A Call for Synchronization of Civil Information Management

by Michael L. Jones

Special operation forces (SOF) and interagency partners face unique challenges when conducting civil information management (CIM) within the joint interagency, intergovernmental, and multinational (JIIM) environments. Information management requires a streamlined technologic system that reduces redundant technological platforms for civil information sharing. Currently, there are more than ten platforms that exist between the military and interagency that are capable of synchronizing and distributing civil information. The lacking definitive definition of collaboration and the necessary technology solution that facilitates streamlined civil information sharing between the Department of Defense (DoD) and the interagency create problematic resistance barriers to streamlined information sharing.

Synchronizing CIM systems improves the sharing of civil information throughout the JIIM. SOF and the interagency community (IC) have successfully shared information, to include civil information and intelligence, foiling more than 60 terrorist attacks against the U.S.[1] Information sharing and deconfliction requires significant synchronization.[2] Successful CIM depends on streamlining organizational processes, synchronizing assets, and developing priorities.

Technology provides the necessary software and infrastructure solutions needed for collaborative analysis of civil information that can be leveraged by combatant commanders to inform and influence the decision-making cycle to achieve strategic success. Streamlining technological infrastructure enables organizations operating within the JIIM to maximize the use of civil information. Technology is the driving factor of synchronization.[3] The United States Special Operations Command (USSOCOM) has built one of the most network-centric organizations, with the capability to collaborate across military and civilian networks.[4] Utilizing a joint program of record for CIM,[5] capable of framing the civil domain by synchronizing civil information in the multilateral JIIM environment would increase efficiency and collaboration.

Major Michael L. Jones is a civil affairs officer assigned to the 96th Civil Affairs Battalion (Airborne) and is currently deployed in support of Operation Inherent Resolve. He received a master's in Global and Interagency Studies from Kansas University, and has multiple deployments to the U.S. Central Command area of responsibility.

Literature Review

SOF face multilateral challenges in maximizing civil information sharing. Multilateral challenges exist in two areas: lack of common policy that enables synchronization and collaboration of civil information between SOF and the interagency when conducting special warfare[6] and the resistance to streamlining organizational and technological systems for the goal of creating transparency. Concise definitions for the conduct of interagency collaboration are lacking and often overlap with other definitions necessary for collaboration within the JIIM; for example, a Congressional Research Service (CRS) search of Lexis-Nexis revealed 21 examples of interagency collaboration that lacked a definitive definition.[7] Multilaterally, these challenges exist for coalition forces and host nation partners.

The development of cohesive policy for the conduct of civil information sharing will shape future successes by streamlining mission command infrastructure technologies...

The multilateral approach to special warfare activities in the JIIM environment has seen successes that range from the Office of Strategic Services in World War II to Operation Enduring Freedom. Developing multilateral relationships among partnered nations, interagency organizations, and the military must focus more on operational efficiency and less on source protection.[8] The development of cohesive policy for the conduct of civil information sharing will shape future successes by streamlining mission command infrastructure technologies, while promoting efficiency and reducing organizational resistance to collaboration.

The CRS examined current agreements and activities to enhance joint efforts among federal agencies, shared responsibilities, and overlapping jurisdictions. Collaboration is defined as "any joint activity by two or more organizations that is intended to produce more public value than could be produced when the organizations act alone."[9] Precise definitions for conducting interagency collaboration are lacking and often overlap with other definitions that are necessary for JIIM collaboration. Lacking and overlapping collaboration policies create information-sharing resistance. The Government Accountability Office (GAO) loosely defines collaboration as two or more organizations contributing for greater gain and is generically considered to be cooperation. The GAO found that the generic interpretation of collaboration within the interagency community has created seven types of collaboration, 34 overlapping definitions, and 200 collaborative devices, many of which were determined to hinder matters of national security.[10]

Leaders within the interagency community identify the lack of authority and legislative policy as key elements that hinder collaboration, which are further complicated by a multitude of information technology solutions that do not easily facilitate information sharing. The CRS cites the changing nature of government organizations, politico-economic pressure, overlapping agency responsibilities and jurisdictions, and crisis response as rationales for definitive improvement in collaboration and coordination.[11] The CRS suggests that resolution begins with eliminating fragmented policymaking and implementing collaborative policies that mitigate redundancies and provide clear directives and jurisdictions for interagency collaboration.

In the conduct of special operations, literature trends associated with CIM indicate that information sharing is critical to operational success in a complex environment.[12] Dawes indicates the benefits of improved efficiency

outweigh the associated risk of misuse of information and data management. Policymakers face significant challenges, such as organizational resistance, organizational discretion, and multiple networks, when developing clear procedures for information management and utilization across multiple agencies and systems.[13] Current data indicates that there is not a standardized system for synchronizing multiple CIM technology platforms. The value and impact of collaborative civil information sharing are not effectively measured. The literature reviewed does not reflect measurable effectiveness statistically; rather, effectiveness is reflected through opinion polls of nongovernmental organizations (NGOs). Although NGO input is valuable, it does not accurately depict the effectiveness of information sharing given the differing nature of NGO humanitarian operations when compared to special operations conducted by USSOCOM. Civil information sharing provides a unique representation of the human domain that when shared among different agencies and organizations increases productivity and improves policymaking.[14] The associated cost of network infrastructure development and management is a limiting factor for synchronizing civil information.[15] The cost of network system development and management warrants further research to determine the impact with the associated cost, creation, implementation, and management of information sharing. USSOCOM has approved the capabilities and production document enabling United States Army Special Operations Command (USASOC) to secure fiscal year 2017 funding for the transition of the Civil Information Management Data Processing System (CIMDPS) to the Joint Civil Information Management System (JCIMS).

This article analyzes the correlation between the normative value of civil information sharing and the conduct of CIM in the JIIM. Can reducing the number of information systems improve the sharing of civil information across the JIIM while improving relationships throughout the SOF enterprise? Based on the data presented and literature reviewed from Hun, Beadenkopf, Kaiser, Carafano, and Hanhauser, I argue that an autonomous adaptive strategy for the standardization of CIM across a synchronized technological infrastructure will improve the conduct of special operations in the JIIM.

The associated cost of network infrastructure development and management is a limiting factor for synchronizing civil information.

Unilateral and Multilateral Challenges

Countering twenty-first century threats poses unilateral and multilateral challenges for conducting special operations in a complex JIIM environment. The evolving complexity of the global environment presents SOF with unilateral and multilateral challenges for maximizing civil information sharing. Challenges exists in three areas unilaterally: the lack of common legislation that synchronizes CIM in support of SOF and interagency operations, the conduct of special warfare[16]and irregular warfare [17] activities, and the synchronization of organizational technologies creating transparency, further building trust within the JIIM. The multilateral challenge is sharing civil information with coalition forces, host nation partners, and the interagency. Over classifying civil information limits information sharing. Accurately classifying civil information ensures the greatest dissemination of information and provides coalition forces and host nation partners access to information that is otherwise limited by classification. Likewise, the interagency shares information through internal and external

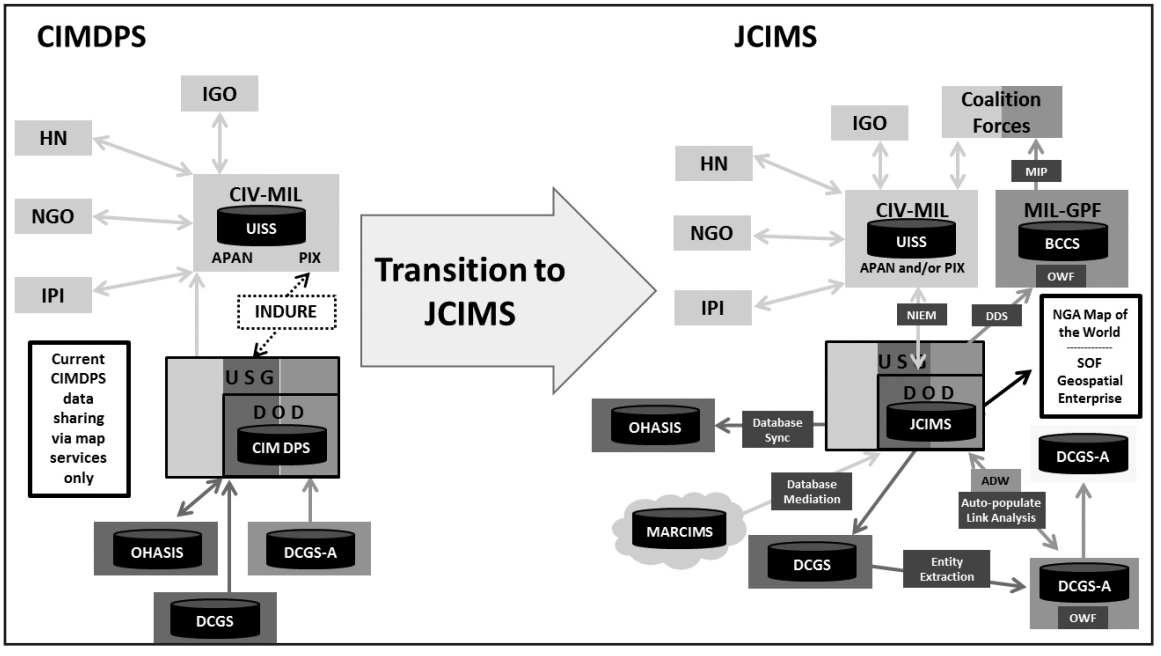

Figure 1. Transition from CIMDPS to JCIMS enhances information sharing.[18]

agreements that define the terms and authorities of the information being shared. The GAO identified 200 processes for collaboration and indicated that these overlapping procedures hinder national security.

The current complex CIM technology infrastructure limits the effective synchronization and distribution of information throughout the JIIM. Figure 1 demonstrates the current limitations and the potential gains for expanding a current civil information management program of record to a joint program of record. The benefit of expanding civil information management into a joint program of record is the facilitation of streamlined civil information sharing through an accessible information communication technology solution. The limitation of non-synchronized, civil-information databases presents a multilateral challenge that impacts the input of information from sister services, the interagency community, NGOs, and host nation partners. Providing the added dimension of civil information collected from external organizations, such as NGOs and host nation partners, expands the DoD capability to provide collaborative civil information analysis that influence strategic success.

CIMDPS is the USSOCOM program of record for synchronizing and collating civil information. USSOCOM has proposed transitioning from CIMDPS to JCIMS. The transition will broaden the global SOF enterprise by enhancing information access across the JIIM that further enables efficient coordination, collaboration, and cooperation in the pursuit of strategic effects. Data suggests that joint synchronization of the information infrastructure effectively integrates multiple operating systems for CIM and increases the efficient distribution of civil information. Streamlining the access to civil information sharing fosters collaboration and efficiency.

Civil Information Sharing Infrastructure

Information and communication technology is the driving factor for the synchronized distribution of civil information that provides accessible real-time information for rapid decision-making. USASOC has built one of the

most network-centric organizations within the JIIM, with the capability to collaborate across military and civilian networks.[19] Technology has enabled organization-centric solutions dependent upon the operating network utilized for CIM. Special operations often require the use of mobile ad hoc networks for locating, managing, and allocating resources in areas where network infrastructure may not be available.[20] The ability to establish accessible networks of different classifications is an equally-critical variable for information sharing. Mobile ad hoc networks and their classification levels in support of special operations within the JIIM environment should be considered when framing the civil domain and evaluating civil information.

Civil information management provides a detailed comprehensive understanding of the impact of the civil domain on the operational environment. Information management is equally important during offensive, defensive, and stability operations. Numerous CIM systems exist at the geographic combatant command and below. For example, United States Pacific Command (USPACOM) and United States Southern Command (USSOUTHCOM) utilize a combatant command-sponsored program called All Partners Access Network (APAN); USSOCOM utilizes CIMDPS; the United States Marine Corps utilizes the Marine Civil Information Management System; the interagency utilizes systems. such as the Overseas Humanitarian Assistance Shared Information System, APAN, and Preservation Information Exchange; while the intelligence community utilizes the Distributed Common Ground System. Each of these systems has a differing classification level and capability for information sharing that range from geographic information system file sharing to real-time chat applications.

Problematically, the multitude of information and communication technology (ICT) systems fails to provide a collaborative analysis of the civil domain within the operational environment.[21] The CIMDPS JCIMS Steering Committee suggests that transitioning CIMDPS to a joint program of record will expand the current data-sharing capability and synchronize the multitude of ICT systems across the JIIM environment. [22] In fiscal year 2017, CIMDPS will transition to a joint program of record. The joint program of record transition enables synchronization of the civil information sharing infrastructure within the JIIM, which mitigates resistance barriers associated with culture, doctrine, and best practice challenges, while providing a comprehensive streamlined access point for analysis of the civil domain.

Civil information management provides a detailed comprehensive understanding of the impact of the civil domain on the operational environment.

Guiding Directives

Within the JIIM, a concise definition for the conduct of interagency collaboration is lacking and often overlaps with other necessary collaboration definitions. To address all stakeholder interests within DoD and the Department of State, a comprehensive legislative policy that defines collaboration and establishes a protocol for information sharing is needed. DoD Directive (DoDD) 2000.13 addresses the need to synchronize the organization by coordinating with other government agencies, host nation militaries, and civil agencies.[23] DoDD 3000.07 provides the necessary guidelines facilitating global collaboration and civil information sharing.[24]

A definitive language for interagency collaboration is lacking.[25] The CSR suggests resolution begins with eliminating fragmented policymaking and implementing collaborative

Categories	Benefits	Barriers
Strategic (Micro)	• Synchronizes the joint network domain • Policy-guided collaboration • Accountability	• Multiple networks • Policymaker resistance • Organizational discretion
Operational	• Collaborative operational picture • Promotes strategic success	• Interagency source sharing • Organizational solutions
Tactical (Micro)	• Streamlines CIM • Expands collaboration	• Tactical organization • Change Resistance

Table 1. Jones CIM benefit/barrier comparison.

policy that mitigates redundancy and provides clear directives and jurisdictions for interagency collaboration. The lack of a common policy definition for CIM within the JIIM environment creates the greatest challenge—providing clear procedures for the utilization and management of information across multiple entities.[26] DoDD 2000.13, and 3000.07 begin to synchronize the organizational infrastructure for civil information sharing and collaboration. Hun et al. suggest further collaborative policy is needed to mitigate secrecy and promote efficiency within the JIIM.[27] Arguably, a multitude of policy and directives exist to foster collaboration. A strategy for integration that stems from collaboration across the JIIM and utilizes a synchronous information communication technology solution is a more feasible approach.

Successful Information Sharing

Special Operations Command (SOCOM) 2020 positions SOF to be globally networked throughout the JIIM to rapidly and persistently address regional threats to stability. In support of the National Defense Strategy, collaborative information sharing has manifested success in the integration of SOF, conventional, and interagency counterparts. Successful information integration is dependent upon flattening the organization, synchronizing systems, information collection assets, and intelligence development priorities. Table 1 demonstrates the potential benefits and possible barriers associated with synchronizing civil information management.

Strategic success, that is the ability to implement operational systems that produce predictable outcomes and directly contribute to the decision-making process, is rarely defined by a specific accomplishment. Civil information sharing has mitigated the threat of terrorism against the U.S., improved global military and interagency effectiveness, and reduced unnecessary expenses associated with information and communication technology development. Strategic success has directly resulted from civil information sharing within the JIIM.

Since the Heritage Foundation began tracking post 9/11 foiled terrorist attacks against the U.S. in 2007, 69 foiled terrorist plots have been reported.[28] Increased information sharing between the U.S. and its allies has improved interagency communications among the State Department, the Department of Justice, the Department of Homeland Security, and the interagency community, and support for NATO and U.S. counterinsurgency strategies in Afghanistan, as well as for missions around the globe, are eliminating terrorist safe havens.[29] Information sharing ensures the comprehensive domestic counterterrorism enterprise is capable of understanding the evolving complex terrorism threat in the strategic defense of the U.S.[30]

Successful information sharing requires significant synchronization and deconfliction.[31] The Heritage Foundation study demonstrates the effectiveness of collaborative civil information sharing. Civil information provides the operational picture of the human domain that supports military and interagency operations. The complexity of the emerging terrorism threat underscores the importance of global collaboration and cooperation. Collaboration and cooperation is a move beyond the independent centers of excellence within the geographic combatant commands and the interagency community. Sharing civil information across the JIIM environment requires an autonomous adaptive approach encompassing both the military and interagency to accomplish organizational synchronization.

Discussion

This discussion reviews the benefits and challenges of synchronizing CIM to increase effective collaboration within the JIIM and proposes future research recommendations. Can synchronizing the numerous CIM systems through a singular ICT infrastructure, such as JCIMS, improve civil information distribution throughout the JIIM? An examination of current DoD policies, USSOCOM guiding directives, and military-interagency information sharing success trends identifies three issues: defining the definition of interagency collaboration within the JIIM, synchronizing a complex ICT infrastructure, and developing a multilateral policy for sharing and synchronizing civil information.

Synchronizing CIM requires an autonomous adaptive approach to establish a definitive definition of collaboration, facilitate information sharing within the joint interagency environment, and fully implement the transition to JCIMS across the levels of war (strategic, operational, and tactical). Information and communication technology intensive systems, such as JCIMS, must synchronize data received from the operational environment and interact across the JIIM to provide the geographic combatant commander with an operational framework of the civil domain. Civil information management synchronization cannot be accomplished with an autonomous software solution. Synchronizing civil information requires an autonomous adaptive strategy of personnel and technology to monitor the internal system (JCIMS) and the operational environment. Information providers, system operators, and network technicians are the adaptive elements that enable the autonomous element (software) to provide the civil domain common operating picture. In addition to the autonomous, adaptive strategy, guiding policies that standardize collection and input of civil information between the DoD and the interagency are needed. Establishing guiding policy can mitigate the confusing interagency collaborative framework identified by the GAO. An autonomous, adaptive system strategy enables stakeholders to shape diverse policies into common language that benefits numerous agencies throughout the joint interagency environment. An autonomous, adaptive system strategy enables users at the strategic, operational, and tactical levels of war to implement the transition to the JCIMS. Utilization of multilateral guidelines maintains the SOF capacity to frame the civil domain providing the geographic combatant commanders the ability to adapt to emerging twenty-first century threats.

Synchronizing civil information requires an autonomous adaptive strategy of personnel and technology to monitor the internal system (JCIMS) and the operational environment.

Support for Standardization

United States Army Special Operations Command and other government agencies have each established separate, non-synchronized, CIM systems to support their operations. There is organizational support for standardizing the collection and management of civil information within the DoD. Army Special Operations Forces (ARSOF) 2022 establishes a benchmark for the development of a standardized system for information sharing. Standardizing information management operations within the JIIM environment is an extensive, large-scale implementation that will require multilateral agreement upon guiding legislation that solidifies the practices across the DoD and the interagency community. Synchronizing CIM policy and systems cannot be broken down into smaller policies until a clear policy that synchronizes information collaboration is established. Policy implementation requires complex utilization of policy, power, and negotiation.[32] Additional policy alone will not facilitate improved information management. Improving information management also requires an effective ICT solution that is user friendly and accessible across the joint environment. Utilizing an autonomous, adaptive strategy of people and technology for the implementation of the JCIMS program of record enhances the synchronization by mitigating the associated time and cost of developing an autonomous software solution.

The nature of conflict is evolving into an ill-defined, complex, grey area of political conflict teetering on the verge of full-spectrum conflict. The strategic challenge facing the DoD and the interagency is adopting and implementing a concise policy for collaboration and the conduct of CIM. Synchronizing the multitude of information and communication technologies systems is an essential element of maintaining an interconnected, joint enterprise capable of addressing complex and emerging threats. Expanding the current U.S. Army program of record for CIM into a joint program of record is a significant move toward multilateral synchronization and is scheduled to go into effect fiscal year 2020. There remains a need for unified policy that establishes concise definitions of collaboration and synchronization between the military and interagency. Utilizing an autonomous, adaptive strategy for implementing a joint CIM program will improve information collection, enhance collaboration, and improve trust within the JIIM. Through the application of comprehensive CIM, framing the civil domain enables informed operational development, which influences strategic success. ***IAJ***

NOTES

1 David Inserra, "69th Islamist Terrorist Plot: Ongoing Spike in Terrorism Should Force Congress to Finally Confront the Terrorist Threat," Heritage Foundation Issue Brief #4416 on terrorism, June 8, 2015, <http://thf_media.s3.amazonaws.com/2015/pdf/IB4416.pdf>, accessed on May 23, 2016.

2 Ronald Beadenkopf, "Conventional Forces Intelligence Integration with Special Operations Forces in Support of Operation Iraqi Freedom III," Joint Special Operations University and National Defense Intelligence Agency SO/LIC Division Essays, 2007.

3 Yasser Gadallah et al., "Middleware Support for Service Discovery in Special Operations Mobile Ad Hoc Networks," *Journal of Network and Computer Applications*, Vol. 33, Issue 5, September 2010, p. 611.

4 Jon R. Lindsay, "Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations," *Journal of Strategic Studies*, Vol. 36, Issue 3, 2013, pp. 422–453.

5 Joint Publication 3-57, *Civil Military Operations*, September 11, 2013, p. GL-6. Civil information management (CIM). Process whereby data relating to the civil component of the operational environment is gathered, collated, processed, analyzed, produced into knowledge products, and disseminated.

6 Army Doctrine Reference Manual 3-05, *Special Operations*, August 2012, p. 1-5. Special warfare activities involve the ability to operate within the population—specifically, to address sociocultural factors by understanding the culture of the population.

7 Frederick M. Kaiser, "Interagency Collaborative Arrangements and Activities: Types, Rationales, Considerations," Congressional Research Service report to Congress, May 31, 2011.

8 Lee Jae Hun et al., "Countering 21st Century Threats: The Need for an Increased Joint, Interagency, Intergovernmental and Multinational (JIIM) Approach to Irregular Warfare," *Small Wars Journal*, January 6, 2015.

9 Kaiser

10 Ibid.

11 Ibid.

12 Beadenkopf and Susan S. Dawes, "Interagency Information Sharing: Expected Benefits, Manageable Risks," *Journal of Policy Analysis and Management*, Vol. 15, Issue 3, June 1996, pp. 377–394.

13 Kaiser and Robert David Steele, "Intelligence Reform: More Needs to be Done," commentary and reply, *Parameters*, Vol. 35, Issue 2, Summer 2005, p. 135.

14Dawes.

15 Gadallah and Lindsay.

16 Ibid and Army Doctrine Reference Manual 3-05, *Special Operations*.

17 Joint Publication 1-02, *Department of Defense Dictionary of Military and Related Terms*, April 12, 2001, p. 280. Irregular warfare. A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary's power, influence, and will. Also called IW.

18 United States John F. Kennedy Special Warfare Center and School Civil Information Management Data Processing System (CIMDPS)/Joint Civil Information Management System Steering Committee (JCIMS) Presentation, May 2015, Fort Bragg, NC, slide 7, "CIMDPS/JCIMS Steering Committee Minutes," May 20, 2015, <https://wss.apan.org/2476 /CIMDPSJCIMS Steering Committee/Steering Committee/CIMDPS-JCIMS Steering Committee_20May2015x.pdf>, accessed on June 2, 2016. United States John F. Kennedy Special Warfare Center and School is the U.S. Army Proponent for Civil Affairs and as a Requirements Manager conducts JCIMS Working Groups and Steering Committees to capture CIM requirements. The Committee consists of joint services, active, and reserve component civil affairs leadership and interagency representation.

19 Lindsay.

20 Gadallah.

21 George J. Hanhauser, IV, "Comprehensive Civil Information Management: How to Provide It," Strategy Research Project, U.S. Army War College, Carlisle Barracks, PA, April 2012, p. 22.

22 United States John F. Kennedy Special Warfare Center and School Civil Information Management Data Processing System/Joint Civil Information Management System Steering Committee Presentation.

23 John M. Deutch, "Civil Affairs," Department of Defense Directive Number 2000.13, The White House, Washington, DC, June 27, 1994, pp. 2–3 and 25.

24 Gordon England, "Irregular Warfare," Department of Defense Instructions Number 3000.07, The White House, Washington, DC, December 1, 2008, pp. 2–3.

25 Kaiser.

26 Kaiser and Steele.

27 Hun et al.

28 Inserra.

29 Steven Bucci et al., "Fifty Terror Plots Foiled since 9/11: The Homegrown Threat and the Long War on Terrorism," The Heritage Foundation, April 25, 2011.

30 Steven Bucci et al., "60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism," The Heritage Foundation, Special Report #137 on terrorism, <http://thf_media.s3.amazonaws.com/2013/pdf/SR137.pdf>, accessed on May 23, 2016.

31 Beadenkopf.

32 Patrick E. Connor et al., *Managing Organizational Change,* 3rd ed., Praeger, Westport, CT, 2003.