — epitomized the Army's lack of strategic mobility and resulted in new claims that land power had become obsolete. The Army's central task in the post-Cold War era was thus twofold: They had to counter the theory that there would no longer be a need for large land forces in future conflict, and they had to demonstrate relevance by improving their ability to rapidly project power.

Navy.[191] However, inter-service competition failed to explain why the Army's reform efforts failed in the late 2000s — a time when the Army had bureaucratic primacy among the services and a strong operational need to adopt a more psychologically focused information doctrine.

A partial explanation for the information doctrine outcome may be found in arguments about structural reform, with specific reference to the role of new career fields and new organizations in either encouraging or stifling change.[192] The information doctrine case study affirms that structural reform is necessary to make an innovation enduring. For example, while the Army had been experimenting with information doctrine since at least 1981, it was not until after the creation of the Land Information Warfare Activity in 1995, followed soon thereafter by an information-focused career path, that information operations emerged as an institutionally viable doctrine.

However, the creation of the structural mechanisms that were necessary for information operations' initial viability had second- and third-order consequences for how the doctrine would evolve in the future. The FA30 career field, largely insulated within information operations organizations — which were themselves informed by the broader intelligence culture in which they were embedded — developed its own unique perspective on what information operations was and how it ought to be leveraged in and out of conflict. This perspective diverged from that of the service's culturally dominant maneuver community, whose attempts to redefine information operations in the late 2000s ultimately failed due to intractable intra-service disagreements.

The history described in this paper thus offers a unique contribution to our understanding of doctrinal change processes by demonstrating how intra-organizational competition can act independently of the strategic environment to affect change outcomes. In so doing, it depicts both the consequences and the limitations of military structural reform. Structural reform creates specific professional pathways and operational experiences that shape the conceptual orientations of those who participate in them. These conceptual orientations result in organizationally unique and specific interpretations of the operating environment that bear on broader questions of strategy and technology — and that determine the limit of what is considered a doctrinally appropriate response to those questions. In other words, it is not enough to argue that organizations are motivated by mere bureaucratic self-interest. Instead, they possess unique conceptual orientations that fundamentally define both how they conceive of a new problem and how they perceive their own usefulness in solving it. These perspectives will affect how the organization interprets the strategic environment, how it frames solutions to that environment, and how it interacts with other relevant actors to affect which solution is ultimately chosen.

The implications of this argument extend beyond the field of information operations. If an organization is created to solve a specific problem, born from a specific strategic and technological context, then it may be difficult to redefine, reorient, or even eliminate that organization or its motivating capability when the source problem is no longer relevant, or when it is discovered that the source problem can be tackled in a different way. This difficulty is only partially explained by the prevailing organizational explanations of sunk costs and bureaucratic interests. A more complete explanation should take into account the organization's metaphysical perspective — a perspective in which the organization legitimately cannot conceive of a world in which its function is not important, could be performed in any other fashion, or could be performed by anyone else.[193] In the grand scheme of military change, it is relatively easy to create new structural appendages and to equate the existence of those appendages as its own measure of effectiveness. However, it is far more difficult to determine when they have outlasted their relevance, and more difficult still to change or eliminate them.[194]

Implications for Information Doctrine

In addition to clarifying our understanding of the process of doctrinal reform, the history described in this paper offers additional insights into why information, as a concept, has proven uniquely difficult to tame doctrinally. The word "information" pos-

[191] Numerous sources from internal Army discussions in 1991 and 1992 discuss downsizing and budget cuts as a critical factor in determining how Army doctrine should change. For example, see U.S. Army Training and Doctrine Command, "The Army in Transition," slide 29, which places its discussion of doctrinal change in the context of Army downsizing from 1990 to 1995. See also, U.S. Army Combined Arms Command, "FM 100-5: Evolution or Dynamic Change?" PowerPoint Presentation, Fort Leavenworth, KS, 1992, slide 29, which lists "Army downsizing principles" as a consideration for Field Manual 100-5.

[192] Rosen, *Winning the Next War.*

[193] I will add that this perspective is exacerbated when the organization is responsible for something that demands unique technical expertise, in which case alternative points of view are often evaluated superficially according to the perceived technical credentials of the source.

[194] Future research into military change decisions that involved the elimination of core service components, such as the U.S. Marine Corps' elimination of its tank formations or the U.S. Army's elimination of long-range reconnaissance companies, would provide a fruitful exploration of this concept.

sesses irreconcilable conceptual tensions that complicate efforts to unify it into a single operational framework. As a result of these tensions, Army information doctrine vacillated between technical and psychological interpretations in mutually exclusive fashion over the course of its four-decade history. The extent to which information doctrine was institutionally accepted — and therefore the extent to which it had the capacity to endure — varied not according to its level of strategic appropriateness, but according to its conceptual proximity to the Army's core sense of purpose as well as its resonance with the Army's dominant culture.

Information operations gained its strongest institutional acceptance when it presented itself as a set of technological capabilities designed to affect an adversary in a discrete conventional conflict. This understanding was in accordance with an American way of war that favors technological solutions over human ones and that favors conventional over unconventional conflicts.[195] It suffered its weakest institutional acceptance when it presented itself as an integrating strategy designed to ensure coherence between a unit's messaging and its actions for the purpose of winning the psychological contest of wills. The former was tangible, measurable, and intellectually simple, while the latter was intangible, immeasurable, and intellectually complex. This pattern suggests that the primary determinant of an information doctrine's success at any given point in history was internal organizational dynamics rather than external strategic coherence. In other words, whether a doctrine succeeded or failed had less to do with the extent to which it was appropriate for a given strategic context, and more to do with the perceptions of internal organizational actors about that appropriateness.

The history of Army information doctrine contains three additional insights that are worth discussing further. The first is that information itself is an extraordinarily complex concept whose application to war possesses infinite versatility and variation. The versatility of its application means that there can be different types of informational challenges, and thus different interpretations of the applicability of information to war. It is likely impossible to create a single information framework that can satisfactorily encompass all these disparate meanings, and to do so in a way that is operationally useful. As a result, information doctrine should be understood within the context of the strategic environment that created it in order to ascertain what specific problems it is intended to solve. Moreover, information doctrine should take great pains to explain that strategic context and to articulate how it has influenced particular doctrinal choices.

A second insight concerns the tension between technical and psychological interpretations of information. This tension has been at the heart of Army information operations doctrine for the past 40 years and is one of the reasons why creating a single, unified doctrine has been so difficult. The tension between psychological and technical interpretations of information was most evident in the doctrinal changes that took place during the Global War on Terror. This phase featured a decisive shift away from the language of "effects" and toward the language of "influence," with a focus on shaping perceptions rather than targeting information systems. "Information operations" as a term was replaced with "inform and influence," while the technical component of information operations was codified in separate doctrine on cyberspace and electromagnetic activities.

However, while the overt information doctrine changed, the Army never changed the definition of "information" upon which the new cognitive framework rested — nor did it change the organizational infrastructure that had been built to service this technical interpretation of information operations. The resulting doctrine employed information as a tool for affecting perceptions, but held an implicit understanding of information — and an information organizational infrastructure — that was based upon information as data. Moreover, the new inform and influence activities concept was poorly aligned to both the prevailing institutional culture and the micro-organizational culture of the information operations community, which favored discrete, measurable, and technological solutions to information problems. The result was a doctrine that was widely misunderstood, poorly executed, and short-lived, despite its overall appropriateness for the strategic environment in which the Army found itself.

While this tension between technical and psychological applications of information is endemic to the Army's doctrinal history, the controversy over this tension is not inevitable. Reconciling it demands a more compelling articulation of the relevance of the psychological dimension to the central activities of war — one that reflects the manner in which this dimension is enabled by the technological realities of the information age. It also requires breaking down both the policy and structural impediments to closer collaboration between the psychological and technical communities. At present, responsibility for considering the psychological

[195] Colin S. Gray, "The American Way of War," *Rethinking Principles of War*, ed. Anthony D. McIvor (Annapolis, MD: Naval Institute Press, 2005), 13–40.

dimension is relegated to a small sub-component of Army special operations. This component remains largely distinct from both the conventional force and from the cyber force, which has default responsibility for the technological component of information operations.[196] Importantly, the Army should also figure out how to measure the effectiveness of activities in the cognitive space, the failure of which contributed substantially to the difficulties of inform and influence doctrine during the Global War on Terror.

Despite this measurement problem, the present age of digital connectivity and diffuse information sources has made evident that information and influence can affect war outcomes.[197] In China, war over Taiwan might be avoided by influencing the Chinese Communist Party's perception of its ability to successfully seize the island, or its perception of the long-term costs of war.[198] In Russia, war with Ukraine might slow to an end through the manipulation of relevant senses of national identity or the erosion of internal Russian popular support.[199] While exerting this level of national strategic influence may extend outside the Army's purview, there is little reason why the Army's conception of the information dimension of conflict ought to preclude or minimize it.

However, effective information doctrine should also address the opposite problem, in which a bias for the technological aspect of information results in overly narrow measures of effectiveness that do not communicate an operation's real impact. The ease of creating cyber personas or posting online content, for example, should not allow mere posting volume to substitute for an analysis of the posts' effectiveness.[200] Likewise, simply tossing content into the digital ether to "counter" a near-peer adversary, absent the specific ability to determine that content's impact, should not be misconstrued as a viable influence campaign.

A final insight is perhaps the most obvious one: that Army information doctrine has experienced consistent, frequent, and often radically vacillating change since its inception. With the exception of the period from 1981 to 1991, when the doctrine was at its most primitive, the Army has never had an opportunity to build meaningful capacity around a single doctrinal construct. From the time of its formal recognition with the 1996 Field Manual 100-6, Army information operations was always under resourced and over extended, and thus was incapable of making a reality the vision that its written doctrine had laid out. This lends credence to the argument put forth by the FA30 community in 2009: that information operations' operational struggles were less the result of a failed concept than an under-resourced one.

When taken together with the inherent complexity of information as a concept, the frequent changes to information doctrine offer an additional answer to this paper's motivating inquiry: Why has the Army struggled to create an enduring doctrinal framework for information? The very lack of doctrinal consistency over time created a perpetual confusion as to what, exactly, information operations was supposed to offer to the force. This confusion then contributed to the field's inability to gain widespread, enduring institutional acceptance. Current doctrine, while clearly written in the spirit of its predecessors, fails to offer any clarity on this fundamental question of what information operations is. It instead argues that Army units "employ information operations to create effects in and through the information environment" — a rigorously tautological take that fails to explain how information operations creates effects, what those effects could or should be, or how the success of those effects ought to be measured, all while creating an artificial sense of distinction between the "information environment" and the rest of a unit's operating space that fails to capture the pervasive reality of the information age.[201]

[196] Conventional units will receive psychological operations planners to serve on staff during major training rotations, but lack recurring touchpoints into the psychological operations world outside of these infrequent events. Likewise, periodic integration between cyber and psychological operations does nothing to address either the policy or broader structural separation that exists between these communities.

[197] T.S. Allen and A.J. Moore, "Victory Without Casualties: Russia's Information Operations," *Parameters* 48, no. 1 (2018): 59–71, https://doi.org/10.55540/0031-1723.2851; Theodore W. Kleisner and Trevor T. Garmey, "Tactical TikTok for Great Power Competition: Applying the Lessons of Ukraine's IO Campaign to Future Large-Scale Conventional Operations," *Military Review*, April 2022, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2022/KleisnerandGarmey/Kleisner-Garmey.pdf.

[198] David C. Gompert, Astrid Stuth Cevallos, and Cristina L. Garafolla, *War with China: Thinking through the Unthinkable* (Santa Monica, CA: RAND Corporation, 2016).

[199] For a good summary source on the role of identity in Russian imperial strategy, see Jeffrey Mankoff, "Russia's War in Ukraine: Identity, History, and Conflict," Center for Strategic and International Studies, April 22, 2022, https://www.csis.org/analysis/russias-war-ukraine-identity-history-and-conflict.

[200] Naomi Nix, "Facebook, Twitter Dismantle a U.S. Influence Campaign about Ukraine," *Washington Post*, Aug. 24, 2022, https://www.msn.com/en-us/news/world/facebook-twitter-dismantle-a-us-influence-campaign-about-ukraine/ar-AA113HY4. The article states that "the vast majority of posts and tweets we reviewed received no more than a handful of likes or retweets."

[201] Department of the Army, *Information Operations*, FM 3-13 (2016), vi.

The lack of doctrinal consistency or clarity is especially salient when one considers that information operations, as a low-density career field without a significant champion among senior leadership, has never enjoyed a position of relative advantage with respect to the Army's central culture or organizational priorities. If information operations — whatever that might be — is as vital to the conduct of future warfare as 40 years' worth of commentary suggests it is, then it must possess a level of institutional prestige that is commensurate with the Army's favored functions of fire and maneuver. This is a cultural problem as much as it is a doctrinal one. The prestige of information operations, in turn, will depend on a clear demonstration of how the function can assist the Army with the accomplishment of its core missions, along with a clear emphasis on the relevance of informational and cognitive effects to combined arms operations. The reality is that *all* of a unit's capabilities can achieve cognitive effects — not just those that are clearly information related. However, until the Army decides upon an enduring information construct, it will be impossible to demonstrate its effectiveness or for it to gain long-term institutional acceptance.

The complexity of information as a concept offers an additional lesson on the distinction between creating a doctrine that is institutionally viable and creating one that is efficacious.[202] Structural reform is necessary to create viable doctrine, one that will outlast leadership changes and survive the residual frictions produced by any large-scale change. However, just because a doctrine is viable — in other words, just because a doctrine is accepted by the institution — does not mean that it is either strategically correct or operationally effective. The challenge of information doctrine thus presents two separate but related problems. On the one hand, the Army must create an information doctrine that resonates with the broader institution and its core sense of purpose. On the other hand, however, the Army must create a new way of war that conceptually unifies the disparate threads of the information age — one that, for example, speaks to the unique technological vulnerabilities of modern military systems,[203] while acknowledging the historically unparalleled potency of influence in the digital age.[204] Perhaps, then, the historic struggle of information doctrine is less an indictment of the doctrine itself than it is of the underlying theory of victory upon which the doctrine must be built.

__Sarah P. "Sally" White__ is an Army cyberspace operations officer and former assistant professor of international affairs in the West Point Department of Social Sciences. She holds a Ph.D. in political science from Harvard University and has operational experience in both joint and Army cyber organizations as well as in the special operations community.

The views expressed in this article are the author's own and do not represent the U.S. government, Department of Defense, or the U.S. Army.

[202] For more on the puzzle of why some innovations enhance combat effectiveness while others do not, see Kendrick Kuo, "Dangerous Changes: When Military Innovation Harms Combat Effectiveness," *International Security* 47, no. 2 (Fall 2022): 48–87, https://doi.org/10.1162/isec_a_00446.

[203] Bruce Schneier and Tarah Wheeler, "Hacked Drones and Busted Logistics are the Future of Cyber Warfare," Brookings Tech Stream, June 4, 2021, https://www.brookings.edu/techstream/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/.

[204] Kleisner and Garmey, "Tactical TikTok."