The Simons Center
Fort Leavenworth, Kansas

InterAgency Journal

The Journal of The Simons Center
Vol. 5, Issue 2, Summer 2014

InterAgency Journal

The *InterAgency Journal* (*IAJ*) is published quarterly by the Command and General Staff College Foundation Press for the Arthur D. Simons Center for Interagency Cooperation. The *InterAgency Journal* is a national security studies journal providing a forum for professional discussion and the exchange of information and ideas on matters pertaining to operational and tactical issues of interagency cooperation, coordination, and collaboration.

Contributions: The Simons Center encourages the submission of original articles based on research from primary sources or which stem from lessons learned via personal experiences. For additional information see "Simons Center Writer's Submission Guidelines" on the Simons Center website at www.TheSimonsCenter.org/publications.

About The Simons Center

The Arthur D. Simons Center for Interagency Cooperation is a major program of the Command and General Staff College Foundation, Inc. The Simons Center's mission is to foster and develop an interagency body of knowledge to enhance education at the U.S. Army CGSC while facilitating broader and more effective cooperation within the U.S. government at the operational and tactical levels through study, research, analysis, publication, and outreach.

About the CGSC Foundation

The Command and General Staff College Foundation, Inc., was established on December 28, 2005 as a tax-exempt, non-profit educational foundation that provides resources and support to the U.S. Army Command and General Staff College in the development of tomorrow's military leaders. The CGSC Foundation helps to advance the profession of military art and science by promoting the welfare and enhancing the prestigious educational programs of the CGSC. The CGSC Foundation supports the College's many areas of focus by providing financial and research support for major programs such as the Simons Center, symposia, conferences, and lectures, as well as funding and organizing community outreach activities that help connect the American public to their Army. All Simons Center works are published by the "CGSC Foundation Press."

The CGSC Foundation is an equal opportunity provider.

InterAgency Journal

Vol. 5, Issue 2, Summer 2014

Arthur D. Simons Center
for Interagency Cooperation

P.O. Box 3429
Fort Leavenworth, Kansas 66027
Ph: 913-682-7244
Fax: 913-682-7247
Email: office@TheSimonsCenter.org
Web site: www.TheSimonsCenter.org

Publisher/Editor-in-Chief
Raymond D. Barrett, Jr.

Mananging Editor
Elizabeth Hill

Copy Editor
Valerie Tystad

Design/Production
Mark H. Wiggins
MHW Public Relations

Printing
Allen Press, Inc.
Lawrence, Kansas

Features

Worth Noting

Worth Noting *(cont'd)*

Book Review

Losing Lessons at the Water's Edge:
Applying FEMA's Interagency Coordination Doctrine to International Stabilization and Reconstruction Operations

by Benjamin Cabana

There are two things for certain when it comes to the study of the interagency process for successful stabilization and reconstruction operations. First, a successful operation requires the coordinated application of the three tools of U.S. foreign policy—diplomacy, defense, and development. Second, the successful coordination of the U.S. government agencies and departments that hold these tools has been critically ineffective. The vast majority of literature on interagency coordination has focused either on increased training and collaboration efforts or on structural reorganization to remedy the problem. On the surface, this is a logical approach. There are two schools of thought when it comes to achieving cooperation across independent organizations. Either you build trust and familiarity across independent partners to increase the willingness and ability to work together, or you merge them under one umbrella, in fact removing the separateness altogether. The first approach is problematic because it relies solely on the willingness of the parties involved to cooperate. If parties want to cooperate, they may, but if they do not wish to do so, this approach is doomed. Lessons from Iraq, Afghanistan, and beyond demonstrate that Soldiers and diplomats often do not tend to cooperate, so policymakers should not rely solely on mutual volition to improve the interagency process. The second approach is equally flawed because the conduct of complex contingency operations is not the primary function of any of these organizations. Unity of effort must take place amidst an operation, but this does not change the fact that each agency is rightfully independent in their day-to-day operations. The reasonable conclusion is that neither pure cooperation nor ultimate unification is possible, some sort of hybrid is necessary. The solution must include strong mechanisms for operational coordination, while respecting each organization's autonomy.

Interagency coordination for international stability operations is largely conducted on an ad hoc basis. Each time the U.S. government finds itself conducting an international operation, it constructs mechanisms for interagency coordination anew, and after each failure, lessons learned

Benjamin Cabana is a program analyst with the Federal Emergency Management Agency (FEMA) and is a member of the National Response Coordination Staff. Cabana served in the National Response Coordination Center during Hurricanes Sandy and Isaac. He earned his Master's Degree in Peace Operations Policy from George Mason University's School of Public Policy.

are forgotten before they can be indoctrinated. Domestically, the federal government has indoctrinated an effective interagency process across various agencies and jurisdictional authorities. The skeptic will quickly dismiss any correlation, arguing that responding to a hurricane domestically is far different than trying to bring peace and democracy to Iraq.

Only within the past decade has the homeland security apparatus standardized tools for domestic incident response.

However, upon further examination, this author contends that emergency management offers valuable lessons to foreign policy practitioners. The issue at hand is one of process, not mandate. The Federal Emergency Management Agency (FEMA) coordinates federal assistance of seven cabinet-level departments and two independent government agencies which have **lead** responsibilities for aspects of a large-scale disaster response. America's federal system of government also poses challenges because the federal government must coordinate activities with the state and local governments with primary security mandates. Despite the challenges, FEMA has created binding doctrine that governs how the U.S. government holistically conducts domestic emergency response—which has inspired similar doctrine around the world.[1] This article seeks to demonstrate the applicability of FEMA's model and calls for academia and foreign policy practitioners to consider the application of this largely untapped and useful field of study to improve interagency coordination during complex contingency operations that take place outside U.S. borders.

Domestic Incident Response: The National Response Framework (NRF) and National Incident Management System (NIMS)

In domestic emergency response, the Department of Homeland Security (DHS) has developed a systematic approach to interagency coordination through the NRF and the NIMS. Only within the past decade has the homeland security apparatus standardized tools for domestic incident response. Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*, published in February 2003, directed the Secretary of Homeland Security to develop a national response plan and the NIMS to manage the complex task of coordinating response activities across the federal government and in cooperation with state and local governments.[2] The two documents work hand in hand. The NIMS provides the template for the management of domestic incidents, and the NRF provides the structure and mechanisms for national-level policy for incident management.[3] HSPD-5 requires all federal departments and agencies to implement NIMS, and its application is a requisite for state and local governments to receive preparedness assistance.[4] Both documents were developed through a collaborative partnership across the federal government and in cooperation with state and local governments and private and non-profit sectors.[5]

The current NRF is a third-generation document. The founding document, the 1992 Federal Response Plan, focused primarily on federal roles and responsibilities in incident response.[6] The original National Response Plan mandated by HSPD-5 superseded the Federal Response Plan, until it was superseded by the current NRF in January 2008, based on lessons learned from Hurricane Katrina. The framework is a "guide to how the nation conducts all-hazards response."[7] Recognizing that new administrations make the application of long-

term lessons and best-practices challenging, the NRF is intended to provide a "playbook" to ensure that consistent and proven capabilities are maintained and continuously applied in emergency response.[8] The NRF broadened the scope of the National Response Plan to explain the roles and responsibilities of all parties to incident response, not just those of the federal government.[9]

Federal and other agencies carry out their emergency response responsibilities within the mechanisms established in the NRF.[10] The NRF assigns federal response coordination to the Secretary of Homeland Security. The Secretary's coordination role does not in any way impede other departments and agencies or state or local partners from carrying out their responsibilities.[11] FEMA coordinates the response activities across the federal government and of certain nongovernmental organizations (NGOs) by activating 15 emergency support functions (ESF). Each ESF has a lead and supporting agencies, and these 15 ESFs, applied together, constitute a holistic response to any incident.

At the field level, the NRF mandates joint field offices be established to coordinate federal, state, local, private sector, and NGO actors, according to organizational principles of the NIMS.[12] A unified coordination group (NIMS unified command), consisting of senior officials with primary statutory and jurisdictional responsibilities for the response,[13] oversees the operation. The Federal Coordinating Officer is a senior FEMA official appointed to coordinate federal support, to execute Stafford Act authorities, and to execute mission assignments for other departments and agencies.[14] The Federal Coordinating Officer interfaces with state and local authorities to determine priorities and objectives for the federal response, and the Defense Coordinating Officer is responsible for coordinating Department of Defense (DoD) activities with civilian responders.[15]

The NRF also establishes consistent planning requirements. A strategic guidance statement and strategic plan define broad national strategies, establish objectives and responsibilities, and determine performance measurement strategies. A national-level interagency concept plan describes concepts of operations for integrating federal capabilities to meet objectives established in the strategic plan. Finally, federal departments and agencies create operations plans to describe how they will allocate resources and personnel to support the concept plan objectives.[16]

The NRF's counterpart, the NIMS, is flexible enough to be used for management of any incident, regardless of size, complexity, cause, or location.[17] It establishes a standard organizational structure for management of operations and allows agencies with different legal, geographic, and functional authorities to work together effectively without impeding individual organizations' authorities, responsibilities, or accountability through unified command.[18] Within a unified command, the leaders of each organization jointly determine objectives, strategies, plans, resource allocation, and priorities. A single set of objectives is established, and the efforts of all participating agencies are performed under a single incident action plan.[19] The effectiveness of the NIMS is enhanced because it is used across the entire U.S. emergency management community, not just by federal responders. The National Integration Center manages NIMS implementation, training, administration,

The NRF's counterpart, the NIMS, is flexible enough to be used for management of any incident, regardless of size, complexity, cause, or location.

and revision, and ensures that state and local jurisdictions are compliant with and proficient in NIMS.[20]

The NIMS is built around a common and proven command and management system: the Incident Command System (ICS). The ICS, initially developed in the 1970s in California to coordinate firefighting forest fires across multiple jurisdictions, is designed to enable efficient management of any incident. It consists of six functional areas—command, operations, planning, logistics, finance/administration, and intelligence/investigations.[21] It is based on 14 proven management characteristics that strengthen efficiency—common terminology, modular organization, management by objective, incident action planning, manageable span of control, incident facilities and locations, comprehensive resource management, integrated communications, establishment and transfer of command, chain of command and unity of command, unified command, accountability, dispatch/deployment, and information and intelligence management.[22] In other words, the NIMS uses proven management and organizational practices, not ad hoc systems created largely in isolation.

...the U.S. government has created an effective system of interagency coordination by incorporating organizational theory and proven management strategies into strategic doctrine...

Admittedly, the NRF and the NIMS have received their fair share of criticism over the years. However, the NRF has been far more successful than its predecessor, the National Response Plan.[23] The NIMS was initially criticized after Katrina because parallel command structures between federal and state personnel created questions of authority and complicated responsibilities.[24] Further, state authorities lacked sufficient knowledge of the NIMS, had confusing jurisdictions and authorities, and operated under different leadership styles.[25] This criticism was largely unfair, because the NIMS was designed to provide a mechanism for joint command without imposing a central command over all partners. Ongoing training and practice of the NIMS has greatly improved its effectiveness.[26] These are living documents, and as shortcomings are learned through application, the NIMS and NRF are updated and improved. Having doctrine and improving upon it as lessons are learned is far better than having no doctrine whatsoever.

In sum, in order to improve interagency coordination in domestic complex contingency operations, the U.S. government has created an effective system of interagency coordination by incorporating organizational theory and proven management strategies into strategic doctrine that is binding across the federal government and state and local partners. The critical features that make the NIMS and NRF effective include the following:

- **Standardization**. NRF is a basic "playbook" that ensures that institutional knowledge and best practices are applied across administrations.
- **Clear lines of authority.** Roles and responsibilities are clearly delineated and defined across the U.S. government through ESFs.
- **Consistent planning.** Consistent planning requirements ensure that operations of each agency contribute to the strategic objectives for the operation
- **Autonomy of stakeholders**. DHS coordinates the response, but the autonomy

and jurisdictional authority of all U.S. government entities are respected.

- **Universal application.** Both documents apply to all incidents, regardless of size, complexity, cause, or location.
- **Consistent application.** Both documents are always in effect, ensuring that these tools are applied to all domestic response operations.
- **Binding across the U.S. government.** All federal agencies are mandated by executive order to use the NRF and NIMS.
- **Used by non-U.S. government stakeholders.** State and local governments must implement the NIMS to receive federal preparedness assistance, ensuring that all levels of government operate under the same structure.
- **Living doctrine.** The NIMS and NRF are always subject to revision based on lessons learned to improve on their content without losing the progress made thus far.

No such framework and system of management has been created for international contingency operations. The next section reviews a history of far less ambitious interagency coordination efforts for international contingency operations.

Interagency Coordination Efforts in International Operations

Presidential Decision Directive 56

President Clinton established the first interagency coordination mechanism for complex contingency operations overseas. The lessons of Somalia and Bosnia demonstrated a need to remedy the failures to coordinate planning and execution for these missions.[27] After Operation Restore Hope in Haiti applied many lessons learned from Somalia and Bosnia, Clinton sought to institutionalize these lessons so that interagency planning and coordination improvements would not be lost.[28] After two years of planning and vetting across the government, Presidential Decision Directive 56 (PDD-56) *Managing Complex Contingency Operations* created the first internal management tool for complex contingency operations.[29] The directive had five central pillars:

- A National Security Council Executive Committee provided unified planning guidance and oversaw the day-to-day management of the operation.
- A political-military plan established a whole-of-government strategy.
- Interagency rehearsals refined agency plans and unity of effort.
- Interagency after-action reviews allowed for assessment and lessons learned.
- Interagency training would create a cadre of officials with improved interagency management skills.[30]

The lessons of Somalia and Bosnia demonstrated a need to remedy the failures to coordinate planning and execution for these missions.

PDD-56 was largely focused on achieving strategic consensus in Washington, but did not seek to translate this into effective coordination at the operational level.[31] The heart of PDD-56 was the political-military plan, which would provide the strategic objectives to govern the interagency operators in the operational area.[32] After-action reviews would identify legal,

budgetary, and execution problems to ensure that future operations did not repeat these mistakes.[33] Like the NRF, PDD-56 recognized the need for ongoing improvements. However, the initiation of PDD-56 required a National Security Council judgment call or pressure from a high-level official, and the process was thus never initiated, and its utility was never demonstrated.[34] PDD-56 was a promising first-step for managing complex contingency operations, but failure to implement it left room for improvement. In sum, PDD-56 had a much smaller scope than the NRF and NIMS. The strategic planning and training requirements in PDD-56 are only two aspects of a much larger domestic response framework, and PDD-56 provided no efforts to remedy interagency coordination at the operational level.

NSPD-44 established a Policy Coordination Committee for Reconstruction and Stabilization Operations, to be chaired by the Coordinator for Reconstruction and Stabilization and a National Security Council staff member.

The Bush Administration never initiated PDD-56. Planning for operations in Afghanistan and Iraq largely removed civilian agencies from the initial planning process.[35] After three years in Iraq, it was clear that interagency coordination and a robust civilian capacity were required to conduct effective reconstruction activities.[36] In other words, the conclusions drawn from operations in Somalia and Bosnia that led to PDD-56 were relearned in 2005, because the initial lessons were lost due to failure to implement PDD-56.

National Security Presidential Directive 44

In December 2005, George W. Bush implemented National Security Presidential Directive 44 (NSPD-44) *Management of Interagency Efforts Concerning Reconstruction and Stabilization* formally superseding PDD-56. The directive assigned the Secretary of State as the lead coordinator of U.S. government efforts to prepare for, plan, and conduct stabilization and reconstruction activities.[37] The Coordinator for Reconstruction and Stabilization would coordinate all U.S. government reconstruction and stabilization activities. The Secretaries of State and Defense were to jointly develop a framework to coordinate civilian and military operations at all levels.[38] Finally, NSPD-44 established a Policy Coordination Committee for Reconstruction and Stabilization Operations, to be chaired by the Coordinator for Reconstruction and Stabilization and a National Security Council staff member.[39]

As a result, the State Department established the Office of the Coordinator for Reconstruction and Stabilization (S/CRS) in 2004 to organize all civilian efforts of the U.S. government and coordinate them with the military.[40] Until S/CRS was created, all elements of the Iraq operation were conducted out of the Pentagon.[41] From the outset, S/CRS was hampered because the U.S. Agency for International Development (USAID), the Department of Justice, State Department regional bureaus, and other stakeholders tried to limit the office's role.[42] Nonetheless, the S/CRS progressed and by 2007 created an Interagency Management System (IMS) to coordinate international operations.

Interagency Management System

The IMS sought to bring USAID, State Department, DoD, and other actors into a loose command and control structure.[43] The IMS has three components of interagency management. First, at the Washington-level, the Country Reconstruction and Stabilization Group would prepare a strategic plan to include a common strategic goal, concept of operations, major U.S.

government tasks, and resource requirements to guide all U.S. civilians in Washington and in the field.[44] Second, at the geographic combatant command headquarters, an Integration Planning Cell would integrate the civilian component of the operation with the military operational plans.[45] Finally, in the field or at an embassy, an Advance Civilian Team, overseen by the assigned Chief of Mission, would integrate into the existing embassy or USAID mission structure, and Field Advance Civilian Teams could deploy to implement programs at the local or provincial level.[46]

The IMS established no framework for roles and responsibilities, no coordination mechanisms with non-U.S. government partners, and no system of command and management at the operational or tactical level. It did, however, explain the relationship of the strategic headquarters-based planning with operational- and tactical-level operations and designated the Chief of Mission as the leader of all civilian actors. It largely failed to address exactly how civilians would coordinate efforts with the military command. If the NIMS were used at the field level, a consistent rather than ad hoc structure would exist through which the DoD could interface with civilian leaders. Though IMS was approved at a high level in the Bush Administration, it was never implemented in a real-world crisis.[47]

Quadrennial Development and Diplomacy Review: Creating an IORF Based on the NIMS/NRF

Secretary of State Hillary Clinton published the first ever Quadrennial Development and Diplomacy Review (QDDR) in 2010. The QDDR set forth an ambitious review and reform agenda for State Department and USAID.[48] One principal challenge recognized in the QDDR was that efforts to coordinate with DoD and other civilian agencies had been "largely ad hoc or post hoc," and the U.S. government had not made crisis management a central mission under an adequate operational structure.[49]

The QDDR rescinded the IMS and proposed an International Operational Response Framework (IORF), which would ensure accountability, clarify responsibilities, and establish procedures for planning and operations both in Washington and in the field.[50] As inspiration, the IORF would apply lessons learned from both domestic and international interagency response and would "draw on the widely recognized FEMA NIMS" and other international mechanisms.[51] However, progress toward creating the IORF has been lacking. This author seeks to promote the merits of following through on this particular QDDR proposal.

...for international operations, no binding doctrine has been created to govern the interagency process.

Analysis and Recommendations

This analysis of policy efforts to improve interagency coordination has sought to demonstrate a failure of the U.S. government to apply the same set of lessons to the same problem in two different contexts. The domestic model coordinates seven cabinet-level departments and two independent agencies with lead roles in large-scale emergency response. However, for international operations, no binding doctrine has been created to govern the interagency process. DoD is probably the most organized, plan-oriented organization in the world, whereas civilian diplomats and development experts have no such expertise in operational planning. FEMA has unique expertise in civilian operational planning for contingency operations that the State Department could leverage, but

it has largely failed to do so. The QDDR was a critical first step, but years after the QDDR was published, there is still no IORF. Academia and emergency management and foreign policy practitioners should analyze the applicability of the NIMS and an overarching policy framework like the NRF to stability operations, and this paper seeks to initiate that largely absent but critical discussion.

The NRF is built around 15 ESFs, which taken as a whole constitute a comprehensive emergency response. Similarly, George Mason University's School of Public Policy has developed a "Conceptual Model of Peace Operations" that breaks down a complex contingency operation into functions, tasks, and organizations. Four functions (peacemaking, peacekeeping, peace building, and peace support) are needed to achieve success in stability operations.[52] Each function is broken down into various tasks that may be assigned, as appropriate, to individual organizations and can be measured for success.[53] Tasks are related to the organizations that have the appropriate capacity to accomplish them.[54] The "Conceptual Model of Peace Operations" tasks and related organizations could provide the basis for the international version of the domestic ESFs and lead agencies.

The IORF would clarify how the whole-of-government conducts contingency operations and transitions from stabilization to reconstruction and demobilization.

An IORF should serve as the official "playbook" for stability operations, ensuring that the overall strategic framework will be implemented and improved upon across administrations. It should be a living document, continuously improved upon, but always in effect. Like the NRF, it should be unclassified, with classified annexes, as necessary. The writers of the NRF understood the importance of providing partners with a familiarity with the baseline concepts and mechanics of the document, and an IORF would benefit similarly.[55] The IORF would clarify how the whole-of-government conducts contingency operations and transitions from stabilization to reconstruction and demobilization. It would establish mechanisms for coordination, funding, and cross-agency mission-assignment. It would hold agencies accountable for their respective assigned tasks. This would greatly assist the State Department in getting much-needed buy in and support from other civilian agencies that are key partners in such international operations but are reluctant to commit resources to such missions.

The NRF is nothing without the NIMS, and the NIMS is nothing without the NRF. Because the NIMS can be applied to any incident, regardless of size, cause, location, or complexity, it could be directly adopted in international contingency operations. It is already known around the world, and its contents are already the inspiration for many foreign emergency management systems. The IORF should work hand in hand with the NIMS, as does the NRF. In order to implement such a sweeping reform, the NIMS/IORF must be mandated by Presidential Directive, as was the NRF/NIMS in HSPD-5, and it should be vetted across the U.S. government.

The NIMS and an IORF would give the U.S. government a playbook for how to conduct stability operations overseas. It would define concepts, identify key players and responsibilities of U.S. government agencies, and explain the interactions of the U.S. government with local governments, NGOs, the private sector, and other international actors. It should use the "Conceptual Model of

Peace Operations" as a basis for establishing the international version of the ESFs and assign lead agencies for each task. The NIMS, based on its flexibility to be used in any incident, should eventually become an international standard for management of stabilization and reconstruction activities, and the United Nations, NGOs, and foreign governments should be encouraged to utilize the principles of the NIMS, as many already do for emergency management. The NIMS is successful because all emergency responders in the U.S. use it. NIMS compliance is required for a state or local organization to receive federal preparedness assistance. Similar incentives could eventually be used for awarding development contracts to NGOs. If all parties involved in a stability operation were to eventually use the NIMS, our ability to successfully unite efforts among various organizations would also greatly increase.

Conclusion

International contingency operations that require a large civilian response for stabilization and reconstruction tasks are largely in their infancy, whereas emergency management mechanisms have evolved over decades. It would be tragic if the foreign policy community continued to ignore the large field of knowledge and expertise that exists domestically. A contingency operation is a contingency operation, whether domestic or international, and the challenges associated with navigating the complex web of interagency partners is no less challenging domestically. It appears that in managing complex contingency operations, lessons learned stop at the water's edge. It falls to the academic community and to policymakers to advance or refute the ideas in this paper and evaluate the applicability of the NIMS and NRF to international stability operations, but no good will come from continuing to ignore this potential application of tried interagency principles. The NRF and NIMS are the best tools for managing complex contingency operations that currently exists. If a better system existed for managing the interagency process, the emergency response community would probably already be using it. ***IAJ***

NOTES

1 Kevin Arbuthnot, "A Command Gap? A Practitioner's Analysis of the Value of Comparisons Between the UK's Military and Emergency Services, Command and Control Models In The Context of UK Resilience Operations," *Journal of Contingencies and Crisis Management*, Vol. 16, No. 4, December 2008, p. 188.

2 George W. Bush, Homeland Security Presidential Directive 5 *Management of Domestic Incidents*, The White House, February 28, 2003.

3 "National Incident Management System," Department of Homeland Security, 2008, p. 1.

4 Ibid., p. 3.

5 Ibid., p. 4.

6 "National Response Framework," Federal Emergency Management Agency, 2008, p. 2.

7 Ibid., p. 1.

8 Ibid., p. 2.

9 Ibid., p. 3.

10 Ibid., p. 6.

11 Ibid., p. 24.

12 Ibid., p. 62.

13 Ibid., p. 63.

14 Ibid.

15 Ibid., p. 68.

16 Ibid., p. 73.

17 National Response Framework, p. 1.

18 Ibid., pp. 49–50.

19 Ibid., p. 50.

20 Ibid., p. 78.

21 Ibid., pp 45–46.

22 Ibid., 47–49.

23 Erik Brattberg, "Coordinating for Contingencies: Taking Stock of Post-9/11 Homeland Security Reforms," *Journal of Contingencies and Crisis Management*, Vol. 20, No. 2, June 2012, p. 82.

24 Ibid., p. 82.

25 Ibid., p. 83.

26 Ibid.

27 Tonya Langford, "Orchestrating Peace Operations: The PDD-56 Process," *Security Dialogue*, Vol. 30, 1999, p. 138.

28 Ibid., p. 139.

29 Ibid., p. 140.

30 Langford, p. 140.

31 Ibid., p. 147.

32 William P. Hamblet and Jerry G. Kline, "PDD 56 and Complex Contingency Operations," *Joint Force Quarterly*, Vol. 24, Spring 2000, p. 94.

33 Ibid., p. 4.

34 Ibid.

35 Joseph J. Collins, "Planning Lessons from Afghanistan and Iraq," *Joint Force Quarterly*, Vol. 41, 2nd Quarter, 2006, p. 10.

36 Ibid., p. 10.

37 George W. Bush, National Security Presidential Directive 44, *Management of Interagency Efforts Concerning Reconstruction and Stabilization*, The White House, December 7, 2005.

38 Ibid.

39 Ibid.

40 John B. Herbst, "Complex Operations and the Comprehensive Approach, in Derrick J. Neal and Linton Wells, III (eds.), *Capability Development in Support of Comprehensive Approaches: Transforming International Civ-Mil Relations*, National Defense University, p. 27.

41 Ibid., p. 27.

42 Ibid.

43 Ibid. p. 29.

44 "Interagency Management System for Reconstruction and Stabilization," Department of State, 2007, p. 4.

45 Ibid.

46 Ibid.

47 Herbst, p. 29.

48 "Quadrennial Diplomacy and Development Review: Leading through Civilian Power," Department of State, 2010, p. ii.

49 Ibid., p. 123.

50 Ibid., p. 141.

51 Ibid.

52 "Conceptual Model of Peace Operations," George Mason University School of Public Policy, 2002.

53 Ibid.

54 Ibid.

55 "National Incident Management System," p. 1.

Deep Analysis:
Designing Complexity Into Our Understanding of Conflict

by Thomas G. Matyók, Hannah Rose Mendoza and Cathryne Schmitz

Conflict is inherently messy, and today those analyzing conflicts are confronted with an incredible number of problems that resist resolution. Chaos, ambiguity, and contradiction are routine. The vast majority of today's social conflicts can be characterized as "wicked problems," meaning they are a combination of ill-defined questions and multiple possible responses.[1] Simple answers are rarely sufficient to address the dynamics of modern struggle.

Recognizing that conflict analysis remains fundamentally anchored to the 1990s and is heavily influenced by greed and grievance thinking, conflict analysis searches for responses to today's wicked problems, often disregarding the mounting research that suggests existential concerns of culture, identity, and religion are playing increased roles in conflict.[2] As a result, we need enhanced ways of analyzing conflict and communicating knowledge that allow us to make sense of the chaos, ambiguity, and contradiction. Contrary to creating mental frames that work to simplify conflict into compartmentalized technical problems solvable in the same way as a mathematics equation, we suggest heading in the other direction—away from such reductionist tactics and toward complexity. Deep analysis is a textured study of conflict that identifies patterns of contradiction present in the struggle that can lead to detailed responses.

Current mental frames of conflict quite often appear antiquated or simply not helpful as tools

Thomas Matyók, Ph.D. is Associate Professor in the Department of Peace and Conflict Studies at The University of North Carolina Greensboro. Currently, he is a Visiting Research Professor at the Army's Peacekeeping and Stability Operations Institute and teaches classes at the Army War College on Religion and Violence, and Conflict Analysis.

Hannah Mendoza, M.F.A is Assistant Professor, Department of Interior Architecture at The University of North Carolina Greensboro. Her scholarship focuses on gender, identity, and the built environment; design education, research methods, theory and philosophy; and design for the disenfranchised.

Cathryne L. Schmitz, Ph.D. is Professor & Chair, Department of Peace and Conflict Studies, and Professor, Department of Social Work, at The University of North Carolina Greensboro. She teaches graduate classes on organizational development, leadership, and peacebuilding.

to understanding what we are seeing. Individual and group intellectual habits form the frame within which we construct and reassemble reality. When conflict analysis frames are outdated or insufficient, they can have serious unintended negative consequences.[3] We need expanded ways of analyzing conflict that recognize and embrace complexity.

In addition, once we have conducted conflict analysis, we need a common language for communicating lessons learned across organizational or agency boundaries. Rarely is one agency analyzing a conflict. Often several are studying conflict, viewing it through different lenses with analysis tools appropriate to their organizations, and being influenced by desired outcomes. Prejudice and bias are built into these frameworks, and organizations' patterns of behavior influence actions.[4]

The desire to roll-up shirtsleeves and get down to work tackling conflict and violence is certainly laudable; however, the desire for action cannot be allowed to push analysis out of the peacebuilding process. Abraham Lincoln wisely noted that if he had six hours to chop down a tree, he would spend the first four sharpening his ax. So it is with conflict work. Given a conflict to transform, ongoing analysis provides an understanding of context as well as an opportunity to develop a holistic view of the situation for the long term.

Our experience suggests that many practitioners of conflict resolution spend little time performing or simply ignore analysis. As indicated by the popular phrase of "paralysis by analysis," perhaps analysis has taken on a bad name Certainly, many students of peace and conflict studies resist analysis and express an active hostility toward it, preferring instead to focus almost exclusively on interventions.

As a result, many take an approach that begins with answers and then looks for problems to apply them against. When asked to confront issues outside of those answers, they either shoehorn the problem into their frame of understanding or imagine it as an irresolvable problem for the ages. In doing so, they reject their creativity and do not develop their abilities to design new responses to changing contexts.

Ongoing analysis is the *sine qua non* of successful conflict transformation. Context drives analysis, and analysis is action. Analysts interpose themselves between the conflict and the outcome, becoming an actor within the context. Equally important, analysis is what allows for the possibility of learning from the intervention techniques and outcomes of resolution. Unless we understand why we make certain decisions, we can never understand why those decisions fail or succeed, nor can we identify future situations in which particular aspects can be successfully applied or redesigned. The analyst is a constant learner.

The desire to roll-up shirtsleeves and get down to work tackling conflict and violence is certainly laudable; however, the desire for action cannot be allowed to push analysis out of the peacebuilding process.

The purpose of this article is to contribute to the emerging narrative that focuses on conflict analysis and the multiple ways it can contribute to understanding crises. We propose that analysis is layered and never completed. It leads to a more informed understanding of a conflict and generates a response that leads to another analysis of a new conflict state—an epistemic cycle. Like conflict itself, analysis is a never-ending process. There will be no moment in which all is on a trajectory of peace that requires no captain, no course adjustment, but simply travels eternally and without maintenance.

It is misleading to think of analysis as

linear—analysis leading to action, leading to an end state. Rather, analysis occurs along a spiral where conflict is re-examined as it manifests itself in new conditions. We suggest a critical realist philosophy that removes human beings as the center of the social universe and focuses on decision-making in context. The social structure restricts analysis through culture, cognitive dissonance, group-think, and conscious and unconscious psychological misperceptions.[5] Using a spiral metaphor and model of transformative conflict work, we advance the idea that at each stage of a conflict's evolution, analysis and intervention are bound by a newly-created social structure. Thus, the social framework moves from being a rigid, angular structure to becoming a constantly reforming liquid mass.

Rather than replacing existing models of conflict, deep analysis offers a multi-dimensional mental-frame that can be applied to existing conflict analysis models to complement their approaches.

We introduce the idea of deep analysis as a framework for approaching complex and ambiguous conflict contexts. Rather than replacing existing models of conflict, deep analysis offers a multi-dimensional mental-frame that can be applied to existing conflict analysis models to complement their approaches. Deep analysis extends models used to understand conflict and provides analysts with a mental strategy for going beyond the artificial limits imposed by model parameters. Deep analysis also provides a common language that conflict workers can employ across organizational boundaries.

The absence of joint conflict analysis models suggests that organizations' institutional inertia resists being forced into a Procrustean bed, where a one-size-fits-all approach is imposed. Agency-specific analysis tools develop organically because they meet a need in addressing wicked problems.[6] The answer we propose is to maintain organization-specific approaches to conflict analysis while introducing a universal translator that can facilitate joint understanding of the conflict environment: Social Cube 2.0.

Background

A quick Google search of the phrase "conflict analysis models," results in more than 235,000[7] hits. The number of hits suggests the significance of analysis to conflict work. With this number of resources available, how do we know which one is best? Certainly this does not indicate that there are more than 235,000 unique models of conflict analysis, but a cursory scan of the results indicates that there are a wide variety of models and model variants discussed. How does a peace worker begin to choose one over another? How does an ambassador know which ones she will need? In order to prepare practitioners for the multitude of contexts, many of which will include elements we cannot currently predict, should we use one, two, a dozen? Further, it is not enough to be versed in the models available, but rather true fluency comes with an ability to reform them to unique requirements. With so many models available, how do we become sufficiently versed in their possibilities to meaningfully fuse the results of multiple analyses to inform an intervention strategy?

It is not possible to arrive at a qualitative decision on which analysis model is best; in fact, such a standard of measurement requires making a false choice. Models develop because they are appropriate for the organizations using them and in the contexts in which they

operate. They are not always the right choice for all organizations at all times and places. Additionally, the language employed is different among various groups (i.e., government, military, nongovernmental organizations, and academics). Organizations need a process that allows them to undertake analysis in a way that meets their unique needs, while allowing them to speak with other entities working on the same conflict from vastly differing perspectives in order to harmonize their responses.

Single descriptions of conflict provide limited information. Imagine learning about the American Civil War solely from the descriptions of Robert E. Lee. Even assuming that Lee presented a fact-based narrative and did not intentionally misrepresent the truth, his account would only provide a partial understanding of how the conflict developed, what occurred during the various phases from initial disagreements to all-out war, and the possibilities and consequences of the way it ended. Imagine pairing that insight, however, with descriptions from leaders of all sides, widows of Civil War soldiers, Matthew Brady's photos, slaves, children of the privileged, and so forth, and a much more complex image begins to emerge. Conflict analysis that is fused in this way can lead to insights of a higher logical type.[8]

Social cube analysis provides a ready-made analysis framework that practitioners can apply to existing conflict analysis models.[9] Simultaneously employing the social cube with other models provides a common language that analysts can use to fuse multiple models and approaches. A social cube approach to analysis follows a design approach to peacebuilding and conflict transformation.[10] Design approaches move beyond the artificial boundaries of academic disciplines to engage scholarship and practice, broadly integrating knowledge holistically. Employing a design approach to peacebuilding, practitioners abandon discrete disciplines of academic study to assume a renaissance attitude toward knowing, an attitude that focuses on the whole as a complete entity, not simply the sum of its parts.

Complexity is free. In facing wicked problems, it is no longer enough to think outside-the-box, it is now absolutely necessary to get out of the box entirely. Conflict analysis should engage complexity and encourage complex thinking. Simple conflict analysis can lead to simplistic responses. However, inviting complexity into analysis should not result in a chaotic mess; rather, complexity should result in deep, nuanced, and textured analysis that can be articulated in a common language all can understand. When our models and metaphors betray us, we need to develop new models, despite the adage that the only thing more difficult than getting a new idea into an organization is getting an old idea out.

In facing wicked problems, it is no longer enough to think outside-the-box, it is now absolutely necessary to get out of the box entirely.

Deep Analysis

A primary rule of conflict analysis is that there is never enough. This is not to say that conflict analysis should lead to a state of "analysis paralysis," an inability to make a decision for want of ever more data. Rather, the point of deep analysis is that through an ongoing study of conflict, we can arrive at a more comprehensive approach to transformation. Deep analysis views conflict moving continuously upward along a spiral toward improved conditions and becoming a new conflict at each position. Systems adapt to transforming interventions and manifest new

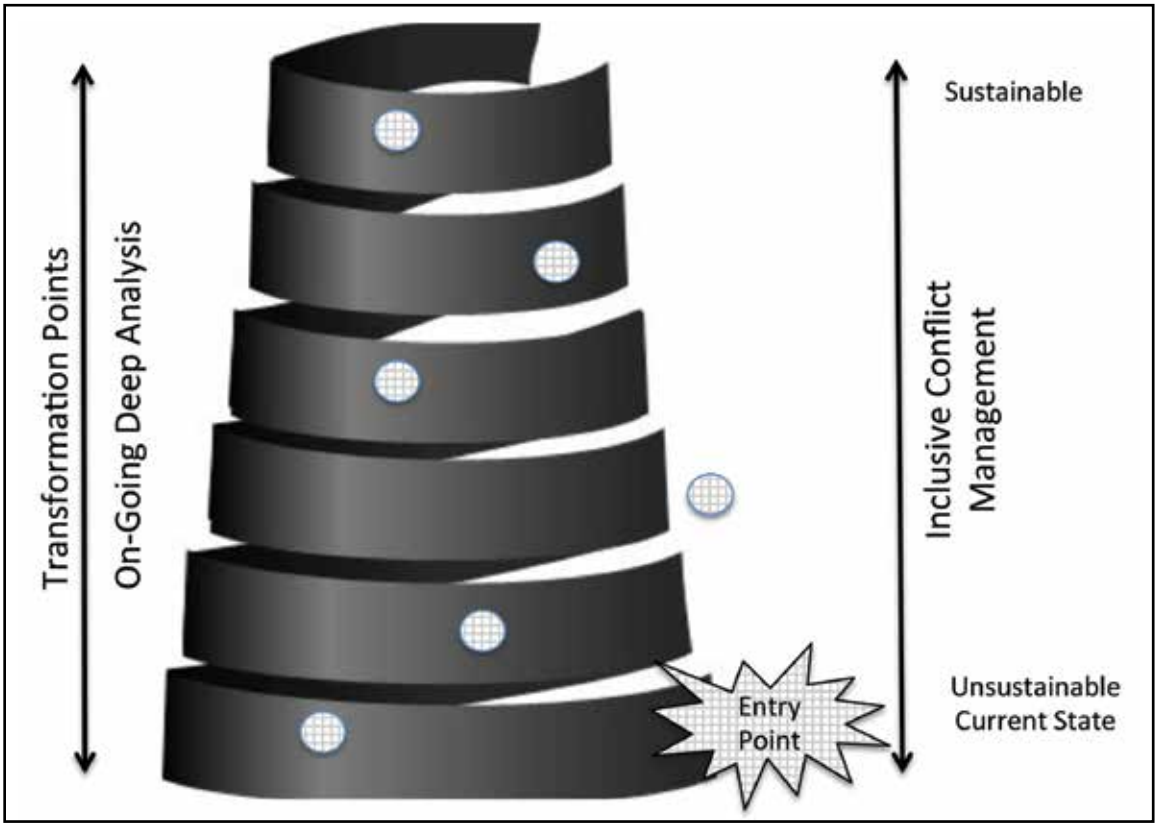


Figure 1. Spiral Model of Conflict Transformation

forms of old conflict. The use of the reflexive social cube results in an epistemic complex. An epistemology develops through use of the cube—knowledge is produced through analysis,[11] which leads to a transformational understanding of conflict. Every act of analysis creates new conflict; agent and structure interact in a creative and reinforcing activity. (See Figure 1.)

Deep analysis recognizes that conflict never ends, and because history never ends, conflict is rarely resolved. Boulding notes that if humankind's future relies on its ability to eliminate conflict, the future is bleak.[12] Conflict may be either latent or manifest; however, it is never absent. In deep analysis, the goal is conflict management and non-violent transformation. Conflict lives on in the collective unconscious and individual psyches.[13]

Deep analysis is based on three complementary components of conflict transformation; design, liquid knowing, and social cubism. Design suggests that sustainable peace processes are deliberate activities created in context to achieve deliberate goals. Liquid knowing advances the notion that conflict analysis eschews linear thinking in favor of thinking without boundaries in multi-dimensional space. The social cube offers a mental frame for multi-dimensional analysis of conflict, which allows analysts to develop an informed theory of change.

Design

Sciences can tell us what something is. Science informs us of a substance's physical properties and provides insights into the physical world. The humanities and social

sciences explain why something is. Humanities and social science disciplines contextualize what the sciences tell us exists. However, it is design disciplines that inform us about what something can be. Clearly, the sciences, humanities, and social sciences inform design thinking; however, they are viewed as restrictive. The design theorist and practitioner seek an integration of ideas. There are no design disciplinary boundaries to defend.

Design disciplines such as peace and conflict studies (PACS) are pointing to a new direction in scholarship. As fields of engaged-scholarship, design disciplines advocate for a transformative future unrestricted by disciplinary boundaries.[14] We anchor our approach to analysis in design theory as articulated by Rittel, Webber,[15] and Buchanan.[16] PACS moves beyond multidisciplinary and interdisciplinary approaches to scholarship and practice, to conceptual ground that frames the disciplines as integrative. Integrative fields of study move out of silos where knowledge is stored for use by approved elite within discrete domains. Design disciplines focus on the study and practice of what can be, rather than engaging in continuous study of objectified past knowledge or the physical world. The focus of integrative design disciplines is "the conception and planning of the artificial."[17] Peace design is about the artificial.

Design focuses on the creation of artifacts.[18] The existence and degree of peace within society is evaluated through the presence of artifacts. For instance, peace scholars ask, "What institutions of peace are present? How do they function? What peace symbols are in use?" The practice of building peace artifacts is what connects PACS to design and the practice of creating futures.

Design thinking is the scholarly practice of social construction that links theory and practice to create the field of design. Design thinking takes design out of its disciplinary boundaries and places it in non-design fields. Design thinking is more than creative thinking.[19] Creative thinking occurs inside the box using imaginative realignments of existing artifacts. Design thinking focuses on the not yet existing and how to make it real. It is not restricted by a finite number of existing artifacts.

Academia is dominated by disciplines that fall into one of two categories—sciences and humanities. Emerging to confront the wicked problems of our time are design disciplines engaged in substantive social change. Design disciplines challenge traditional ways of knowing and introduce ways of understanding not anchored to specific fields of study that possess their own unique logics. In vogue on college and university campuses today is the notion of interdisciplinary knowing. Interdisciplinary is another form of coordination or cross-talk among discrete academic disciplines. Interdisciplinary approaches to knowing fall short of the thinking required when addressing conflict issues using deep analysis. Interdisciplinary approaches keep academic disciplines intact. And, disciplines employ compartmentalized approaches to problems based on their limited views of reality. Design disciplines suggest that disciplinary approaches to scholarship and practice are outdated modes of thinking.

Liquid Knowing

Liquid knowing is a metaphor used in deep analysis to move beyond the notion of interdisciplinary bridging. Interdisciplinary thinking advocates for a form of enhanced communication among disciplines. At best, it suggests a "little of this and a little of that" approach to knowledge development, where disciplines accept into their canons only that which they find useful in supporting already established truths. These closed disciplinary systems can be thought of as boxes, outside of which designers are encouraged to think.

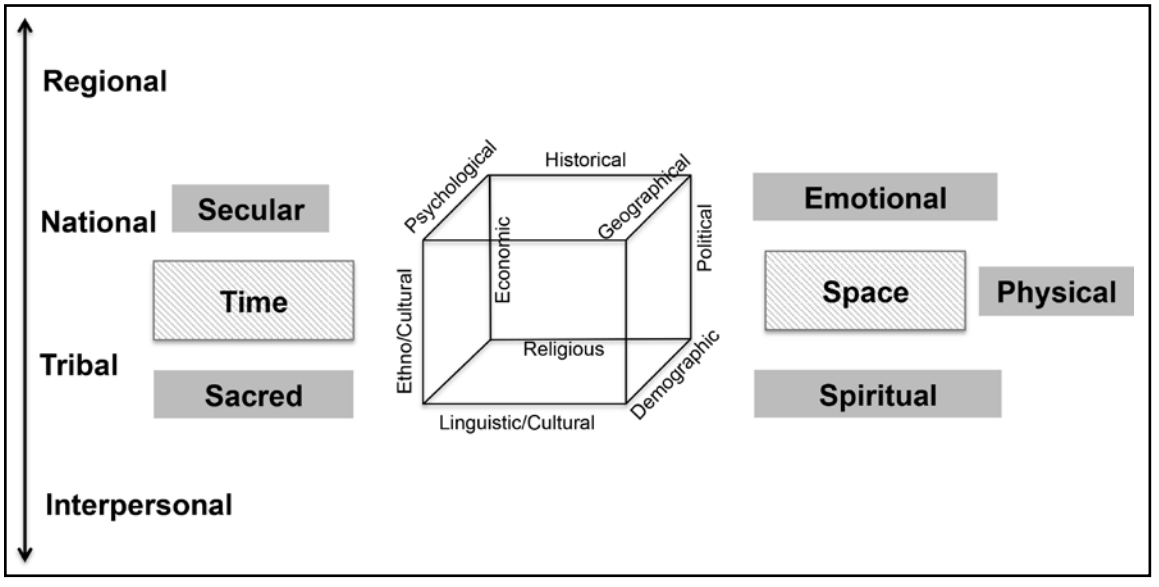


Figure 2. Social Cube Analysis 2.0 – Based on the work of Sean Byrne

What is needed is thinking that encourages contamination, not purity, of thought.

Analysis is not neutral, and it is influenced by the level at which it occurs.[20] At higher levels of analysis, responses are general, while at lower levels, they are specific.[21] The box, or structure itself, influences and modifies thinking. It creates the borders outside of which people are discouraged from wandering. We need people who are intellectually capable of stepping out-of-the-box and think in new spaces.

The opposite of linear thinking that moves along a plane, conflict analysis is a form of intellectual scaffolding that continuously builds on itself. It is thinking spatially.

Social Cube 2.0

As an outcome of their structures, all social conflict models are inherently flawed. Possibly, the best we can do is construct models that view a specific conflict as a human system and advance our knowledge of it while being aware that we can only know a limited amount of all that can be known. Corralling human behavior is not an easy job. Complexity theory and chaos theory suggest that in non-linear systems—such as social conflict—we are restricted to predictions based on probabilities influenced by constraints imposed on a system.[22] The best we can hope for in understanding human behavior is to recognize possible patterns, because a particular stimulus does not always lead to the desired response.

The social cube outlined by Byrne et al. is a multi-dimensional mental frame that is used to analyze social conflict. (See Figure 2.) As an analysis tool, the social cube allows for the construction of a three-dimensional model of the social context within which conflict manifests itself. Two-dimensional, linear thinking can lead to an analysis that fails to recognize the holistic nature of conflict, and the social cube corrects the limitations of these approaches. A model of social conflict must be sufficiently complex to make sense of the chaos. Conflict analysis looks at the patterns involved, which develop in multi-dimensional space. The social cube serves as a foundational piece of deep analysis. Organization specific analysis, social cube analysis, and the addition of time and space form the architecture of deep analysis.

By adding time and space as elements of

analysis to the social cube and placing it in a hierarchical holographic position, we can develop a deeper understanding of conflict at all levels: micro, meso, macro, and mega. Analysts cannot fully understand conflicts outside the time and space in which they are analyzed. Time and space will always be the ether in which the social cube moves, and they allow analysts to think deeply, holistically, and expansively. We suggest expanding Byrne's model and employing an enhanced model, Social Cube Analysis 2.0, which incorporates time and space.

Byrne et al., outline the social aspects of conflict that construct a mental model for analysts. A limitation of the social cube is that it follows a Euclidean geometry with distinct lines and angles. In contrast, deep analysis using Social Cube 2.0 adds in a respect for hyperbolic geometry recognizing conflict's non-linear nature. We recognize this limitation and do our best to adjust to compensate for angular thinking. Very often, conflict manifests itself as ill-defined patterns in multi-dimensional space. Metaphorically, conflict has a fractal nature replicating itself at each level of analysis.[23] Conflict fractals function independently at each level of analysis in pursuit of specific goals, and they simultaneously influence fractals above them impacting their goal pursuit.[24] Conflict can be viewed as holographic,[25] the entire conflict present in each autonomous fractal manifestation. Social Cube 2.0 exists in three-dimensional space and time and moves freely within each level of analysis.

Though space and time are considerations within social cube analysis, they are treated independently of the cube, forming the context within which the cube is suspended and conflict is understood. Conflict requires space and time to provide context.

Outside conflict moves into the social cube and is acted upon through analysis that results in an epistemic complex moving conflict continually along the mental spiral. As each conflict becomes new following each analysis and intervention, it is transformed through the social cube's mechanisms.[26]

Interagency coordination is challenging for multiple reasons: competing goals and priorities, cultural differences, resource and power disparities, competition for resource turf, different assumptions and expectations, and lack of line authority.[27] Added to these challenges is the recognition that no uniform language exists that facilitates clear interagency communication regarding conflict analysis.

Social Cube 2.0 translates analysis into a common language that can facilitate interagency communication.

Social Cube 2.0 translates analysis (conducted by agencies that view specific conflicts from different perspectives) into a common language that can facilitate interagency communication. Agents and agencies view conflict through unique lenses. These lenses bend the conflict "light" to create a focused picture meaningful to the individuals involved. Agencies view conflict with a goal of connecting it to their "distinct data bases, decision variables, decision makers, and affected constituencies."[28] A common Social Cube 2.0 language assists in developing an operational narrative.

What does the common language provided by the social cube look like? What does each dimension of analysis contribute to the narrative?

- **Historical**. All conflict has historical components. Deep analysis focuses on a specific manifestation of a historically-situated conflict. Since history does not end, it will always be a component of conflict.

- **Demographic**. Consideration of majority/minority demographics is necessary, as is the control and distribution of resources within communities and the society at-large.

- **Geographical**. Physical and social geography play crucial roles in understanding conflict. Geography influences conflict-resolution schemes. Specifically, what do lines of communication look like?

- **Psychological**. Conflict is existential, and to varying degrees, people's identities are linked to the conflict. The psycho-cultural dimension of analysis addresses the psychological and subjective characteristics of conflict. The psycho-cultural creates the narrative that describes what it all means. This psycho-cultural narrative is the domain of fear and anger.

- **Ethno/Cultural**. What in and out groups are present? How do they interact?

- **Religious**. What is the role of religious institutions within the conflict? Do religious actors and institutions follow the same scripts, or is there a difference between the formal and informal narratives? Are religious institutions and actors available to participate in conflict reconciliation?

- **Linguistic/Cultural**. Language and culture are interconnected. What symbols are used to legitimize the conflict?

- **Political**. Is the government legitimate? What is the accessibility to governance structures? What institutions of peace are present? How do they function? Is there trust in the political system?

- **Economic**. What economic resources are present, and are they equitably distributed throughout the social groups?

Space, an under-researched dimension of conflict, is assumed and rarely considered. Space is not another word for geography. Space is multi-dimensional and can be further viewed as having physical, emotional, and spiritual characteristics. Space and time are additions to the social cube. Conflict analysis is best accomplished in context with particular attention to the geographic, social, and emotional space within which it occurs. Woven into space is the dimension of time. These two additional dimensions of analysis place conflict in a unique contextual time-space. Conflict can only make sense within its designated space and time.

Secular and sacred time exist simultaneously.

Conclusion

The Social Cube 2.0 model presented in this paper offers a language that can facilitate interagency communication regarding conflict assessment. By acting as the framework for deep analysis, Social Cube 2.0 provides a common tool for multi-dimensional, on-going analyses that enhances and does not detract from agency-specific processes that have developed over time to meet specific needs. It is not about seeking homogeneity or removing complexity, it is about building in complexity and diversity of analyses.

Mental models grow from the metaphors in use to communicate the reality we know. The wicked problems we face today are too complex for the limitations of two-dimensional models. Conflict

workers are challenged to think in intellectual regions not yet explored, nor even discovered. Social Cube 2.0 multi-dimensional thinking is a step toward engaging in that intellectual terrain, and a model that encourages others to build upon it. We design our way forward. ***IAJ***

NOTES

1 Richard Buchanan, "Wicked Problems in Design Thinking," *Design Issues,* Vol. 8, Issue 2, pp. 5–21.

2 Sultan Barakat and Thomas Waldman, "Conflict Analysis for the Twenty-First Century," *Conflict, Security & Development,* Vol.13, Issue 3, pp. 259–283.

3 Hannah Rose Mendoza and Thomas Matyók, "We Are Not Alone: When the Number of Exceptions to a Rule Exceeds its Usefulness as a Construct, It is Time for a Change," in Tiiu Vaikla-Poldma (ed.), *Meanings of Designed Spaces,* Fairchild, New York, 2012, p. 47–58

4 David Litaker, et al., "Using Complexity Theory to Build Interventions that Improve Health Care Delivery in Primary Care," *Journal of General Internal Medicine*, Vol. 21, Supplement 2, 2006, pp. 30–34.

5 Touko Piiparinen, "Reclaiming the Human Stratum, Acknowledging the Complexity of Social Behaviour: From the Linguistic Turn to the Social Cube in Theory of Decision-making," *Journal for the Theory of Social Behaviour*, Vol. 36, Issue 4, December 2006, pp. 425–452.

6 Horst W.J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences*, Vol. 4, 1973, pp. 155–169.

7 The term was searched in quotes in order to only return results for this specific concept. A search for the term without quotes returned over 42 million results, indicating that there is even greater public conversation spreading outward from this specific idea.

8 Y.Y. Haimes and A.Weiner, "Hierarchial Holographic Modeling for Conflict Resolution," *Philosophy of Science*, Vol. 53, No. 2, 1986, pp. 200–222.

9 Sean Byrne and Neal Carter, "Social Cubism: Six Social Forces of Ethnopolotical Conflict in Northern Ireland and Québec," *ILSA Journal of International & Comparative Law*, Vol. 8, No. 3, Summer 2002, pp. 741–769; Sean Byrne et al., "Social Cubism and Social Conflict: Analysis and Resolution," *ILSA Journal of International & Comparative Law*, Vol. 8, No. 3, Summer 2002, 725–740; and Sean Byrne and Loraleigh Keashly, "Working with Ethno-Political Conflict: A Multi-Modal Approach," *International Peacekeeping*, Vol. 7, No. 1, Spring, 2000, pp. 97–120.

10 Mendoza and Matyók, 2012, pp. 47–58.

11 Piiparinen, pp. 425–452.

12 Kenneth E. Boulding, *The Meaning of the 20th Century*, Harper & Row, New York, 1964, p. 14.

13 Vamik Volkan, *Blood Lines: From Ethnic Pride to Ethnic Terrorism*, Basic Books, New York, 1998, pp. 48–49.

14 Hannah Rose Mendoza and Thomas Matyók, "Designing Student Citizenship: International Education in Transformative Disciplines," *International Journal of Art and Design*, Vol. 32, Issue 2, June 2013, pp. 215–225.

15 Rittel and Webber, pp. 155–169.

16 Buchanan, pp. 5–21.

17 Ibid., p. 14.

18 Ulla Johansson-Sköldberg, et al., "Design Thinking: Past, Present and Possible Futures," *Creativity and Innovative Management*, Vol. 22, Issue 2, June 2013, p. 124.

19 Ibid., p.131.

20 Barakat and Waldman, pp. 259–283.

21 Rittel and Webber, pp. 155–169.

22 James Gleick, *Chaos: Making a New Science*, Penguin Books, New York, 2008, pp. 41–45 and David Litaker et al., pp. 30–34.

23 Benoit B. Mandelbrot, *Fractals: Form, Chance, and Dimension*, W.H. Freeman, New York, 1977, pp. 1–25 and Benoit B. Mandelbrot, *The Fractal Geometry of Nature*, W.H. Freeman & Company, San Francisco,1982, pp. 1–24.

24 Moonsoo Shin et al., "Conflict Detection and Resolution for Goal Formation in the Fractal Manufacturing System," *International Journal of Production Research*," Vol. 44, Issue 3, 2006, pp. 447–465.

25 Haimes and Weiner, pp. 200–222.

26 Piiparinen, pp. 425–452.

27 Andrea Strimling Yodsampa, "Coordinating for Results: Lessons from a Case Study of Interagency Coordination in Afghanistan," IBM Center for the Business of Government, Washington, DC, 2013, p. 9.

28 Haimes and Weiner, p. 204.

Why We Can't All Just Get Along:
Overcoming Personal Barriers to Inter-organizational Effectiveness

by William J. Davis, Jr.

> ***DoD placed Pakistan and India in separate geographic combatant commands in order to foster U.S. military relationships with each country, given their history of tension and conflict. In contrast, State placed Pakistan and India in the same regional bureau because of political-military issues between the two nations, as well as other crosscutting issues that affect the region as a whole.[1]***

Shared Disunity

The opening quote of this article illustrates the differing cultural lenses through which organizations will view the same problem. However, as in the case of the India-Pakistan situation, it will take the resources and talents of a multitude of government agencies working in unity to realize the interests of the U.S. A question remains, however, as to how agencies with such dissimilar views can work together to solve complex problems. Increasing effectiveness when disparate inter/intra-government organizations must work together to solve problems is not easy. Many solutions have been offered, from increasing organizational cross-pollination by enforcing Goldwater-Nichols-type legislation upon the executive branch, to standing up centers for inter-organizational cooperation. *America's Army: A Model for Interagency Effectiveness* even suggests that if every agency modeled its organization on that of the U.S. Army, inter-organizational operations might be more effective.[2]

However, barriers to effective interaction might not be so much about collective organizational differences, but about how the preferences and prejudices of individuals manifest in ethnocentric behaviors. For example, both the Departments of Defense (DoD) and State organizationally share a disdain for the values of innovation and adhocracy, and each views the other organization not only

William Davis, Ph.D. is an associate professor at the U.S. Army Command and General Staff College with degrees from Old Dominion University, Marine Corps University, and Harvard University. He is a former Naval Officer and enjoys researching, writing, and facilitating on the leadership challenges in the Joint, Interagency, Intergovernmental, and Multinational environment.

as more inflexible, but also at times, inferior.[3] This ethnocentric phenomenon might be explained by looking to Edgar Schein, a most respected theorist of organizational psychology, who defines organizational culture as, "A pattern of shared basic assumptions that the group learned as it solved its problems that has worked well enough to be considered valid and is **passed on to new members as the correct way to perceive, think, and feel in relation to those problems"**[4] (emphasis added).

Those who have become invested in an organization have been taught the correct way to perceive, think, and act, so not only are they wary of any other way, but they also consider any other way of doing things as just plain wrong.

Those who have become invested in an organization have been taught **the correct way** to perceive, think, and act, so not only are they wary of any other way, but they also consider any other way of doing things as just plain wrong. The negative impact of such mistrust, even among individuals within organizations, has been thoroughly documented.[5] The prevalence of this normative thinking and subsequent exclusive behavior becomes amplified within the agencies of the federal government. Employment mobility among agencies is minimal, so exposure to the culture, capabilities, and limitations of other agencies is limited. Federal job security within agencies is so strong that an employee is more likely to die than go to work for another agency.[6]

However, recent studies point to some successes in overcoming the prejudice associated with ethnocentric thinking. For example, Davis finds that although DoD officers hold a significant amount of mistrust toward members of other agencies, that mistrust was negated whenever the officer spent significant time working with other agencies.[7] In addition, Munsing and Lamb report that Joint Interagency Task Force South continues to effectively prosecute a counter-trafficking mission without the administrative burden of memorandum of agreements between agencies, thus establishing an environment of trust and unity of effort.[8] Additionally, Davis finds that although from the same federal agency, members of the various Services within the DoD used to revile each other almost to the point of not being able to be effective when working together, they now, arguably, have an equal sense of community and trust among the Services as they do within their own Service.[9]

While the literature on cross-functional (inter-organizational) organizations is replete with social science theory that might be helpful to those who are charged with putting together one of these efforts, case studies of previous successes fail to come up with a cookie-cutter solution to make inter-organizational efforts a success[10] Although a one-size-fits-all theory does not exist in social science,[11] identifying variables that consistently appear as keys to the environment is not a reach, and indeed, the literature is replete with best practices. Organizational culture is one variable identified throughout the literature as having some sort of impact on inter-organizational effectiveness. Assumptions influenced by organizational culture are often the major source of conflict in any effort.[12] According to Schein, within the tenets of organizational culture is a built-in prejudice that one's organizational culture is the correct organizational culture. Overcoming ethnocentric prejudices manifested by organizational parochialism is the key to success for members operating in an inter-organizational environment. This article is

intended to provide some insight into the common cognitive obstacles that feed individual prejudices, in hopes that self-understanding will mitigate organizational parochialism and result in practices that will enhance interactions among all organizations.

Self-Examination: A Difficult Task

Overcoming one's prejudices is difficult under the best of circumstances and more complicated than most think. Perhaps even more difficult than overcoming prejudices is identifying organizational assumptions and differences among organizations that are potential friction points. For example, how can an individual who works for DoD a very hierarchical organization, realize and overcome prejudice against a non-hierarchical organization, especially if there is not individual self-awareness that it is the very idea of non-hierarchy that leads to feelings of contempt? Instead of focusing on the differences, an individual attempting to overcome ethnocentric prejudices needs to determine why those differences and subsequent feelings might exist. To overcome one's inbred cultural biases, one must focus on the "whys" of culture, not solely on the differences.

Becoming aware of the "whys" of one's culture should provide insight into why an organization is the way it is (why something or some way is taught as a correct way). Once that is determined, one can analyze the "whys" of the partnering culture. Typically, members of an organization make observations and jump to conclusions without examining the assumptions that they hold dear.[13] For example, in general, the U.S. Army is a very planning-oriented culture, whereas the U.S. Navy has more of an emergent approach to operational decision making, and there are good reasons for each culture. The Army has a mission to maneuver thousands of people in a defined battle space, so in order to avoid tragic outcomes, such as fratricide, in a chaotic environment where the leaders cannot control most decisions, the organization gives preeminence to planning. In contrast, the U.S. Navy's maneuver element usually consists of 6–8 ships with each one outfitted with a full communications suite and seasoned personnel able to communicate critical decisions to all involved. The operating environment for each is quite different and requires different approaches to operations. If one were from the U.S. Army, and did not understand what was just explained, there might be a tendency to denigrate the U.S. Navy as a cowboy culture that does not properly plan; or likewise, someone from the U.S. Navy might have a tendency to label the U.S. Army as overly inflexible.

Perhaps even more difficult than overcoming prejudices is identifying organizational assumptions and differences among organizations that are potential friction points.

Ways of Viewing Inter-organizational Efforts and Cultures

To be effective in the inter-organizational arena (i.e., accomplish the dictates of the effort while also protecting one's organizational interests), members of agencies within the inter-agency effort must understand their own organizational cultures and how they view other cultures. Members often differ on how they view their roles in the inter-organizational arena.

Some members hold the naïve view that they and others can freely set aside their long-held perspectives and beliefs and just work together "to get the job done." However, it often becomes the other organization's burden to set aside its cultural proclivities to make the

effort more harmonious. Members who view inter-organizational efforts as unitary will be severely disappointed and frustrated and, most likely, minimally effective when incorporating the capabilities and limitations of the various organizations to affect the mission.

Some members hold the view that although some differences in the cultures of the various organizations exist, all members of the effort are unitary in their purpose and will set aside those differences for the betterment of all. The members of an inter-organizational effort might believe that since all members are agencies of the U.S., that the purpose is singular; therefore, there should be a dominant goal and shared values. Although most inter-organizational efforts have some sort of shared purpose, that shared purpose does not always translate well into shared vision. A disparate frame of reference will most likely result in a tension-filled effort. For example, military joint doctrine emphasizes determining an end state and accompanying termination criteria for DoD. In contrast, State hopes to have a mission in the country without termination; therefore, its goal is to establish a position of continuing advantage and long-term benefits at the expense of immediate results. Although some long-term approach thinking as applied to crisis situations has manifested in the Theater Campaign Plan (the preeminent plan to which all military operations will eventually transition),[14] in a cultural sense, the military still focuses on more immediate, measurable results. Any member of an inter-organizational effort who believes such organizational values will be set aside in pursuit of a common objective will also be frustrated.

...some members become frustrated with the differences in culture among organizations, conclude there is no hope for the inter-organizational effort, and just go their own way.

Some members may be aligned completely with the purpose of the effort, while others may have cultures and agendas that lie outside the dominant effort. However, it is important to note that being a member of a culture on the periphery of the effort is not necessarily pejorative—it is only different. For example, DoD might concentrate on handling short-term challenges with the goal of handing off the effort to a long-term focused organization, while the long-term focused organization will most likely view problems through a different lens than those who are the first responders. Building consensus as to what values and purposes make up the inter-agency effort should be built through consensus.[15]

Most members share the interests of the larger inter-organizational effort; however, they also have their own interests. For example, organizations that make up a provincial reconstruction team (PRT) focus on immediate security, providing economic systems, providing basic services, and gaining support for representative government.[16] Organizations whose primary efforts are this disparate will have significant differences. Accepting those cultural differences can make a PRT member more effective in accomplishing an agreed-upon vision and thus be better able to realize how the capabilities and limitations of one's organization might benefit the effort.

Finally, some members become frustrated with the differences in culture among organizations, conclude there is no hope for the inter-organizational effort, and just go their own way.

The key to success is realizing that an inter-organizational effort lies somewhere between the overly optimistic view that agencies will "just work together to get the job done" and the counter-productive attitude of dismissing the

idea out of hand.

Other Bad Thoughts

There is a tendency among members of any organization to view askance the members of another organization who are not similar, and in some cases, even those organizations that are similar will view each other's motives as suspect. One of the most discouraging episodes of this country's recent inter-organizational history was the cultural fault line that appeared more often than it should have between State and DoD during Operation Iraqi Freedom. Senior DoD officers made disparaging comments about State members who were having a difficult time filling personnel requirements in Iraq. However, what these DoD officers did not understand was that few, if anyone, sign up to work for State in order to go to war. Perhaps State employees knew that austere environments or even some potentially hazardous working conditions might exist, but the veil of diplomatic immunity made the idea of having one's life threatened at all times completely incongruent with the assumed values of the organization.

It is quite common for members of one organization to be critical of another organization's members because of a lack of understanding of the other (and one's own) organization's culture. One culture's perception of chaos might be another culture's perception of discipline, or one culture's bureaucracy might be another culture's order. Each organizational culture develops based on the group's unique operating environment and mission. As much ridicule that is often focused on the Air Force from other Services for being a "country club" culture, the fact is that the Air Force is the best Air Force in the world. Although the discipline displayed in that organization is quite different from the discipline displayed in the Marine Corps, it was developed pursuant to the optimization of the mission in its environment. Oftentimes, members of distinct organizational cultures use visible cultural differences as a poor excuse for not getting things done in an inter-organizational effort.

...the secret to the success was in finding a "coupler" that allowed the different cultures to work together, not forgoing cultural individuality.

Finding Your Personal Coupler

When members from disparate agencies of Joint Interagency Task Force South were asked if their culture was changed because of the inter-organizational environment, they replied with a very firm "no." They said the secret to the success was in finding a "coupler" that allowed the different cultures to work together, not forgoing cultural individuality.[17] Potential couplers mentioned were building true consensus, communicating the environment and options for actions, coordinating harmoniously, cooperating in compliance with the aforementioned agreed upon consensus, and, most important, comprehension of each other's roles, limitations, and capabilities.[18] Of these couplers, the understanding of each other's roles, limitations, and capabilities was deemed to be the most useful.

One thing is evident: Each coupler requires individuals who are able to overcome systemic problems associated with inter-organizational efforts. Anyone operating within the inter-organizational environment should consider incorporating the following recommendations into any actions taken to frame and operate in the environment:

- **Understand your culture**. All members of an organization should know the "whys" of their culture. For example, it is not enough

to know that DoD is a planning culture, members must also understand the reason behind this proclivity and the subsequent limitations and capabilities associated with it. Knowing the "whys' will allow the member to better communicate the nuances of the culture to those of other organizations, thus enhancing communication and understanding.

- **Ask questions**. Members should ask questions of other participants to better appreciate the cultural and physical capabilities and limitations that an organization brings. Cultivating a culture of inquisitiveness during inter-organizational operations is critical to success. Assumptions are dangerous in situations such as crisis response. Sometimes for DoD personnel, whose culture, most times, is a rapid action-oriented one, taking the time to understand the culture of the other participants can be frustrating. Likewise, a member of an organization more concerned with long-term success will become frustrated with an individual or organization that appears to be doing things without regard for "what happens next."

- **Build consensus**. Consensus must be achieved through dialogue. This dialogue takes time and requires an ability that may not necessarily be fostered within a single organization. It is a special skill that should be cultivated for those operating in the inter-organizational environment. A lot of government organizations highly value their form of hierarchy, even though the hierarchies among organizations will look different to the casual observer.[19] For example, an ambassador has no less hierarchical authority within State than a general officer has within DoD. The organizations may just internalize that hierarchy differently. Any form of consensus building will most likely involve waiting for those personnel involved in solving problems to gain permission to do things that are outside of their cultural norm.

As a reflective practitioner, understanding and making conscious one's organizational assumptions will provide a basis for examining one's biases, prejudices, or unfounded expectations toward another organization. It will only be through a mutual understanding of how group identity affects thoughts and behaviors that those involved in inter-organizational efforts will be able to effectively operate as a team. It is not a matter of creating like organizations, but of developing couplers that maximize the unique capabilities of each organization. Inter-organizational efforts begin with individuals meeting together to tackle problems that no single organization has the talent or resources to solve on its own. It will be those same individuals, creating personal couplers to overcome perceived barriers, who will ensure the effort is a success. ***IAJ***

NOTES

1 Government Accountability Office, "Interagency Collaboration: Implications of a Common Alignment of World Regions Among Select Federal Agencies," Washington, DC, 2011, <http://www.gao.gov/new.items/d11776r.pdf>, accessed on 30 April 2013

2 Zeb B. Bradford, Jr. and Frederic J. Brown, *America's Army: A Model for Interagency Effectiveness*, Praeger Security International, Westport, CT, 2008, p.xiv

3 William Joseph Davis and Christopher R. Paparone, "Departments of State and Defense Relations: Are Perceptions Important? *InterAgency Journal,* Vol. 3, No.1, Winter 2012, pp. 31–40.

4 Edgar H. Schein, *Organizational Culture and Leadership*, 4th edition, Jossey-Bass, San Francisco, 2010, p.12.

5 C. Ashley Fulmer and Michele J. Gelfand, "At What Level (and In Whom) We Trust: Trust Across Multiple Organizational Levels," *Journal of Management*, Vol. 38, No. 4, July 2012, pp. 1167–1230.

6 Dennis Cauchon, "Some Federal Workers More Likely to Die than Lose Jobs," *USA Today*, 2011, <http://usatoday30.usatoday.com/news/washington/2011-07-18-fderal-job-security_n.htm2011>, accessed on 30 April 2013.

7 William J. Davis, Jr., "Is a Sense of Community Vital to Interagency Coordination? *InterAgency Paper,* Arthur D. Simons Center, Leavenworth, KS, January 2011.

8 Evan Munsing and Christopher J. Lamb, "Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success," *Institute for National Strategic Studies Strategic Perspectives*, No. 5, NDU Press, Washington, DC, 2011.

9 Davis, p.12

10 Michael A. Hogg, et al., "Intergroup Leadership in Organizations: Leading Across Group and Organizational Boundaries," *Academy of Management Review*, Vol. 37, No. 2, 2012, pp. 232–255.

11 John Lewis Gaddis, *The Landscape of History, How Historians Map the Past,* Oxford University Press, New York, 2002, p. 71-89

12 Ibid.

13 Chris Argyris and Donald A. Schon, *Theory in Practice: Increasing Professional Effectiveness*, Jossey-Bass, San Francisco, 1974, p. 84

14 Joint Publication 5-0, *Joint Operation Planning*, Department of Defense, Joint Chiefs of Staff, Washington, DC, August 11, 2011.

15 Tucker B. Mansager, "Interagency Lessons Learned in Afghanistan," *Joint Forces Quarterly*, Issue 40, January 2006.

16 *Provincial Reconstruction Team Playbook*, Center for Army Lessons Learned, No. 07-34, September 2007, <http://call.army.mil>.

17 Meeting between author and various principals of JIATF South, July 2009.

18 William J. Davis, Jr., "The Challenge of Leadership in the Interagency Environment," *Military Review*, Vol. 90, No.5, September-October 2010, pp. 94–96.

19 Kim S. Cameron and Robert E. Quinn, *Diagnosing and Changing Organizational Culture*, Jossey-Bass, San Francisco, 2006, p.37

Interagency Areas of Responsibility:
It Shouldn't Take a Genius to Make Geography Simple

by Mark Sweberg and Allan Childers

Many philosophers, artists, strategists, and inventors talk about the value of simplicity. Singer Pete Seeger said, "Any darn fool can make something complex; it takes a genius to make something simple."[1] Philosopher Henry David Thoreau mastered the art of living simply. A principle of war is simplicity in planning and operations. Yet, bureaucracy inherently leads to complexity that requires constant monitoring, correction, and new vectoring when opportunities arise. Now is the opportune moment to align interagency departments and agencies for managing international affairs through consistent organizational structures in a whole-of-government perspective.[2]

Today's unsettled post-Cold War and post-Operations Iraqi Freedom/Enduring Freedom environment has driven U.S. policymakers and war planners to shift their focus. Instead of focusing on warfighting and international development and assistance, they are now focusing on combating terrorism, managing stability and capacity building in host countries, applying a whole-of-nation approach, working within fiscal constraints, and increasing collaboration among U.S. and international agencies. Russia's and North Korea's increasingly threatening postures in Europe and Asia make such strategies particularly urgent. And yet the global structure of the U.S. government's international posture has not changed much since the Cold War. The fact that key foreign affairs departments each view the world differently creates unnecessary complications and bureaucracies that waste precious resources and create more complex coordination challenges.

In July 2013, Secretary of Defense (SecDef) Chuck Hagel announced a 20 percent cut in the number of senior military and civilian positions within the Pentagon by 2019. An estimated 3,000

Mark Sweberg has over 30 years' experience working on government domestic and foreign policy, programs, and operations stemming from 21 years in the army, 10 years with the U.S. State Department and 10 years as a defense contractor. Sweberg is currently working towards his Ph.D., and holds an MBA from the University of Puget Sound, an MA from University of Southern California and a BS in Engineering from the United States Military Academy.

Allan Childers is a retired USAF colonel with more than 30 years' experience working on government domestic and foreign policy, programs, and operations stemming from a full career in the Air Force, assignments with the U.S. Department of State and over 10 years as a defense contractor. He holds an MS from the National Defense University, MA from Webster College, and BBA from Chaminade University of Honolulu.

to 5,000 jobs will be cut from a bureaucracy that has heretofore shown remarkable resistance to cuts or even to a freeze on growth at the upper echelons.[3] The Office of the Secretary of Defense (OSD) is again considering rearranging the combatant commands (COCOM) and their areas of responsibility.[4] Congressional efforts to cut the International Affairs budget have placed the Department of State (State) and U.S. Agency for International Development (USAID) in positions where they may also need to slash billets.

Whether or not further cuts in defense spending become reality, Secretary Hagel, like his predecessors, has expressed the need for the Pentagon to examine its operations and the size and shape of the armed forces and command structures. Cutting senior level positions and reshaping U.S. military forces provide an opportunity to align boundaries within the Department of Defense (DoD) and with other departments to create a more efficient bureaucracy. Creating this efficient bureaucracy will require "out of the box" thinking, and the jury is still out as to whether DoD and the other foreign affairs departments will come together to effectively resolve this issue.

Bureaucracy Creates Unique Boundaries

Bureaucracies are slow and unyielding when challenged to respond to change, whether it be building capacity or responding to crises. Task alignment through consistent areas of responsibility (AORs) within the national security bureaucracy is problematic. The biases of different bureaucrats responsible for regional engagement in overlapping AORs and bordering areas of interest send mixed signals, as each agency serves different missions, offers extremely different capacities and resources, and views each country's requirements from different perspectives. Unlike cutting positions, aligning AORs results in improved agility and eliminates unnecessary bureaucracy, waste, redundancy, accountability disparities, and differences in measures of effectiveness/performance.

Aligning AORs requires a comprehensive structure that clearly defines and aligns responsibilities and functions among U.S. government departments and agencies. This structure would enhance efficiencies and reduce the added expenses that plague government action on a daily basis. During the past decade, the interagency has sought to articulate a comprehensive approach for international affairs. However, this comprehensive approach is hindered by a bureaucracy that consists of a spider web of decision-makers, assistants, advisers to department and agency leaders, and representatives to various international groups that complicate and slow execution of programs at the operational and tactical levels. A fundamental solution is to align engagement regions within the Pentagon and other U.S. government agencies and departments responsible for international engagement.

...the global structure of the U.S. government's international posture has not changed much since the Cold War.

Many planners and policymakers across the U.S. government complain of a lack of consistency of geographic boundaries for coordination among agencies and departments. There is such a complicated morass of overlapping roles and responsibilities among regional and functional advisers and implementers within the interagency that even with an understanding of each agency's or department's responsibilities and functions, coordination among all the potential stakeholders on international activities is cumbersome, if

not impossible. The only daily link between each department's or agency's bureaucracy occurs at the top leadership positions and the bottom country director or desk officer within OSD, DOS, USAID, and COCOMs. These desk officers must work through a complicated structure with overlapping and/or incongruent guidance across areas of responsibility that are managed differently at the mid levels.

OSD, State, COCOMs, Services, and separate operating agencies do not align geographically or functionally with each other or with other departments and agencies.

In the last 10 years the government has taken steps to resolve some of the bureaucratic challenges the foreign affairs organizations face. Presidential Policy Directive (PPD-6), "U.S. Global Development Policy," elevates development to a status equal to diplomacy and defense and seeks to "foster the integration of capabilities needed to address complex security environments."[5] PPD-23, "U.S. Security Sector Assistance Policy" guides departments to "foster U.S. government policy coherence and interagency collaboration" by synchronizing interagency efforts.[6] The PPDs create interagency and departmental working groups to formalize the informal coordination that occurs in the field and align implementation at the strategic levels in Washington from a functional perspective. However, these solutions fail to align policy attention by geographic regions across the diplomacy, development, and defense functions.[7]

Titles 10 and 22, U.S. Code identify how OSD and State offices are organized.[8] The Unified Command Plan establishes the COCOMs, their geographic AORs, and missions, among other actions. OSD, State, COCOMs, Services, and separate operating agencies do not align geographically or functionally with each other or with other departments and agencies. OSD's AORs do not align with geographic bureaus within State that are responsible for U.S. government foreign policy, within USAID that are responsible for implementing development policy, or within COCOMs that are responsible for implementing most DoD programs within the AOR.[9] This situation unnecessarily complicates DoD's planning and execution of a comprehensive approach with State, USAID, and other interagency stakeholders with international affairs responsibilities and functions.[10]

Key Players and Their AORs

The Under Secretary of Defense for Policy (USD [P]) is the principal staff assistant responsible for DoD policy development and implementation. Among many critically important activities concerning national security policy, the USD(P) is responsible for regional security affairs that include contributing to a holistic U.S. government engagement in programs and policies in cooperative engagement with foreign countries.[11] The USD(P) conducts these responsibilities through several regional and functional deputy and assistant secretaries (Assistant Secretary of Defense for International Security Affairs [ASD(ISA)], Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs [ASD(HD&AS)], and Assistant Secretary of Defense for Asian and Pacific Security Affairs [ASD(APSA)]) and other staff.

Within State, the Under Secretary for Political Affairs manages regional and bilateral policy issues for all individual countries around the world. The office conducts these responsibilities through assistant secretaries who manage six geographic bureaus (Africa,

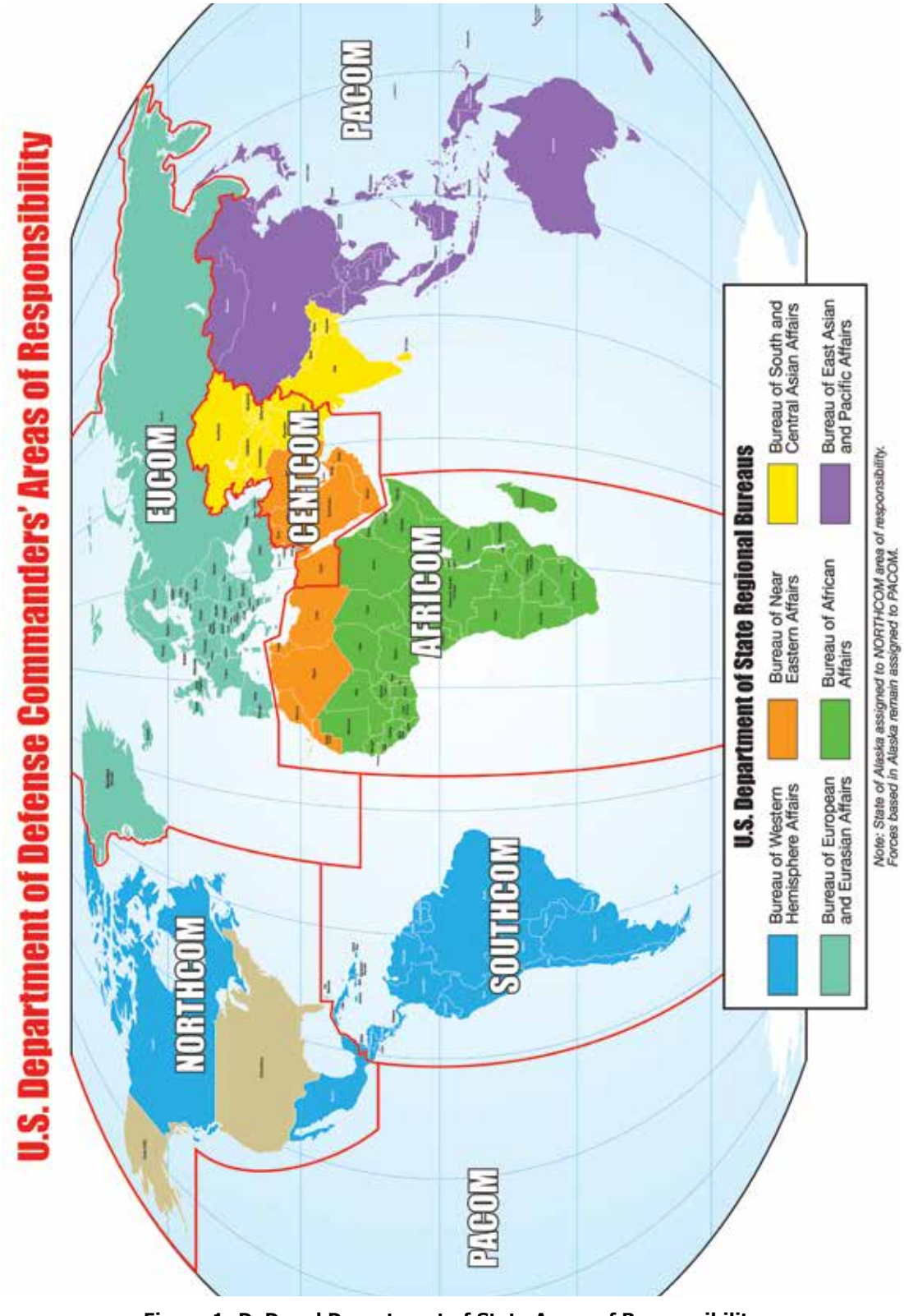


Figure 1. DoD and Department of State Areas of Responsibility
Source: www.state.gov

East Asia and the Pacific, Europe and Eurasia, the Near East, South and Central Asia, and the Western Hemisphere) and a functional bureau for International Organizations. State also uses a Political-Military Policy and Planning Team located in the office of the Under Secretary for Arms Control and International Studies Bureau for Political-Military Affairs to support interagency cooperation and regional support for civilian-led tasks directly with the COCOMs.[12]

The USAID Office of the Administrator manages five regional bureaus (Africa, Europe and Eurasia, Asia, Middle East, Latin America and the Caribbean) that are inconsistent with State and an Office of Afghanistan and Pakistan Affairs.

Figure 1 depicts how State and the COCOMs organize the world for international engagement. When overlaying the different geographic AORs of the OSD, USAID, and other agencies, the graphic becomes too complicated to sort out.

Within the Pentagon's Office for Security Defense (Policy), the ASD (ISA) is the principal advisor to the USD (P) and to the SecDef on international security strategy and policy on security cooperation and foreign military sales for Europe, the Middle East, and Africa. Sub-level Deputy Assistant Secretaries of Defense (DASD) for specific AORs manage day-to-day relations with foreign governments; develop regional security and defense strategies; and implement policy, plans, and activities that support responsibilities for capacity building of foreign militaries.[13]

- The AOR for DASD's European and Eurasian Affairs AOR extends across 51 countries, dependencies, and areas of special sovereignty from the Atlantic Ocean to the Mediterranean. The AOR for USAID's Bureau for Europe and Eurasia parallels State's AOR but only operates programs in 15 of the countries. State and USAID AORs are consistent with the United States European Command AOR (USEUCOM).

- The AOR for DASD's Middle East Affairs AOR includes 15 countries that stretch from Egypt and the Arabian Peninsula to Lebanon, Syria, Iraq, and Iran.[14] Thirteen of these countries are among the 20 countries within the USCENTCOM AOR;[15] however, the AOR also includes Israel and the Palestine Territories also assigned to the USEUCOM AOR.[16] Meanwhile, State's Near Eastern Affairs (DOS/NEA) AOR includes the same countries as the DASD, plus the six countries of North Africa. Five countries in the DOS/NEA AOR lie within United States Africa Command's (USAFRICOM) AOR and two within USEUCOM's AOR. The remaining 12 countries make up a portion of United States Central Command's (USCENTCOM) AOR. USAID's Bureau for the Middle East covers the same areas as DOS/NEA; although, USAID only operates in six of the countries and in West Bank and Gaza.[17]

- The AOR for DASD's African Affairs AOR includes all of the countries on the African continent except Egypt, which is part of DASD's Middle East Affairs AOR. This is the same construct for two COCOMs (USAFRICOM's AOR includes the entire continent except for Egypt, which is assigned to USCENTCOM's AOR). State's Bureau of African Affairs and USAID's Bureau for Africa include only the 49 countries in sub-Saharan Africa. It does not include the six countries of North Africa that are collocated with the DOS/NEA and USAID's Bureau for the Middle East, which is divided into offices covering sub-regions of the AORs.

Different OSD assistant secretaries oversee Asia, the Pacific region, Latin America, and South America.

The ASD(HD&ASA) consists of several functional offices for homeland defense issues and one office (Western Hemisphere Affairs [WHA]) that is responsible for engagement with AOR countries.[18] WHA covers responsibility for 39 countries within the Western Hemisphere but not the U.S.[19] USAID's Bureau for Latin America and the Caribbean currently has programs in 18 countries throughout Mexico and South America. COCOMs split the region into two AORs: United States Northern Command's AOR includes Canada, Mexico, and the Bahamas in addition to the U.S. and its territories, and United States Southern Command's AOR includes the countries in Central and South America and within the Caribbean Sea.

The ASD(APSA), responsible for policy, strategy, and relations with governments, defense establishments, and international organizations within the OSD-defined Asia-Pacific region, is broken into three DASD sub-regions—Afghanistan, Pakistan, and Central Asia (APC); East Asia (EAS), and South and Southeast Asia (SSA). State conducts operations within the Asia-Pacific region through two bureaus—the Bureau of East Asia and the Pacific (EAP) and Bureau of South and Central Asian Affairs (SCA). USCENTCOM and United States Pacific Command (USPACOM) are responsible for portions of these AORs. USAID covers this region with two sections—Bureau for Asia (East Asian Affairs and South and Central Asian Affairs) and Office of Afghanistan and Pakistan Affairs.

- DASD sub-region APC includes seven countries from Kazakhstan to Pakistan. The SCA is responsible for foreign policy and relations with these seven countries, as well as India, Nepal, Bhutan, Bangladesh, Sri Lanka, and the Maldives. These seven countries are among the 20 countries within USCENTCOM's AOR, and six of these countries are also located within USPACOM's AOR. The remaining 13 countries in USCENTCOM's AOR are also within DASD(ME)'s AOR. USAID's Office of South and Central Asian Affairs parallels SCA, except they have no programs in Bhutan, while USAID's Office of Afghanistan and Pakistan Affairs covers the remainder of the AOR.

Figure 1 depicts how State and the COCOMs organize the world for international engagement. When overlaying the different geographic AORs of the OSD, USAID, and other agencies, the graphic becomes too complicated to sort out.

- DASD sub-region EAS aligns with seven of the 36 countries in USPACOM's AOR. EAP's AOR includes 31 countries from Mongolia and China to Australia and New Zealand and the island nations of the Pacific. All of these countries are also within USPACOM's AOR, which also includes five countries within SCA's AOR. USAID's Office of East Asian Affairs programs operate in 21 countries consistent with the EAP's AOR.

- DASD sub-region SSA aligns with the other 24 of 31 countries within the EAPS AOR and 29 of 36 countries[20] within USPACOM's AOR.

Complicating the OSD structure even more is the organization of separate defense agencies that support capacity building in foreign countries. For example, the Defense Security Cooperation Agency (DSCA) divisions do not align with any other AOR among organizations responsible for capacity building, including OSD and the COCOMs.[21] DSCA is organized

under the Principal Director for Operations into Regional Deputies for Asia Pacific Americas, Europe/ Africa, Middle East, and South and Central Asia to support security cooperation programs around the globe. The Regional Deputy for Asia Pacific Americas supports countries in the USPACOM, USNORTHCOM, and USSOUTHCOM AORs; the Regional Deputy for Europe/Africa supports countries in the USEUCOM and USAFRICOM AORs; the Regional Deputy for the Middle East supports countries in the USCENTCOM AOR; and the Regional Deputy for South and Central Asia supports countries in the USCENTCOM and USPACOM AORs.

Other departments and agencies that interact with the country desk officers in OSD, State, USAID, or the COCOMs may also be regionally structured differently. For example, the Drug Enforcement Agency has 86 foreign offices in 67 countries structured within seven different regions: Andean and Southern Cone, Caribbean, Europe and Africa, Far East, Middle East, North and Central America, and Southwest Asia.[22]

Why Is It Like This?

The current number of offices and shape of the DoD, State, USAID, and COCOM AORs are primarily an evolution from nearly 70 years of White House, State, and Pentagon leadership decisions and personal perspectives on the importance of engagement with various countries. They have evolved based on perspectives of how these countries influence and may be influenced by the U.S. on a regional, continental, and global basis.

The organizational structures of today were originally based on the National Security Act of 1947 that mandated a major restructuring of the institutions that formulate and implement foreign policy (the National Security Council (NSC), DoD, and State).[23] Until recently, NSC Policy Coordinating Committees led by State-level Under or Assistant Secretary rank provided interagency coordination for foreign affairs through the same six geographic AORs as defined by the State Department. Even the recently renamed NSC Staff includes Special Assistants to the President and Directors that are so numerous in regions and issues for foreign policy that Wikipedia is needed to sort them all out. They are all shaped differently from all Executive department AORs.[24] The Goldwater-Nichols Department of Defense Reorganization Act of 1986 and subsequent changes continue to articulate why COCOM AORs are drawn the way they are.[25] In the past, policymakers also believed that two countries with the potential to wage war with each other should be in different COCOM AORs. This has not been a cause of concern outside of DoD, and the concept is changing within the department.

Recommendations

The following solutions are simple, compelling, and only require a resolve and commitment to efficiency and effectiveness to implement:

- Establish a standing interagency working group tasked to align and maintain or evolve (as needed) fewer AORs between the NSC and departments/agencies with responsibilities for country engagement. This group should also develop and implement policies/strategies to provide a comprehensive perspective to U.S. country, regional, and global engagement for each country desk officer to better implement U.S. government policy and strategy consistently and synergistically. While this recommendation creates yet another bureaucracy, if it is given a strong mandate and high-level support to reach a genuine solution, it can and should put itself out of business in a reasonable period of time.

- Redraw the AORs across all departments

and agencies supporting international engagement programs to make them consistent. Consider that political realities in the current environment should trump geographic boundaries. Align the regions of DoD DASD and ASD, State, USAID, and offices responsible for providing regional and country policy and planning direction so they are consistent with the State bureaus' AORs. For example, including North Africa countries in the Middle East bureau may be more appropriate that fencing the continent of Africa. Combining Pakistan-India into a broader AOR can provide new, more realistic perspectives to the Central-South-Southeast Asia region.

- Reduce the number of sub-region offices/positions reporting to senior policymakers and to whom country desk officers must report. Consider eliminating sub-regional breakouts within bureaus and directorates.

- Provide consistency of guidance/formats across departments/agencies to all country desk officers. For example, DoD and COCOM desk officers should receive all traffic passing through State and USAID desk officers for particular countries and vice versa.

- Modify the Unified Command Plan during the next update.[26] COCOMs should be totally aligned with DoD and State directorates/bureaus.

What Are the Risks and Advantages?

The risks and the advantages can be viewed collectively. Consistency among the interagency department/agency AORs would improve comprehensive implementation and engagement of U.S. government policies/strategies, programs, and activities with countries around the globe. The changes would demonstrate a refocusing of defense, diplomacy, and development priorities at a time when non-lethal solutions are the preferred method of country engagement. The changes will also help reduce the number of mid-level managers who may be currently providing different interpretations of senior-level guidance to their subordinates. Span of control could be better managed, and divisions in perspectives/approaches at key unstable borders can be eliminated (e.g., the separation of Israel from other Middle East countries, Pakistan-India, and northern Africa countries from sub-Saharan African countries).

Now is the most opportune time to align the AORs and the offices that manage them. Success can be realized if the leadership of DoD, State, and USAID address the challenges not from a department-centric point of view, but from a whole-of-government perspective. Alignment should be driven by the need for engagement in a new strategic environment, efficiencies, savings, and consolidations that are free from internal politics and "not invented here" turf wars. ***IAJ***

NOTES

1 Kim Ruehl, "Pete Seeger, Biography and Profile, About.com, <http://folkmusic.about.com/od / artistsaz/p/PSeeger_profile.htm>, accessed on April 2, 2014.

2 This subject has been addressed from smaller perspectives of reorganizing COCOM AORs in the past. See Nathan Freier, "The 2011 Unified Command Plan—A Missed Opportunity?" Center for Strategic and International Studies webpage, <http://csis.org/publication/2011-unified-command-plan-missed-opportunity>, accessed on May 24, 2011. This article only addressed realigning the COCOMs to reduce resourcing levels. See also Lieutenant Commander David Coghlan, "Redrawing the COCOM Map," *Armed Forces Journal*, October 2012, <http://www.armedforcesjournal.com/archive/issue/2012/10>, accessed on April 17, 2014.

3 "Hagel Orders 20 Percent Cut in Pentagon Top Brass, Senior Civilians," *Washington Post* webpage, <http://articles.washingtonpost.com/2013-07-16/world/40609812_1_george-little-pentagon-defense-business-board>, July 16, 2013, accessed on April 2, 2014.

4 Marcus Weisgerber, "DoD Weighs Major COCOM Realignment," *DefenseNews* webpage, April 11, 2013, <http://www.defense.com/article/20130811/DEFREG02/308110001/DoD-Weighs-Major-COCOM-Realignment>, accessed on April 17, 2014.

5 "Fact Sheet, U.S. Global Development Policy," <http://www.fas.org/irp/offdocs/ppd/global-dev.pdf>, accessed on April 2, 2014.

6 Office of the Press Secretary, White House, "Fact Sheet: U.S. Security Sector Assistance Policy," April 5, 2013, <http://www.fas.org/irp/offdocs/ppd/ssa.pdf>, accessed on April 2, 2014.

7 The important role that Congress plays in defining and supporting interagency structures and the missions they implement is recognized but is outside the purpose of this paper.

8 Title 10, United States Code, Section 113 and 134 provide guidance to DoD. Within OSD, DoD Directive 5111.x-series publications provide guidance on the authorities and responsibilities for USD(P) and subordinates. Title 22, USC, refers to State's organization. See <http://www.law.cornell.edu /uscode/ text/10/113/, http://www.law.cornell.edu/uscode /text/10/134>, <http://www.law.cornell.edu /uscode/ text/22/chapter 38>, and <http://www.dtic.mil/whs/directives/corres/dir/htm>, accessed on April 2, 2014.

9 Joint Staff Directorate for Strategic Plans and Policy (J-5), Directorate for Politico-Military Affairs is structured both functionally and geographically. The geographic deputy directorates include desk officers in Africa, Asia, Europe, Middle East, and the Western Hemisphere and a Pakistan Afghanistan Coordination Cell. Although they have roles and functions in assisting the Chairman of the Joint Chiefs of Staff to provide military advice to the President and guidance to the combatant forces, they are not in the chain of command and control to provide the same level of direct engagement on capacity building with host countries. The J-5 offices are, therefore, excluded from this paper but should be included in any future alignment of AORs among departments. For more information on the Joint Staff see the *Joint Officer Handbook*, August 2012, <http://www.dtic.mil/doctrine/training/joh_aug2012.pdf>, accessed on April 2, 2014.

10 This paper primarily addresses the OSD, State, and COCOMs because the operational chain of command runs from the President to the Secretary of Defense to the combatant commanders in the defense side and to the Secretary of State on the diplomacy side.

11 Office of the Secretary of Defense, "Fiscal Year 2012 Budget Estimates," February 2011, p. 27, <http://comptroller.defense.gov/defbudget/fy2012/budget_justification/pdfs/01_Operation_and_ Maintenance/O_M_VOL_1_BASE_PARTS/OSD_OP-5_FY_2012.pdf>, accessed on April 2, 2014.

12 For a description of the PPT, see Department of State website, <http://www.state.gov/t/pm/ppa/pmppt / index.htm>, accessed on April 2, 2014.

13 <http://policy.defense.gov/OUSDPOffices/ASDforInformationSecurityAffairs.aspx>, accessed on April 2, 2014.

14 For simplicity in discussion only, the Palestinian Territories will be referred to as a country. This should not be construed as a statement of policy.

15 For a list of USCENTCOM AOR countries, see USCENTCOM homepage, <http://www.centcom. mil>, accessed on April 2, 2014.

16 For a list of USEUCOM AOR countries, see USEUCOM homepage, <http://www.eucom.mil>, accessed on April 2, 2014.

17 See <http://www.usaid.gov/who-we-are/organization/bureaus/bureau-middle-east>, accessed on April 2, 2014.

18 Department of Defense Directive, no, 5111.13, "Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs," January 16, 2009, <http://www.dtic.mil/whs/directives /corres/ pdf/511113p.pdf>, accessed on April 2, 2014. This directive delegates this office with responsibility to serve as principal civilian advisor to the SecDef and USD(P) on Western Hemisphere security affairs but does not delineate which countries are included in the responsibility. For a list of USSOUTHCOM AOR countries, see USSOUTHCOM homepage, <http://www.southcom.mil>, accessed on April 2, 2014.

19 See a description of State's regional breakdowns and specific country information at U.S. Department of State homepage, <http://www.state.gov/countries>, accessed on April 2, 2014.

20 This DASD includes India and all other South Asian countries, except Afghanistan and Pakistan, the nations of Southeast Asia, plus Australia, East Timor, New Zealand, and the Pacific Island States, <http:// www.defense.gov/bios/biographydetail.aspx?biographyid=189>, accessed on April 2, 2014.

21 See DSCA link at <http://www.dsca.mil/about-us/operations-ops>, accessed on April 2, 2014.

22 Drug Enforcement Administration homepage, <http://www.justice.gov/dea/about /foreignoffices. shtml>, accessed on April2, 2014.

23 National Archives, Online Public Access, <http://research.archives.gov/description/299856>, accessed on April 2, 2014.

24 No official source for this breakdown was found. Reference <http://en.wikipedia.org/wiki /United _States_National_Security_Council>, accessed on April 2, 2014.

25 U.S. Code Legal Information Institute, Cornell Law School, "Goldwater-Nichols Act of 1986," <http:// www.au.af.mil/au/awc/awcgate/congress/title_10.htm>, accessed on April 2, 2014.

26 For current insight to the Unified Command Plan, see Andrew Feickert , "The Unified Command Plan and Combatant Commands: Background and Issues for Congress," Congressional Research Service, January 3, 2013, <http://www.fas.org/sgp/crs/natsec /R42077.pdf>, accessed on April 2, 2014.

Understanding the Human Dimension for Unified Action:

An Approach to Scholarship, Complexity, and Military Advice

by Stephan Bolton

Now is the time for enlivened discourse about unified action, national policy, and the human dimension. The peoples and institutions that inhabit operational environments are always significant to our desired outcomes. As the U.S. military moves through that traditional period of postwar reflection when leaders re-professionalize their forces, identify and capitalize on the lessons of recent conflict, and pursue efficiencies in the face of resource constraints, the question of human engagement becomes central to achieving the intent of policy. This is a question for the whole-of-government. National security is a multiagency responsibility in the era of globalization. The rapid diffusion of ideas across borders and peoples carries the promise of progress, but also the potential for threats to emerge in unexpected policy environments. At the intersection of national policy and the human dimension, the first obligation is to understand the environment. All that follows is contingent on that understanding. Many senior leaders have recognized this obligation, but they have also recognized that there is something missing in the military's approach to understanding the world. This gap does not always preclude policy success, but it is often responsible for seeming failures. New approaches to understanding the human dimension are needed to fill this gap.

Mid-war Department of Defense (DoD) initiatives, such as the return of counterinsurgency and cultural intelligence methods, approached the human dimension in doctrinal and practical ways that lay the groundwork for concepts currently under development, such as Strategic Landpower and the Engagement Warfighting Function. Those first efforts held great promise, but often left leaders frustrated, as both the military doctrinal framework for understanding and the common practice of it habitually produced suboptimal results. Reports given by Generals Stanley McChrystal and David Petraeus while commanding in Afghanistan show that both were keenly aware of the untoward strategic effects caused by failures to understand tactical-level social dynamics. Awareness of the gap is also evident in the 2012 *U.S. Army Capstone Concept,* which recognizes that "current doctrine does not address the moral, cognitive, social, and physical aspects

Major Stephan Bolton is a U.S. Army Special Forces officer with operational experience in South and Central America, Afghanistan, and Iraq. His most recent experience includes support to U.S. embassies and Joint forces in Africa. He is currently a student at the Command and General Staff Officer Course at Fort Leavenworth, Kansas, and is pursuing a Master's degree in International and Interagency Studies at the University of Kansas.

of human populations."[1] Another component to operational understanding, perhaps more fundamental than doctrine and practice, is the professional ethic. The 2010 Army White Paper, "The Profession of Arms," and Chairman of the Joint Chiefs of Staff General Martin Dempsey's subsequent adaptation of that paper for the joint force have renewed a necessary dialogue within the military about professional obligations, the exercise of judgment, and the way in which these influence military contact with the human element in the world.

To help fill the gap in the current military method, I propose the following approach:

- The practice of multidisciplinary analysis to develop deep situational understanding of cause-and-effect relationships in complex environments.
- A menu-of-options approach to intervention.
- An expanded concept of military advice.

All of these approaches enable the unified action community of interest to achieve policy objectives. The "Local Dynamics of War" seminar at the Command and General Staff Officer Course (CGSOC) employs this approach to augment doctrine, inform the practice of planning, and pursue a comprehensive understanding of the operational environment. The seminar also answers the calls to action from several of the military's top leaders to study the most modern perspectives on the social science aspects of warfare. The social sciences are comprised of several domains and sub-disciplines, such as political science, economics, sociology, and anthropology, and examine environmental variables of great interest to the military practitioner. Among these variables are the peoples, cultures, ideologies, and institutions found in operational environments, the socioeconomic and political underpinnings of state and non-state actors, and the complex microdynamics of their interactions.

This article discusses the benefits of multidisciplinary thought and the importance of causality and complexity, addresses the potential of deep situational understanding, and describes how a spectrum of interventions based on acceptable or desired conditions may be more appropriate for complex environments than traditional end-state campaigning. It closes by proposing an expanded professional responsibility to unified action in all environments. Many of the references are to Army or military usage, but in principle, the ideas presented here are applicable by all policy actors. Similarly, use of the term "unified action" refers primarily to U.S. actors, but admits to contexts where international or non-governmental actors are partners in policy efforts. Unified action is defined in joint doctrine as "the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort."[2]

Unified action is defined in joint doctrine as "the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort."

The Benefits of a Multidisciplinary Approach

A multidisciplinary approach emphasizes openness to ideas, drawing upon expertise in many fields of study. Its strength is in its diversity, as contrasting ideas promote critical thought. Critical thought increases the objectivity and reality of one's understanding. A multidisciplinary approach achieves two immediate purposes. First, such an approach

helps to mitigate many of the pitfalls inherent in the military's institutional planning processes. These pitfalls constrain understanding of complex environments. Three common pitfalls in military planning and decision making are a tendency to focus on macro-level narratives about conflict, excessive use of reductionism and simplification to explain cause-and-effect relationships, and the influence of organizational and individual cognitive biases.

Conflict and war in all its forms are studied in great detail by many social scientists... Few military practitioners know of such research...

The second purpose of a multidisciplinary approach is to enhance existing practice through the frequent engagement of scholarly research and methodology. Conflict and war in all its forms are studied in great detail by many social scientists. They regularly contribute to a large body of knowledge about micro-level human dynamics, causation, and other topics of specific interest to the military profession. These scholars share perspectives on the operational environment that practitioners might not have considered when using doctrinal planning processes. Few military practitioners know of such research, where to find it, or how it can inform their understanding. Military operations, actions, and activities are always guided and underwritten by policy, plans, and doctrine. The decision-making process is still influenced by the practitioner's education, training, and experience. But when practitioners consult scholarly perspectives on a given environment, they introduce valuable information, sometimes contrarian or counterintuitive, which brings their understanding closer to reality. The work of proven scholars, by virtue of the rigor and validity in their research, may add to, confirm, or refute the facts and assumptions upon which practitioners base their understanding.

This knowledge is available to the practitioner from many sources. Scholarly journals present research articles whose arguments are succinct and easily assimilated. Publications such as *Perspectives on Politics*, *Journal of Conflict Resolution*, *Armed Forces and Society,* and many others can be of great value to a commander and staff's understanding. More extensive research is published in book form by university presses. The value of large-scale research is evident in three recent works by political scientists about the tactical-level influences of sub-state conflict. In *Alliance Formation in Civil Wars*, Fotini Christia examines conflicts in Afghanistan and Bosnia to describe how minority actors continually shift their allegiances and coalitions in order to maximize the outcome of their particular interest. In *The Trouble with the Congo,* Severine Autesserre studies why external intervention in internal conflicts often fails to achieve sustainable peace. She finds that the perceptions held by foreign interveners, formed from their own institutional biases, frequently leads to incorrect assessments about the nature of conflict, and then to ineffective actions. And in *The Logic of Violence in Civil War*, Stathis Kalyvas studies the local and geographic dynamics in civil wars that lead to violence by all parties against non-combatants as a means of influencing popular support. These are only three examples of the wealth of knowledge available on elements of conflict with which the unified action community has become very familiar. The theories of these scientists ought to contribute to the understanding of similar environments.

Causality, Complexity, and Microdynamics

Multidisciplinary and scholarly approaches

also seek out the hidden, but influential, cause-and-effect relationships that are poorly described by macro-narratives and strategic-level understanding. Design and other planning processes do account for cause-and-effect relationships; however, the oft-heard claim that military efforts have fallen short of achieving the desired political end states in Iraq and Afghanistan begs the question: Why? General Dempsey echoed as much in an interview in 2013 when he related a key lesson he learned as a wartime leader: "The application of force rarely produces—and, in fact, maybe never produces—the outcome we seek."[3] He and many senior military leaders assess that this shortfall begins with how the military understands the environment and the causal mechanisms of conflict. This assessment applies across all policy domains. Military and political actions and measures of effectiveness are often tied to assumptions that those policies and actions are engaging the right cause-and-effect relationships. If, however, those assumptions about causation are wrong, then agents of policy cannot hope to achieve their intended ends via their designed ways.

The military's institutional fixation on end states and the campaign plans to achieve them also highlight another common failing—the perception of the environment as being only complicated, rather than complex. The important distinction, as defined in David Snowden's use of the Cynefin framework for decision-making, is that the action models appropriate in one domain are unsuited for the other. When leaders and planners assess that an environment is only complicated, they mistakenly think of the environment as a problem to be solved through the application of subject-matter expertise, as though it were a calculus or engineering dilemma. This thinking implies that no matter how challenging the military problem, forces can achieve the desired end state if enough experts work on it. However, the solutions produced in this manner break down in complexity, lead to unintended consequences, and are overcome by the system's evolution. One's interaction with the human dimension will never be guided by the tame problems of complicated domains. There is nowhere in the world of policy and human engagement that is not complex. Those environments are permeated by constantly-evolving, wicked problems that are associated with moral, social, and political issues.

The military's institutional fixation on end states and the campaign plans to achieve them also highlight another common failing—the perception of the environment as being only complicated, rather than complex.

In 1973, urban planners Horst Rittel and Martin Weber described the characteristics of wicked problems in complex social planning. By reviewing a few of the rules for wicked problems, one instantly gains an appreciation for the immense challenge of complex environments. According to Rittel and Weber's rules, to fully describe a complex environment, the actor must compile an exhaustive list of possible interventions and their possible effects; it is, however, impossible to consider all potential interventions and effects. Solutions to wicked problems have no immediate means of measuring their effectiveness, have no termination date to their effects, and can only be about better-or-worse outcomes, not definitive ones. All wicked problems are the result or cause of other wicked problems.

Such problems result from the constant interaction among components in complex systems. These components, often systems of themselves, might be individuals, villages,

civic organizations, insurgent groups, and religious sects. They engage and evolve in spatial, temporal, and hierarchical domains, interacting in ways that may defy easy description. In complexity, cause-and-effect relationships do not exist in isolation, and the more subtle among them are rarely self-evident. The effects of micro-level interactions will spiral upwards through the system to influence macro-level actions and objectives. If strategic and operational practitioners are not attendant to tactical-level dynamics, then they cannot hope to influence or even to perceive the system effects occurring at that level.

Situational understanding is the sum of a multidimensional approach, causal understanding, and appreciating complexity.

Situational Understanding

Situational understanding is the sum of a multidimensional approach, causal understanding, and appreciating complexity. This approach supports and augments military doctrine. Army Doctrine Publication 5-0, *The Operations Process*, defines situational understanding as "the product of applying analysis and judgment to relevant information to determine the relationships among the operational and mission variables to facilitate decision making."[4] In practice, planners tend to emphasize the variables themselves, commonly referred to as PMESII-PT (the operational variables: political, military, economic, social, information, infrastructure, physical environment, and time) and METT-TC (the mission variables: mission, enemy, terrain and weather, troops and support available, time available, and civil considerations) .[5] But as our discussion of complexity suggests, the most important word in the definition of situational understanding is *relationships*.

The relationships between sub-variables, including all those associated with the human dimension, "establish the situation's context" in the plan phase of all operational processes dealing with complex problems. It is the evolution of those relationships, sometimes in response to intervention, that causes "periods of reduced understanding."[6] These notions of context and evolution bound up in relationships suggest that a temporal component ought to be more explicit in the definition: situational understanding also demands an appreciation of the historical and potential pathways of key relationships. By what path of contingency did the environment arrive at its current state? What path should military action steer to nudge the environment toward better long-term stability? The goal of such understanding is to more fully appreciate the potential military role within the environment—the more realistic the understanding, the greater the number and variety of interventions that might be brought to bear.

Practitioners must be aware that situational understanding is always fleeting. In some circumstances it may never be satisfactory. The world's pluralistic nature further confuses understanding through friction, emergence, and uncertainty. Friction is a term inherited from Clausewitz and well known among military professionals. It refers to the impossibility of perfect knowledge and prediction due to the constant interaction of events and individual judgments that produce new effects. In systems theory these are described as a system's emergent properties. These are the properties and effects in a system that derive but are completely unique from the properties and effects of its component parts. It is an act of creativity, sometimes accidental, that comes from the engagement of two or more system components.

Uncertainty is evident in both these concepts, but uncertainty implies something more: it is the counterintuitive knowledge that identical interventions conducted on an identical set of initial conditions are not guaranteed to produce the same results. This does not seem like a rational idea, yet it is experimentally proven in the field of physics. The implication for unified action practitioners is that confidence in their actions should be tempered by awareness that those actions will always produce unintended outcomes. It follows that, as Ritter and Weber proposed, a variety of potential actions must be considered against their potential outcomes.

A Menu of Options for Engagement

Unified action practitioners have an obligation to proffer advice to decision makers and partners based on their position and expertise. This advice should include a range of engagement options that inform the debate about policy and plans and give decision makers greater room to conduct cost-benefit and risk analysis. However, common practice in military planning usually limits the number of courses of action (COAs) considered. These COAs may offer little variation in their degree of impact because they all seek to achieve the same end state. This is a result of ends-ways-means thinking. However, if practitioners approach intervention in terms of choices and consequences, the objective is no longer to achieve a fixed, comprehensive end state. Discerning practitioners consider instead a spectrum of desired states and think of their interventions as moving the system incrementally toward a better state of affairs, of "finding our way forward to an improved position"[7] through experimental action. As unified action seeks greater harmony with the human dimension in conflict, this approach might suggest options that are nuanced in their effects and more appropriate in the midst of complexity. Another of Ritter and Weber's rules is that intervention in wicked problems is not about testing hypotheses, but is about trying to improve some aspect of the real world where people live. There is a penalty when the practitioner gets it wrong, and the greater the error, the greater the penalty. When understanding is poor, there is an incentive to tread lightly.

General Dempsey has also alluded to this concept of experimental action. In a recent interview posted on the website War on the Rocks, he contrasts the traditional campaign plan and end state approach to strategy with a complexity-influenced approach in which subtle, probing actions are taken to elicit subtle responses. Experimental action is the mode of choice for engaging newly emerging patterns in the environment. Complexity models like the Cynefin framework and wicked problem criteria also follow this logic. Small interventions allow practitioners to observe emerging patterns, identify cause-and-effect, and maintain greater control. Larger interventions produce larger immediate effects, but are also likely to have a higher number of indirect effects that might be obscured in the chaos of new patterns. So there is a potentially inverse relationship between the degree of intervention and the practitioner's ability to maintain situational understanding or control. As noted previously, once understanding is impaired, so too is the ability to craft effective interventions.

Unified action practitioners have an obligation to proffer advice to decision makers and partners based on their position and expertise.

An Obligation to Unified Action

Military professionals have a responsibility

to provide good situational understanding and advice about the potential influence of military capacity on policy. This is as true for tactical advisors, such as a civil affairs detachment supporting an embassy or regionally aligned force, as it is for the Chairman informing national security discourse. Unified action partners share a similar obligation as the common heritage of the war against violent extremism, which has created a high degree of interdependence among them. Complexity in the human dimension is as much a challenge for unified action partners as it is for the military. They face the same risk of falling short of policy intent if their situational understanding is poor. There ought to be a common desire among these partners to create mutual understanding and a broader narrative of the environment that benefits all. This is not to suggest there should be a common, agreed-upon narrative, but rather a common knowledge of all the conflicting narratives that partners bring into collaboration. Such a diversity of perspectives represents one of the best aspects of unified action and is akin to the multidisciplinary approach.

The spectrum of operations with which the military describes its conduct of policy is too narrow a framework for probable future efforts.

The U.S. military's chief concern is to fight and win the nation's wars. Recent conflicts, however, have led the military to appreciate threats that are not constrained by borders, yet often must be addressed within the boundaries of U.S. partners. The military has long had a role in diplomacy-dominated environments; yet, this role is often viewed as a discrete or technical adjunct to other policies. The growing interdependence of unified action partners prompts a re-evaluation of the benefits that military capacity might bring to peacetime conditions. The *U.S. Army Capstone Concept* still charges the military professional to fight and win the nation's wars, but now also to "prevent" and "shape" potential conflict environments before they give rise to wars or export violence. These two tasks clearly define a military obligation to peacetime national policy. They imply a greater purpose for military capacity than has been previously realized in policy approaches such as security cooperation or partner-capacity building. However, if the military is to fulfill such peacetime policy roles effectively, a change is required in how the military views its place in unified action.

The spectrum of operations with which the military describes its conduct of policy is too narrow a framework for probable future efforts. In its usual representation, the five phases of military operations—deter, seize initiative, dominate, stabilize, enable civil authority—show the rise and fall of military activity in war over time, from initiation of hostilities until transition to peace. Phase 3 (dominate) is largest, suggesting its greater importance to the military over other phases. The five phases are bookended, pre- and post-conflict, by Phase 0, a steady state condition of non-conflict which is represented with no greater significance than any other phase. The graph of activity in these phases suggests that military action in a given conflict starts from nothing in the pre-war Phase 0, and tapers to nothing in the post-war Phase 0. This conceptualization does not represent the reality of the policy world, and it does not resonate with non-military unified action partners.

Military professionals ought to view themselves as unified action partners first and foremost. The "strategic corporal," after all, influences more than military policy; he must ask "how does my tactical action benefit the long-term interests of the nation?" In

recognition of its greater role in non-conflict environments, the military should see that it is only one of many partners acting on a spectrum of policy application. On this policy spectrum, Phase 0 is the predominant global condition. The phases of military operations are the exception, coming into being when necessitated by policy. Extending this perspective, practitioners can appreciate that multiple unified action partners contribute to policy objectives at any point on the spectrum. The implication is clear: defense, diplomacy, development, and other interagency actors share a blending of roles in both peacetime and in war.

Conclusion

The human dimension is an ever-present variable in the operational and policy environment. Improving military engagement in that dimension can only come from constructive changes in ethical, doctrinal, and practical approaches. In "Toward Strategic Landpower," Lieutenant General Charles Cleveland and Lieutenant Colonel Stuart Farris captured the importance of these changes: "If we believe military success will most likely require a deep understanding of…the human factors involved in a given conflict, then recognizing the human domain becomes a critical organizing and resourcing concept for supporting national security."[8] Defense institutions and leaders at all levels must play an important role in bringing better understanding into common practice. To this end, DoD has expanded its research relationships with academic institutions to broadly explore complexity and human elements. Former Secretary of Defense Robert Gates launched the Minerva Initiative in 2007 to "improve the ability of DoD to develop cutting-edge social science research, foreign area and interdisciplinary studies, [which are] developed and vetted by the best scholars in these fields."[9] It only makes sense that the military should consult this body of knowledge as a component of its environmental understanding. But such practice has not yet reached the operational force, and scholarly methods and research are rarely discussed within professional military education. Situational understanding suffers as a result, as do the strategies, campaign plans, and courses of action that are intended to support policy.

Military and other policy professionals have an ethical obligation to advise and inform the conduct of unified action in peace, war, and other circumstances, which requires consideration of a menu of engagement options suited to the environment. Situational understanding of the complex systems and causal stories throughout all levels is critical for identifying interventions that may incrementally improve conditions or minimize unintended consequences. Existing military doctrine and common practice do not support this depth of understanding. Multidisciplinary approaches and rigorous, validated research do improve understanding and warrant consideration by planners and leaders in all policy domains. Adopting these approaches and the forthcoming doctrinal changes focused on the human dimension require open and honest discourse about the military's roles and professional obligations. Now is the time to find the way forward to better understanding. ***IAJ***

NOTES

1 Training and Doctrine Command Pam 525-3-0, *The U.S. Army Capstone Concept*, U.S. Department of the Army, Training and Doctrine Command, Fort Eustis, VA, 2012.

2 Joint Publication 1, *Doctrine for the Armed Forces of the United States*, U.S. Department of Defense, Joint Chiefs of Staff, Washington, DC, 2013.

3 "Joint Chiefs Chairman Gen. Martin Dempsey on 'This Week'," interview with Martha Raddatz, <http://abcnews.go.com/ThisWeek/video/joint-chiefs-chairman-gen-martin-dempsey-week-19865953>, August 13, 2013, accessed on March 29, 2014.

4 Army Doctrine Publication 5-0, *The Operations Process*, Headquarters, Department of the Army, Washington, DC, 2012.

5 Army Doctrine Reference Publication 5-0, *The Operations Process*, Headquarters, Department of the Army, Washington, DC, 2012.

6 Ibid.

7 Huba Wass de Czege, "Strategizing Forward in the Western Pacific and Elsewhere," Landpower Essay No. 13-4, Association of the United States Army, Institute of Land Warfare, Arlington, VA, 2013.

8 Charles T. Cleveland and Stuart L. Farris, "Toward Strategic Landpower," *Army*, Association of the United States Army, Arlington, VA, 2013.

9 The Minerva Initiative, "Program History and Overview," Minerva Initiative homepage, <http://minerva.dtic.mil/overview.html>, accessed on April 20, 2014.

Cyberdefense: *Is Outsourcing the Answer?*

by Kellen Ashford

Speaking at an event for the American Enterprise Institute in 2012, retired General Keith Alexander, the former head of U.S. Cyber Command and Director of the National Security Agency, suggested that "cyber crime is the greatest transfer of wealth in history."[1] The commercial cost of cyber crime is debatable, but General Alexander cited two figures, provided by Symantec and McAfee, that cyber crime costs U.S. companies $250 billion a year and $1 trillion a year globally. While these are estimates, the U.S. weapons systems linked to Chinese cyberespionage not only represent a significant transfer of dollar costs, but also associated military capability. In the non-public version of the Defense Science Board's report, "Resilient Military Systems and the Advanced Cyber Threat," the F-35 Joint Strike Fighter, Littoral Combat Ship, Aegis Combat System, and THAAD missile defense systems were among those whose designs have been compromised by Chinese cyberespionage campaigns. While the Chinese and other attackers pilfer contractor networks for intellectual property, they are also able to map Defense Department networks. For example, during the Chinese cyber campaign against QinetiQ North America, hackers were able to infiltrate the U.S. Army's Aviation and Missile Command.

Traditionally, former Cold War rival, Russia was viewed as the main threat to U.S. cybersecurity. In 2007, Estonia, often referred to as "e-Stonia" in technology circles, experienced "distributed denial of service" (DDoS) attacks that affected the government and financial industry. In an April editorial in *The New York Times*, Toomas Hendrik Ilves, President of Estonia, does not attribute blame for the attacks; however, initial suspicions and blame were cast at Russia. The cyberattacks took place after the Estonian government decided to move the Soviet-era "Bronze Soldier of Tallinn," which was followed by riots from ethnic Russians. Following the DDoS attacks, Estonian

Kellen Ashford is a graduate student at the University of Kansas. Formerly a student of political science, Ashford became interested in cybersecurity while working with clients in the defense and aerospace industries. This essay was written prior to Edward Snowden's leaks on the NSA became public knowledge, during Ashford's internship at the Simons Center.

Prime Minister Andrus Ansip suggested that the attacks originated from "Russian state authorities."[2]

While Russia remains a threat to U.S. cybersecurity, both countries have signed a cybersecurity pact aimed at reducing tensions between the two in cyberspace.

While Russia remains a threat to U.S. cybersecurity, both countries have signed a cybersecurity pact aimed at reducing tensions between the two in cyberspace. The pact calls for increasing communication and information sharing on cyber threats, as well as forums aimed at broadening cybersecurity cooperation.[3] In contrast to the perceived Russian cyberthreat, recent government and media attention has focused on cyberattacks and cyberespionage campaigns waged by Chinese hackers, and rightly so. Verizon's "2013 Data Breach Investigations Report" found that 96 percent of cyberespionage campaigns originated in China.[4] In early 2012, Mandiant, a cybersecurity company, released a report that linked cyberespionage to Unit 61398 (also called the Comment Crew or APT1), a division of the People's Liberation Army (PLA). Additionally, Chinese universities have also been linked to cyberattacks on the U.S. The Key Laboratory of Aerospace Information Security and Trusted Computing at Wuhan University, which receives funding from the PLA, has been linked to cyberattacks, and over 760 Chinese military and government officials are reported to have connections to the university.[5]

While critical infrastructure, government, and military networks remain at the center of cybersecurity concerns, the defense contracting community has been thrust onto the front lines of the cyberwar. Not only are the contractors' weapon systems subject to intellectual property theft, but they are also becoming the first responders for the U.S. government. In order to better secure their networks, defense contractors have taken both defensive and offensive measures against these cyberthreats. "Active defense," "hacking back," and "threat intelligence" are being discussed more frequently, if not becoming common offensive and defensive measures. The Commission on the Theft of American Intellectual Property, led by former Director of National Intelligence Admiral Dennis C. Blair and former Ambassador to China Jon Huntsman Jr., released a report which suggested that companies be allowed to "hack back" against hackers. Furthermore, Jim Jaeger, Vice President of General Dynamics Fidelis Cybersecurity Solutions, recently suggested that "if a company wants to go after a cyber criminal who is responsible for a security breach, who is going to complain? The hacker? Frankly, I think it's really good to see."[6]

Cyberattacks and cyberespionage are likely to continue against private and public networks in the U.S. and cyberdefense remains a priority. While the National Security Agency and defense contractors engage hackers with offensive measures, the need to defend America's networks has never been greater. Yet, in order to understand the importance of cyberdefense in the modern age, it is also important to understand the threat—in this case—Chinese hackers. While media attention continues to focus on how hackers attack and what their specific targets are, the bigger question is why the Chinese wage cyberespionage campaigns against defense contractors, the U.S. government, and critical infrastructure.

"The culture of hacking in China is not confined to top-secret military compounds where hackers carry out orders to pilfer data from foreign governments and corporations. Hacking thrives across official, corporate, and criminal

worlds."[7] Understanding the cyberthreat posed by the Chinese is to understand China, its history, and its intentions on the global stage. In his book, *21st Century Chinese Cyberwarfare*, William T. Hagestad II suggests: "The 'Middle Kingdom,' which is China, is determined, and in their focus destined to achieve worldwide leadership through the use of their state-sponsored, military-developed, and civilian-executed information dominance."[8]

As Hagestad does in his book, it is important to distinguish between the types of Chinese hackers, as their intentions and command and control structures vary. Most often associated with hacking U.S. computer networks, the PLA, under orders from the Communist Party of China (CPC), hacks as a means to equal the playing field between itself and the U.S. in the event of a crisis or war. China's cyberwarfare doctrine began to take shape after PLA officials saw the power that modern, information-enabled forces had during the Persian Gulf War. The U.S. targeted Iraqi command and control sites during the air campaign in order to disrupt its flow of information. U.S. armed forces were also able to use information to coordinate and synchronize movements and attacks. In an interview with PBS Frontline, John Arquilla, an associate professor at the Naval Postgraduate School, suggests that "the cyber things we did in the last Gulf War had much to do with the management of our own information."[9] Seeing how the U.S. used information dominance in the Gulf War, the PLA realized that in any hypothetical, future conflict with the U.S., achieving information dominance would be necessary in order to be victorious. To do so, the Chinese would need to use cyberattacks to disrupt U.S. command and control networks, effectively disrupting the flow of information and intelligence. Thus, as it stands today, the PLA's primary motive is "to map military capabilities that could be exploited during a crisis."[10]

In contrast, yet often in conjunction with the PLA, state-owned enterprises (SOE) use cyberwarfare for industrial espionage. As Hagestad notes, these SOEs are "successful multinational commercial enterprises, which must now compete on the world stage, without the benefit of knowing how to compete fairly."[11]

The industrial espionage typically associated with Chinese state-owned enterprises often concerns weapon designs and weapon systems.

The industrial espionage typically associated with Chinese SOEs often concerns weapon designs and weapon systems. While the PLA often benefits from having these designs, so do SOEs. For example, the Chinese J-31 fighter bears a remarkable resemblance to Lockheed Martin's F-35 Joint Strike Fighter. However, the PLA did not build the J-31; Shenyang Aircraft Corporation built it. Similarly, the J-20 fighter built by Chengdu Aircraft Industry Group closely resembles Lockheed Martin's F-22 Raptor. Interestingly, it has been suggested that Pentagon insiders question the Raptor's ability to perform in combat due to the extensive hacking that subcontractors faced while working on the fighter.[12]

Moreover, SOE-sponsored hacking is not limited to U.S. defense contractor weapon designs. SOE-sponsored hacking plays a role in China as well. For example, Edward Wong of *The New York Times* reported that Sany Group, a construction equipment manufacturer in China, used hackers to spy on a rival company, Zoomlion.[13] There are also political motivations for Chinese hacking. China's "Great Firewall" and Internet censorship have been well documented over the years. According to Wong, "local police departments contract

with companies like Xhunter to monitor and suppress dissent" within China itself.[14] Furthermore, he notes that Ai Weiwei, an artist who was arrested in 2011, stated that "every time anyone is arrested or checked, the first thing [the authorities] grab is the computer."[15] The CPC also uses information gathered by the PLA to map the decision-making process of policymakers and their professional networks, as suggested by the Pentagon's "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013." According to Brian Manzec, "The goal is not to deter other nations from conducting cyberwarfare against the People's Republic of China; rather, it is to use the threat of cyberwarfare to deter an actor from behaving in a manner that is in opposition to Chinese strategic interests."[16]

...hackers themselves often move between the government, military, and corporate positions looking for the largest paycheck.

While the various actors and interested parties engaged in hacking have been identified in China, it does not prevent overlap. As demonstrated, information gathered by the PLA is often used by SOEs or the CPC. Additionally, hackers themselves often move between the government, military, and corporate positions looking for the largest paycheck. Some are even outsourced. An anonymous hacker, quoted in *The New York Times*, adds some important insight on the monolithic nature of hacking in China. "China's government is so big. It's almost impossible not to have any crossover with the government….[The hackers] work for one thing, and that's for money."[17] Ultimately, while there are many interpretations of why the Chinese conduct cyberespionage campaigns, Hagestad's interpretation fits current, global affairs quite well since it makes note of the CPC's intentions on the global stage. "The motivation of the People's Republic of China to conduct cyberwarfare is comprised of fear, self-preservation, and hegemony."[18] One cyberattack, in particular, highlights how multiple Chinese parties benefited from hacking an American defense contractor.

A Bloomberg News investigation, using hacked HBGary Inc. emails from the hacking collective "Anonymous," found that QinetiQ North America was hacked over a three-year operation in which "most, if not all of the company's research" had been compromised by PLA Unit 61398.[19] While the investigation focuses solely on QinetiQ, it does make note that "QinetiQ was only one target in a broader cyberpillage," and that almost every defense contractor in the U.S. was a victim of Chinese cyberattacks during the same period.[20] This long-running hacking operation demonstrates that Chinese hackers have revolving targets that reflect different objectives.

Following the precedent of mapping U.S. networks, one focus of the QinetiQ operation was mapping shared networks between U.S. defense contractors, the government, and the military. For example, NASA alerted QinetiQ that one of its computers was used by hackers to try and infiltrate the agency's network.[21] Likewise, a cyber breach at the Redstone Arsenal, home of the Army's Aviation and Missile Command, Materiel Command, and the Missile Defense Agency, was also linked to a shared network with QinetiQ.[22] The attacks on these networks have allowed the PLA to map important shared networks between the military and defense contractors, not only to exploit during a war, but to also pilfer weapon systems' designs in order to exploit these systems in a war-time scenario or use the designs to manufacture their own.

According to this investigation, the Chinese hackers targeted specific engineers because they

were interested in "an innovative maintenance program for the Army's combat helicopter fleet."[23] Specifically, the target was the U.S. Army's Condition-Based Maintenance (CBM) program. This program was a cybertarget as on-board sensors collect data on deployed Army helicopters, which would allow the PLA to examine the deployment, performance, and maintenance needs of the Army's helicopter fleet.[24] According to an Army logistics presentation, the data gathered by these sensors includes classified command and control information, which gives the PLA access to valuable information, such as secure radio and identification friend or foe frequencies used by the Army. In another case, the hackers also targeted QinetiQ's advanced robotics unit. Not only did the Chinese use the stolen intellectual property to build a bomb disposal robot, similar to QinetiQ's "Dragon Runner," but it also allowed the PLA to understand the hardware the U.S. would deploy in a military conflict. Noel Sharkey, a robotics expert at Britain's Sheffield University, speaking to Bloomberg, suggested that the "chip architecture" used to build the PLA knock-off of the Dragon Runner could also be used against U.S. robotics or unmanned aerial vehicles.[25]

The cyberattack on QinetiQ also illustrates the need for defense contractors to plan for and execute cyberdefense plans. In the case of this hack, the company often ignored recommendations from advisors. "They felt like it was this limited little thing, like they'd picked up some virus," Brian Dykstra, a computer forensics expert said.[26] Worried about the costs associated with patching its networks, executives at QinetiQ continued to ignore recommendations by these hired advisors. In an interview, William Ribich concluded that QinetiQ was worried about the costs associated with securing its computer networks after the breach. A fix, recommended by Mandiant, was ignored. Consultants HBGary and Verizon Terremark faced similar challenges while trying to secure QinetiQ's networks. HBGary faced criticism from both Terremark and QinetiQ, and further believed Terremark was hoarding valuable data for itself. In another example, employees at QinetiQ would often delete security software installed by HBGary. As such, this cyber incident at QinetiQ was a perfect storm—a company with lax security, working on top secret military projects, met a formidable and malicious foe in Unit 61398. While fixes were recommended, they were often ignored by executives or resulted in backlash from employees. In the end, the Pentagon released a statement early in 2013 saying that the QinetiQ leaks were being probed. That statement would later be retracted by the Department of Defense, with spokesman Damian Pickart saying "while the reports of cyber intrusions against QinetiQ are disturbing, the Department of Defense is not in a position to investigate the security practices of a private company—including cleared defense contractors."[27] Overall, the attack on QinetiQ demonstrates the need for companies, in this case, defense contractors, to effectively secure their networks in order to guard valuable military information.

...the attack on QinetiQ demonstrates the need for companies, in this case, defense contractors, to effectively secure their networks in order to guard valuable military information.

According to Mandiant's report on Unit 61398, Chinese hackers begin their attacks on companies with a spear-phising campaign. In such a campaign, hackers send out emails with malicious files attached in hopes that an unsuspecting employee downloads the

attachment, opening a gateway into the target's network. Mandiant further suggests that "spear-phising is [Unit 61398]'s most commonly used technique."[28] In order to defend against such campaigns, defense contractors, including Lockheed Martin and Northrop Grumman, spear-phish their own employees to increase awareness of hackers' techniques to infiltrate computer networks.

According to reports, Northrop Grumman began spear-phising employees in 2009, and has "made running phising exercises a regular habit."[29] The goal of these exercises is to raise awareness among employees of such spear-phising campaigns, regardless of their origins. Brian Fung of the *National Journal* reported that a recent, internal campaign at Northrop Grumman targeted 68,000 employees using the façade of errors on their tax returns as a feint.[30] Similarly, Lockheed Martin began their "I Campaign" in 2009, which targets employees with spear-phising emails as well. These "messages are customized for various groups or individuals in the company" as the attack on QinetiQ often targeted groups of employees or individual business sectors, such as the company's robotics unit.[31] Both Lockheed Martin and Northrop Grumman have reported increased awareness and reporting of these attacks among employees. Chandra McMahon, Chief Information Security Officer (CISO) at Lockheed Martin claims, "I can say definitely that not only do I have more employees taking good actions with regard to emails, but more are reporting suspicious emails to the [Computer Incident Response Team]—and attacks have not been able to get started."[32] Similarly, Michael Papay, CISO for Northrop Grumman, makes a similar point. "If I've got 70,000 employees who are smart enough to say, 'Whoa, looks like a spear-phishing e-mail—I'm going to report it to my cybersecurity operations center,' then my operations center can dig into it and immediately block anyone else in the company from getting that e-mail."[33] Lockheed Martin has also launched products geared toward managing cybersecurity problems. In a 2010 interview with *National Defense Magazine*, the former director of the Defense Information Security Agency and Vice President of Cybersecurity Solutions for Lockheed Martin Charles Croom discussed that the company was automating software and using an encrypted thumb-drive, called "IronClad," to manage cybersecurity needs.[34] While these defense contractors and their competitors continue to work on improving their networks' security, they are also engaging hackers on the front lines of the cyberwar.

Aided by hackers, defense contractors, and the technology industry, U.S. defense and intelligence agencies have turned the world of security research upside down.

Speaking anonymously to Reuters, a former defense contractor executive was quoted as saying "my job was to have 25 zero-days on a USB stick, ready to go," referring to attacks which exploit unknown vulnerabilities in computer programs.[35] While the majority of media reports on Chinese cyberespionage, the offensive cyber capabilities of the U.S. are often overlooked, and for good reason, as "details about the U.S. offensive cyber capabilities and operations are almost all classified."[36] Aided by hackers, defense contractors, and the technology industry, U.S. defense and intelligence agencies have turned the world of security research upside down. In order to gather intelligence on foreign targets and exploit networked military systems, the National Security Agency has reportedly become the largest buyer of security exploits.[37] Companies such as Harris Corporation, Northrop Grumman, and Raytheon

have acquired boutique firms that focus on exploiting these vulnerabilities. Information on bugs in popular Microsoft software is given to U.S. intelligence agencies before the company releases a public patch to secure these flaws.[38] Furthermore, in hacked emails, leaked by Anonymous, the capabilities of Endgame Inc. were exposed as well. The company, chaired by the CEO of the Central Intelligence Agency's venture capital firm In-Q-Tel, markets zero-day exploits and the ability to mobilize and exploit criminal botnets in order to relay important information to clients, including intelligence agencies. However important cyberoffense is to maintaining intelligence capabilities or exploiting and degrading enemy networks, it also comes at a price, and according to Charlie Miller, a security researcher at social media giant Twitter, "the only people paying are on the offensive side."[39]

While these zero-day exploits are being used offensively, the Department of Homeland Security (DHS) has also set up a system to use them defensively, a move which will aid the defense of computer networks tremendously. Through the "Enhanced Cybersecurity Services" (ECS) program, information gathered by defense contractors, intelligence agencies, and telecommunications providers will be offered to other companies, notably those in the critical infrastructure and financial industries.[40] While this program takes a substantial step toward defending the nation's networks, it is important to note that the ECS program is young and still evolving. The ECS program has also come under fire for being too limited. Security officers laud the program for what sharing it does do, but also acknowledge that the government and chosen providers, such as Northrop Grumman and Raytheon, limit the shared data because these vulnerabilities have valuable, offensive capabilities. Wolfgang Kandek, Chief Technology Officer of Qualys states, "From an offensive point of view, it is certainly valuable to maintain a certain number of exploits in private, but for defense the best option is to share the vulnerability information with the software vendor as quickly as possible."[41] Echoing this sentiment, research director for NSS Labs Andrew Braunberg critiques the ECS program stating, "Most obviously, the U.S. government wants it both ways. They don't really want these vulnerabilities to disappear because they want to use them offensively, but they don't want the same vulnerabilities to allow hacking of U.S. assets."[42]

While the ECS program takes an important step in sharing information on network vulnerabilities with companies in the U.S. that could be exploited by Chinese hackers, revelations of the National Security Agency's domestic intelligence gathering could cause a backlash among Americans that harm further efforts to scan Internet traffic aimed at protecting networks from hackers. Under the ECS program, Web traffic that flows into and out of private businesses will be scanned for irregularities, which was initially limited to defense contractors and government agencies. Yet, as revelations about the National Security Agency's PRISM program were leaked to the press by Edward Snowden, more Americans have become aware that information transmitted online was being scanned and could increasingly be scanned as the government seeks to limit cyberattacks. These concerns

...as revelations about the National Security Agency's PRISM program were leaked to the press by Edward Snowden, more Americans have become aware that information transmitted online was being scanned...

could be further echoed by legislators as the debate on the Cyber Intelligence Sharing Protection Act faces Congressional scrutiny, since the legislation seeks to share more threat intelligence with the National Security Agency. Absent and fractured leadership on cybersecurity also threatens the defense of America's computer networks.

Faced with securing civilian networks and assisting the private sector, DHS faces a void of leadership that could complicate efforts to protect American networks from hackers. While these leadership roles can be filled, these vacancies represent a larger, troubling trend for the department as it must compete for hackers and qualified professionals with the National Security Agency and private industry. In an effort to attract technology students to government service, the National Science Foundation's CyberCorps Scholarship for Service program saw a majority of its graduates go on to work for the National Security Agency instead of DHS.[43] Furthermore, on average, government salaries fail to match those offered in industry. For instance, a cybersecurity professional working in government makes $99,000, while the average in industry is $107,000. While the DHS and government as a whole struggle with these discrepancies, Dr. Daniel Goure, vice president of the Lexington Institute, believes this is actually a positive trend. Following the release of the Defense Science Board's report, he penned an opinion piece that called on the private sector to defend the nation's networks, as many defense contractors have set up cybersecurity units in order to plug their leaks. "Major defense companies such as Lockheed Martin, Boeing, Northrop Grumman, and General Dynamics stood up cyberdefense units, initially to protect their own networks and computer systems. In many ways, these companies are now on the front line of the ongoing and intensifying cyberwar."[44] Goure also points out that as private companies, defense contractors have a particular interest in defending their networks and creating cost-effective cybersecurity solutions to market to government agencies and other businesses. He concludes by stating that "when it comes to cyberdefense, the nation increasingly is dependent on the private sector."[45] Goure's statement is echoed by both Boeing and Lockheed Martin who provide their expertise in cybersecurity to their clients.[46] Boeing markets its cybersecurity capabilities commercially using the solutions they employ in-house as the product. Using this technique allows Boeing "to sell that one product many times," according to Bryan J. Palma, vice president of security and information services for Boeing.[47]

This private sector-led model for cyberdefense may be a good fit for U.S. government agencies. As China's CPC uses the PLA and outsourced hackers from SOEs and skilled individuals, the private sector-led model could provide cyberdefense to U.S. government agencies and critical infrastructure. The U.S. government's role in cyberdefense and cyberoffense must be greater. Placing the Homeland Security and Defense departments in regulatory and oversight roles will allow the government to set guidelines and standards that these private sector companies must follow in securing U.S. cyber vulnerabilities. This will also create competition for commercial and government contracts that will continue to drive innovation in cybersecurity research. Potentially, these private sector contactors may also be able to use threat intelligence and intelligence gained by hacking back through intelligence agencies to infiltrate and map Chinese networks for the Department of Defense. However, it would be the role of U.S. government agencies to set limits on the contractors' offensive measures, preventing future conflicts or a full-blown cyberwar. ***IAJ***

NOTES

1 Emil Protalinski, "NSA: Cyber Crime is 'the Greatest Transfer of Wealth in History,'" ZDNet homepage, U.S. edition, <http://www.zdnet.com/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history-7000000598>, July 10, 2012, accessed on June 4, 2013.

2 Richard Koman, "Estonia Reeling from Massive Cyberattack from Russia," ZDNet homepage, U.S. edition, <http://www.zdnet.com/blog/government/estonia-reeling-from-massive-cyberattack-from-russia/3161>, May 18, 2007, accessed on June 4, 2013.

3 Ellen Nakashima, "U.S. and Russia Sign Pact to Create Communication Link on Cybersecurity," *The Washington Post* homepage, <http://articles.washingtonpost.com/2013-06-17/world/40025979_1_cyber-security-pact-homeland-security>, June 17, 2013, accessed on June 18, 2013.

4 Verizon RISK Team, "2013 Data Breach Investigations Report," <www.verizonenterprise .com/DBIR/2013/>, accessed on March 25, 2013.

5 Bill Gertz, "Network Effects: Chinese University Linked to PLA Cyber Attacks," Free Beacon homepage, < http://freebeacon.com/?s=Network+Effects&submit=>, May 14, 2013, accessed on May 15, 2013.

6 Cadie Thompson, Businesses Consider Going Offense Against Cyberattackers," CNBC homepage, <http://www.cnbc.com/id/100789013>, June 4, 2013, accessed on June 8, 2013.

7 Edward Wong, "Hackers Find China is Land of Opportunity," *The New York Times* homepage, <www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html>, May 22, 2013, accessed on May 23, 2013.

8 William T. Hagestad II, *21st Century Chinese Cyberwarfare*, IT Governance Publishing, Cambridgeshire, UK, 2012, p. 2.

9 PBS Frontline, Interview: John Arquilla, Frontline homepage, <http://www.pbs.org

/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html>, March 4, 2003, accessed on May 27, 2013.

10 David E. Sanger, "U.S. blames China's Military Directly for Cyberattacks," *The New York Times* homepage, <http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html>, May 6, 2013, accessed on May 7, 2013.

11 Hagestad, p. 5.

12 Michael Riley and Ben Elgin, "China's Cyberspies Outwit Model for Bond's Q," Bloomberg homepage, <http://www.bloomberg.com/news/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets.html>, May 2, 2013, accessed on May 2, 2013.

13 Wong.

14 Ibid.

15 Ibid.

16 Hagestad, p. 33.

17 Wong.

18 Hagestad, p. 26.

19 Riley and Elgin.

20 Ibid.

21 Ibid.

22 Ibid.

23 Ibid.

24 Ibid.

25 Ibid.

26 Ibid.

27 Ben Elgin, "Pentagon Retracts Statement on Probe of QinetiQ Hacking," Bloomberg homepage, <http://www.bloomberg.com/news/2013-05-07/pentagon-retracts-statement-on-probe-of-qinetiq-hacking.html>, May 7, 2013, accessed on May 8, 2013.

28 "APT1: Exposing One of China's Cyberespionage Units," Mandiant Intelligence Center, <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>, p. 28, accessed on March 5, 2013.

29 Brian Fung, "This Defense Contractor is Reportedly Spear-Phising 68,000 Innocent People," *National Journal* homepage, <http://www.nationaljournal.com/tech/this-defense-contractor-is-repeatedly-spear-phishing-68-000-innocent-people-20130403>, April 3, 2013, accessed on April 4, 2013.

30 Ibid.

31 Kelly Jackson Higgins, "How Lockheed Martin Phishes Its Own," InformationWeek: Dark Reading homepage, <http://www.darkreading.com/risk/how-lockheed-martin-phishes-its-own/d/d-id/1139629>, April 25, 2013, accessed on April 28, 2013.

32 Ibid.

33 Fung.

34 Sandra I. Erwin, "Surge of Cybersecurity Bureaucracies Sparks Lucrative Opportunities for Industry," National Defense homepage, <http://www.nationaldefensemagazine.org/archive/2010 /September/Pages/SurgeofCybersecurityBureaucraciesSparksLucrativeOpportunitiesForIndustry.aspx>, September 1, 2010, accessed on May 30, 2013.

35 Joseph Menn, "Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback," Reuters homepage, <http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510?, May 10, 2013, accessed on May 15, 2013.

36 Warren Strobel and Deborah Charles, "With Troops and Techies, U.S. Prepares for Cyber Warfare," Reuters homepage, <http://www.reuters.com/article/2013/06/07/us-usa-cyberwar-idUSBRE95608D20130607>, June 7, 2013, accessed on June 12, 2013.

37 Menn, "Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback."

38 Michael Riley, "U.S. Agencies Said to Swap Data with Thousands of Firms," Bloomberg homepage, <http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.

html>, June 14, 2013, accessed on June 16, 2013.

39 Menn, "Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback."

40 Joseph Menn, "U.S. to Protect Private Sector from Secret Software Attacks," Reuters homepage, <http://www.reuters.com/article/2013/05/15/us-cyber-summit-flaws-idUSBRE94E11B20130515>, May 15, 2013, accessed on May 15, 2013.

41 Antone Gonsalves, "Experts Ding DHS Vulnerability Sharing Plan as Too Limited," CSO homepage, <http://www.csoonline.com/article/733557/experts-ding-dhs-vulnerability-sharing-plan-as-too-limited>, May 17, 2013, accessed on May 20, 2013.

42 Ibid.

43 Nicole Perlroth, "Tough Times at Homeland Security," *The New York Times*, Bits section homepage, <http://bits.blogs.nytimes.com/2013/05/13/tough-times-at-homeland-security>, May 13, 2013, accessed on May 14, 2013.

44 Daniel Goure, "U.S. Defense Contractors Have Developed Serious Cybersecurity Capabilities," Lexington Institute homepage, <http://www.lexingtoninstitute.org/us-defense-companies-have-developed-serious-cyber-security-capabilities?a=1&c=1171>, May 29, 2013, accessed on May 29, 2013.

45 Ibid.

46 Marjorie Censer, "Defense Contractors Translate Their Own Cybersecurity Protections into Business," *The Washington Post*, Capital Business section homepage, <http://www.washingtonpost.com/business/capitalbusiness/defense-contractors-translate-their-own-cybersecurity-protections-into-business/2013/03/17/75e7098c-82a6-11e2-b99e-6baf4ebe42df_story.html>, March 17, 2013, accessed on March 25, 2013.

47 Ibid.

Worth Noting

Compiled by Elizabeth Hill

Fort Lee Professor Wins 2013 CGSC Faculty Interagency Writing Competition

The Arthur D. Simons Center for Interagency Cooperation would like to congratulate Dr. William J. Davis, Jr., associate professor in the Department of Joint, Interagency, and Multinational Operations at the Fort Lee, Va., satellite campus of the U.S. Army Command and General Staff College, for winning the 2013 CGSC Faculty Interagency Writing Competition sponsored by the CGSC Foundation's Simons Center for Interagency Cooperation.

Dr. Davis is a 24-year veteran of the U.S. Navy and has been a professor at CGSC since 2006. He was previously an associate professor and director of curriculum at Joint Forces Staff College in Norfolk, Va. Davis was presented his award during the College's Golden Pen Award ceremony in January 2014. His manuscript, "Why We Can't All Just Get Along: Overcoming Personal Barriers to Inter-organizational Effectiveness" can be found on page 25 of this edition of the *InterAgency Journal*.

The "Call for Papers" for the 2014 CGSC Faculty Writing Competition will be made in September 2014. ***IAJ***

DISA Releases 2014-2019 Strategic Plan

In May, the Defense Information Systems Agency (DISA) released its strategic plan for 2014-2019. The strategic plan outlines DISA's focus areas, guiding principles, and strategic goals for the future.

In his introduction to the DISA strategic plan, DISA director Lt. Gen. Ronnie D. Hawkins, Jr. (USAF) discusses DISA's shifting priorities in a post-conflict and financially constrained era. Hawkins also explains DISA's focus on cyberspace sovereignty, agility, and innovation, and says that DISA is the premier IT and Cyber Combat Support Agency for DoD, the nation, and U.S. coalition partners

Among DISA's guiding principles is its commitment to support the Department of Defense and DoD's joint, interagency, and international mission partners. DISA's strategic plan includes four strategic goals, and two of these four goals involve increased and more efficient information sharing. For instance, the first goal calls for a consolidated, collaborative, and secure joint information environment that would enable information sharing and interdependent enterprise services across DoD that are seamless, interoperable, efficient, and responsive to joint and coalition requirements. The second goal of the strategy is to engineer, provide, and enhance information sharing capabilities to enable decision makers to exercise authority and direction over forces and resources.

The DISA strategic plan also outlines objectives for the DISA Information Enterprise and makes suggestions for optimizing the department's investments. ***IAJ***

Report Proposes New Civil Service Framework

In April, the Partnership for Public Service and Booz Allen Hamilton released a report calling for major reforms to the federal government's decades-old civil service system. According to the report, while the type of work and skills needed to carry out civil service work have changed, the current civil service system remains "a relic of a bygone era," and is not conducive to addressing today's complex, interagency challenges.

Planning for and supporting the future federal workforce will require adapting to change, and the Partnership report suggests six ways to overhaul the current civil service framework, including unifying the civil service and investing in leadership.

A unified civil service system would enable the federal government to act as an integrated enterprise. The unified service would be joined together by core civil service principles based on lessons learned across multiple agencies that can be used to address issues in 21st century government. The report also suggests creating a single senior federal executive service to foster interagency mobility and the development and deployment of that cadre of elite enterprise executives who can handle multi-agency missions and functions.

The suggested framework also includes a four-tier senior executive service leadership structure, with the top tier reserved for a small number of enterprise executives who have demonstrated the skills necessary to take on government-wide responsibilities and lead cross-agency initiatives. Among their qualifications, these executives would need strong collaborative skills and the ability to lead across organizational boundaries and utilize inter-organizational networks. They would also need to facilitate interagency collaboration through a shared sense of mission. ***IAJ***

Interagency Task Force Reports on Human Trafficking

On April 8, Secretary of State John Kerry chaired the annual meeting of the President's Interagency Task Force to Monitor and Combat Trafficking in Persons (PITF). During the meeting, the PITF discussed progress made by the task force, including the implementation of a whole-of-government approach and incorporating survivors' input and expertise in combating human trafficking. The annual cabinet-level meeting also provided an opportunity to coordinate government-wide efforts and discuss new initiatives in the struggle to end modern slavery. PITF member agencies were also encouraged to pursue innovation in their agency's response to human trafficking.

The PITF also released their progress report on combating trafficking in persons earlier this month. The report reviews PITF's ten strategic objectives and addresses efforts made to combat modern slavery and the trafficking of persons—including sex trafficking, labor trafficking, and the unlawful recruitment or use of child soldiers—by PITF and its operational arm, the Senior Policy Operating Group (SPOG).

The report also highlights PITF strengthening the SPOG as well as accomplishments of the individual agencies in combating human trafficking. Among these accomplishments is the Departments of Justice, Labor, and Homeland Security's collaboration in developing high-impact human trafficking investigations through six pilot Anti-Trafficking Coordination Teams (ACTeams). These departments also developed regional strategic plans, implemented coordinated

strategies, and disseminated ACTeams Operations Guides.

The PITF report praised the work of the departments of State, Defense, Justice, Labor, Health and Human Services, and Transportation. It also commended the U.S. Agency for International Development and U.S. Equal Employment Opportunity Commission for their continued efforts to meet with federal partners, and private sector, nongovernmental, community, and faith-based stakeholders, to receive feedback on programs, help shape future initiatives, and collaborate on anti-trafficking prevention, protection, and prosecution. ***IAJ***

DoD Releases 2014 Quadrennial Defense Review

Earlier this spring, the Department of Defense (DoD) released its fifth Quadrennial Defense Review (QDR), a congressionally mandated review of DoD strategy and priorities. The 2014 QDR builds on the 2012 Defense Strategic Guidance, and seeks to adapt, reshape, and rebalance the U.S. military.

The QDR prioritizes three strategic pillars: defending the homeland against all threats, building security globally by projecting U.S. influence and deterring aggression, and remaining prepared to win decisively against any adversary should deterrence fail. The review also outlines three broad themes: an updated defense strategy, the rebalance of the joint force, and the department's commitment to protecting the all-volunteer force.

The QDR is intended to set the course for DoD to address current and future conflicts and threats. Throughout the QDR, there are several references to the important role interagency and international partnerships play in DoD efforts and operations, including those in conflict prevention, capacity building, counterterrorism, and countering illicit drug trafficking. ***IAJ***

House Committee Cites Need for Better Information Sharing in Boston Marathon Report

In March, the U.S. House Homeland Security Committee released a bipartisan report detailing the timeline of last year's Boston Marathon terrorist attack. The report, The Road to Boston: Counterterrorism Challenges & Lessons from the Marathon Bombings, provides information on the terrorist networks in the Caucasus and the alleged-bomber Tamerlan Tsarnaev, and makes recommendations for improving counterterrorism efforts in the future.

The report exposes shortcomings in interagency cooperation and information sharing on the Tsarnaev brothers between the FBI, Customs and Border Protection, and other U.S. agencies leading up to the bombings. The report identifies four areas for continued improvement, including improved cooperation between federal and local law enforcement and increased information sharing involving various terror/travel watch lists at the federal level. For example, the report suggests fusion centers operated by state and local law enforcement agencies should by supplied with greater access to the FBI's Guardian System terror database. The report also recommends that agencies provide all the information available to them in their nominations to terror watch lists and other databases. ***IAJ***

Interagency Cooperation Important to Border Security

From March 18 to March 19, law enforcement professionals gathered in Phoenix, Arizona to take part in the Border Security Expo. The Expo included keynote addresses from high ranking representatives from the Department of Homeland Security, U.S. Customs and Border Protection, U.S. Border Patrol, and U.S. Immigration and Customs Enforcement.

The event also comprised a number of panel sessions that covered a variety of border security topics, including managing and securing the U.S.-Mexico border and strategic partnerships for intelligence sharing.

During these panels, speakers credited interagency cooperation and information sharing with recent high-profile arrests. Panelists also stressed the important role interagency cooperation has in securing U.S. borders, even saying that such cooperation should possibly be federally mandated.

The 2015 Border Security Expo will be held on April 21 and 22, and will focus on countering transnational organized crime. ***IAJ***

Army Pamphlet Calls for Interagency Partnerships

Earlier this year, the Department of the Army released a pamphlet on the subject of engagement. U.S. Army Training and Doctrine Command Pamphlet (TP) 525-8-5, The U.S. Army Functional Concept for Engagement expands on the ideas of TP 525-3-0, The U.S. Army Capstone Concept and TP 525-3-1, The U.S. Army Operating Concept.

The pamphlet includes a section on special warfare activities which, among other things, calls for Soldiers to be trained to work with host nation security forces, host nation governments, international government organizations, nongovernmental organizations, and interagency partners. The pamphlet also focuses on the interdependence of the Army and their unified action partners, including joint, interagency, and multinational partners.

The pamphlet incorporates building partner capacity tenets and establishes a common framework to capitalize on the integrative opportunities all of the warfighting functions provide to future land operations. ***IAJ***

CSO Evaluates Two Years of Engagement

Early in March, the State Department's Bureau of Conflict and Stabilization Operations (CSO) published a report detailing CSO's efforts in its first two years of operations. CSO was established in 2011 to improve the effectiveness and coherence of the U.S. government in conflict situations, and break cycles of violence through locally grounded analysis that focuses on a top-priority opportunity to address conflict.

CSO set three goals when it began: 1) make an impact in three or four countries important to the United States; 2) build a respected team of trusted partnerships; and 3) be innovative and agile. These goals would be met by working with other State Department and interagency partners to understand and reduce conflict.

The report details many examples of CSO's success in addressing conflict in four top-priority countries, including CSO's contribution to more peaceful elections in Kenya and Honduras,

and CSO's role in generating defections from the Lord's Resistance Army. The report also cites partnerships with host governments, civil society, NGOs, the U.S. Agency for International Development, the Department of Defense, and other bureaus within the State Department as being beneficial to CSO's mission. ***IAJ***

GAO Assesses State and USAID Contracting

In February 2014 the Government Accountability Office (GAO) released a report assessing the progress made by the Department of State and the U.S. Agency for International Development (USAID) in addressing issues related to the contracting of other entities, including government agencies, in contingency operations.

GAO's report, GAO-14-229, stems from a mandate in Section 850 of the Fiscal Year 2013 National Defense Authorization Act (NDAA) that requires State and USAID to assess their organizational structures, policies, and workforces related to contract support for overseas contingency operations. It also requires GAO to report on the progress State and USAID have made in identifying and implementing improvements related to those areas.

In their Section 850 report to Congress, the State Department cited actions needed to improve acquisition planning, contract oversight, and interagency coordination, but concluded that its organizational structure was generally adequate to support overseas contingency operations. USAID focused their report to Congress on agency-wide policies, identifying room for improvement in contractor performance evaluations and in data collection, inventory, and reporting. However, GAO notes that in focusing on policy, USAID may have missed opportunities to leverage its knowledge and skills to better support future contingencies.

While both State and USAID have made strides to improve their role in contingency operations, GAO recommends that both agencies continue to assess how the suggested and intended changes will effect contingency contracting and each agency's objectives. ***IAJ***

Cybersecurity Framework to Protect U.S. Critical Infrastructure

On February 12, the National Institute of Standards and Technology released the Framework for Improving Critical Infrastructure Cybersecurity. The framework was developed by hundreds of companies, several federal agencies, and many international contributors as a how-to cybersecurity guide for organizations in the business of running the nation's critical infrastructure, which includes facilities that generate and transmit electricity, as well as those that manage telecommunications, drinking and waste water, food production, and public health, among others.

The framework is a key deliverable from President Obama's 2013 Executive Order on Improving Critical Infrastructure Cybersecurity, and is described by the president as "a great example of how the private sector and government can and should work together to meet this shared challenge." The framework provides a roadmap to improving cybersecurity as well as a way to better communicate with chief executives and suppliers about managing cyber risks.

The framework has three components—core, profiles, and tiers. The core is a set of cybersecurity activities and references that are common across critical infrastructure sectors; the profiles can help an organization align its cybersecurity activities with business requirements, risk tolerances and

resources; and the tiers allow an organization to view its approach to and processes for managing cyber risk.

Also, in an effort to boost framework use, the Department of Homeland Security (DHS) has established the Critical Infrastructure Cyber Community, or C3 (C-Cubed), Voluntary Program, a public-private partnership that connects companies and federal, state, local, tribal and territorial partners to DHS and other federal government programs and resources for help managing their cyber risks. ***IAJ***

Joint Publication on Counterinsurgency Reviewed by CSIS

In early February, the Center for Strategic and International Studies (CSIS) released their review of recently updated Joint Publication (JP) 3-24 Counterinsurgency (COIN). JP 3-24 was updated in November 2013 and amends the original JP that was published in 2009.

The review of the updated JP credits the revised COIN manual with addressing some of the issues with the original document, including what were seen as unrealistic and overly ambitious expectations for societal and institutional change. However, the CSIS review also notes five shortcomings to the JP.

According to the review, JP 3-24 overestimates the influence the U.S. has with host-nation leaders and power brokers. The updated JP also overestimates the willingness of U.S. political leaders to insist on whole-of-government coordination and of bureaucratic leaders to give up existing decision-making privileges. Additionally, the JP underplays the importance of actors outside the U.S., and does not recognize that any U.S. COIN strategy should be designed to support the host-nation's strategy. Finally, while the JP acknowledges the need to identify and address the root causes of an insurgency, it underestimates the time and resources required to sustainably address these causes.

The review recognizes that it is unlikely that this JP will be used after U.S. involvement in Afghanistan diminishes at the end of this year. Still, the review suggests expanding civilian capacities for conflict diplomacy, prevention, and mitigation to reduce demand for military intervention, but recognizes that the demand for civilian capacity is usually unmet. ***IAJ***

State, USAID Launch Second QDDR

On April 22, the State Department announced the launch of its second Quadrennial Diplomacy and Development Review (QDDR). Several top representatives from State and the U.S. Agency for International Development (USAID) spoke at the launch, including Secretary of State John Kerry, Deputy Secretary of State Heather Higginbottom, USAID Administrator Rajiv Shah, and Special Representative Tom Perriello.

The QDDR focuses on human rights, democracy, and civilian security, while recognizing the importance of engaging diplomats, development experts, and other stakeholders, including NGOs. The first QDDR was released in December 2010, enumerating the diplomacy and development efforts of State and USAID, and outlining several reforms for the agencies. Some of the reforms suggested in the 2010 QDDR have already been implemented, while others remain underway.

In his remarks at the April launch, Special Representative for the QDDR Tom Perriello said

"I know that diplomacy and development work because I've been blessed to witness it myself. Done right, diplomacy and development can prevent wars, it can reduce extreme poverty, it can transform the rights of girls, and advance transparency over corruption."

Secretary of State John Kerry also shared his hopes for the future of diplomacy and development, saying "I want to see us advance diplomacy and advance development." He continued, explaining the importance of the QDDR. "[The QDDR is] also a preview of what State and USAID need to do in order to put the United States of America in the strongest position to face the challenges and seize the opportunities of tomorrow."

The review will take place over the course of a few months. ***IAJ***

Research Suggests Use of DoD-Developed Technology along U.S. Border

Earlier this year, the RAND Corporation completed research into whether or not the Department of Homeland Security (DHS) and the Drug Enforcement Administration (DEA) could use intelligence, surveillance, and reconnaissance technologies developed by the Depart of Defense (DoD) to help secure the U.S. southern border.

RAND's report, which was published in May, focused on the legality of DHS and DEA using DoD-funded technology. The new sensor technologies were created to support military forces operating in Iraq and Afghanistan, and were tested along the U.S. southern border because the field conditions along the border closely resemble those in current military theaters of operation. The technology demonstrations would also reveal if the new technologies would be useful in domestic law enforcement led counterdrug operations along the U.S. border.

This report explores the legality of these technology demonstrations, and whether the DoD sensors can legally be used in domestic counterdrug operations when operated by U.S. military forces. The researchers examined federal law and DoD policy, and found that parts of U.S. law mandate information sharing among federal departments and agencies for national security purposes and direct the DoD to play a key role in domestic counterdrug operations in support of U.S. law enforcement agencies. However, other parts of the law place restrictions on when the U.S. military may participate in law enforcement operations.

After reviewing relevant federal law and DoD policy, the authors concluded that there is no legal reason why a DoD sensor should be excluded from use in an interagency technology demonstration or in an actual counterdrug operation as long as a valid request for support is made by an appropriate law enforcement official. The authors recommend DoD policy on domestic counterdrug operations be formally clarified and that an approval process should be established for technology demonstrations with a counterdrug nexus. ***IAJ***

Report Praises Current Measures in U.S. Biological Defense

In a May report, the U.S. Government Accountability Office (GAO) released a report assessing the U.S. government's preparedness for biological threat agents, including biological weapons. GAO-14-442 is the result of a mandate to review the Department of Defense's efforts to research and develop medical countermeasures against prioritized biological threat agents.

Included in the report are evaluations of DoD's progress in researching, developing, and making available medical countermeasures against biological threat agents. The report also describes DoD's internal coordination to allocate resources to medical countermeasures against biological threat agents, and evaluates DoD's coordination with the Departments of Health and Human Services (HHS) and Homeland Security (DHS) to research and develop medical countermeasures against biological threat agents.

During their evaluation, GAO found that DoD's coordination with HHS and DHS align with the best practices to facilitate collaboration across agency boundaries. GAO also determined that the joint research campus shared by DoD, HHS, and DHS – the National Interagency Biodefense Campus at Fort Detrick, Maryland – has a governance structure that allows the agencies to leverage available resources and facilitate scientific exchange. There are also interagency agreements and established processes that aid in communication between the agencies and help identify threats and risks.

While conducting their review, GAO found that DoD does not use its established process for annually updating its list of threat priorities, and suggested that DoD implement a process to update its list of biological threats according to its current policies. DoD concurred and identified steps to address the recommendation. ***IAJ***

Simons Center Announces Third Annual Open Interagency Writing Competition

The Simons Center for Interagency Cooperation announces its third annual open Interagency Writing Competition for 2014. The competition is open to the public and recognizes papers that provide insight and fresh thinking in advancing the knowledge, understanding, and practice of interagency coordination, cooperation, and collaboration at the tactical or operational level of effort. The competition opens May 1. Deadline for submissions is Friday, Aug. 8, 2014.

Entries must be focused on this topic:

Interagency Imperative for Homeland Defense and Security: Challenges and Solutions

How to enter:

- Submit an unclassified, original paper examining any aspect – broad or specific – of the topic. Papers should be between 4,000 and 8,000 words in length.
- Previously published papers, papers pending consideration elsewhere for publication, or papers submitted to other competitions still pending announced decisions are ineligible.
- Manuscripts should be single spaced in Microsoft Word format using Times, 12-point type. All graphs, charts, and tables should be submitted as separate files in the format they were created.
- Along with their manuscript, writers must agree to the Simons Center copyright transfer agreement, which is detailed online at www.thesimonscenter.org/competition.
- Manuscripts can be submitted on the Simons Center website at www.thesimonscenter.org/contribute-content or emailed to editor@thesimonscenter.org with the subject line "Interagency Writing Competition" by Aug. 8, 2014.

A panel of Simons Center judges will evaluate entries on originality, substance of argument, style and contribution to advancing the understanding and practice of interagency cooperation at the operational and tactical levels of effort.

The first place entry will receive $1,500, an engraved plaque, a certificate of recognition and publication in one of the Simons Center publications series. Second place will receive a $1,000 award, a certificate of recognition and consideration for publication. Third place receives $500, a certificate and also consideration for publication by the Simons Center.

For more information contact the Simons Center at editor@thesimonscenter.org or call 913-682-7244. ***IAJ***

Book Review

Cybersecurity and Cyberwar: What Everyone Needs to Know

by P.W. Singer and Allan Friedman

Oxford University Press, New York, New York, 2014, 320 pages

Reviewed by Lt. Col. Andrew K. Murray
- U.S. Army Command and General Staff College

One could immediately empathize with P.W. Singer and Allan Friedman's challenge of encapsulating "what everyone needs to know" about cyber security/cyber war into one book. To begin with, it is impossible to categorize "everyone." Despite the title, we projectively ascertain the book appeals to a specific market niche of professionals who are novices in the technical aspects of cyberspace, dilettantes in the analogous understanding of the cyber phenomenon, but Subject Matter Experts (SME) in their particular field.

The authors unambiguously open the book with their stated purpose. They speak of a vast knowledge gap, especially egregious among many policy makers in the cyberspace field. If policy makers are the tip of the pyramid, SMEs mentioned in the first paragraph most likely form the base of the intended audience. The book, in and of itself, is neither a placebo, nor a panacea to remedy this knowledge gap. It serves as a satisfactory commencement though, toward understanding the cyberspace phenomenon.

The authors tacitly imply that a foundational knowledge of the internet (what is it and how it works) is a prerequisite for launching into the more strategic and analogous aspects of cyber security/cyber war. This brings into question, how much foundational/technical knowledge is too much (or too little) for the intended readers? They gloss over some key foundational technical aspects of the internet such as packet switching and layered architecture. A methodology for addressing these key technical/foundational topics could be a "top-down" approach starting with the network edge; moving to the network core; addressing protocol layers beginning with the application layer; and finally working toward the physical layer.[1] The authors compensated for any dearth of technical foundation by addressing the salient question of what is cyberspace? The definitional disquisition is a practical segue into the history of the internet, which in turn, is an effective transition into evolving internet governance. The history and governance portion was captivating in and of itself but could have been rendered so much more pedagogically ergonomic if the authors had proceeded in sequential order. A timeline of key events would have been a coup. For example, an effective method could be the explanatory sentences and paragraphs culminating in a key events timeline.

With the technical and foundational aspects covered, the authors moved into the contemporary

intriguing aspects of cyberspace to include cyber attacks, hactivism, anonymous, spying, stuxnet and cyber terrorism. They delve into a rather enlightening (for the general public), "focused study" on the U.S. cyber force structure detailing the structure and mission of Cyber Command (CYBERCOM) and their symbiotic relationship with the National Security Agency (NSA). Beyond a few misinterpretations of the unique military parlance (double hatted versus dual hatted), Mr. Singer and Mr. Friedman did a fairly good job of representing the mission, organization, structure and parameters of our U.S. cyber forces! The next focus study covered the Chinese approach to cyber warfare. The organizational diagrams of suspected Chinese cyber units were validated against our Foreign Military Studies Office (FMSO) and were not found wanting. A missed opportunity for the authors is addressing the Chinese concept of campaign stratagems. China has creatively fused high-technology and stratagems in order to execute operational high-tech stratagem applications.[2] Possibly this could be addressed in a second publication? One can appreciate the author's elucidation, reference the pessimistic interpretation of the covariance between U.S. and Chinese cyber power (with the internet serving as the dependent variable, in this case). Singer and Friedman verily contend that China is not utterly besting us in the cyber domain. In doing so, they allay fears that we need to learn Mandarin. They skillfully illuminate the fact that, for one, the U.S. invented the internet and it is still under some form of U.S. governance or commercial dominance. Secondly, our overall economy and research/development is far ahead of China's. What Singer and Friedman do not wrestle with is the concept of our ingrained avant-garde nature, propelling innovation and keeping the U.S. on the leading-edge of cyber technological development.

The final part of the book is well suited for the military culture and mindset. In the first part of the book, they laid a foundational base, the second part of the book he expounded on the rueful problems associated with the cyber phenomenon including crime, terrorism and foreign relations. In the last phase of the book, they offer solutions, under the auspice of "what can we do?" They astutely propose we challenge the underlying basis of our analogies and metaphors.[3] Singer and Friedman challenge us to reframe the problem, move away from the cold war analogies and evaluate alternative models to deal with cyber challenges. They equate malware more to a communicable disease and consider the public health model. They also suggest a maritime piracy comparison and analogy. They prod law makers into greater action by suggesting meaningful legislation i.e. disclosure laws. They contend a codified system of cyber security incentives would prove useful. Importantly, they focus on personal actions and individual responsibility.

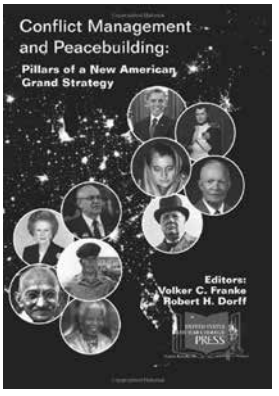
In conclusion, *Cybersecurity and Cyberwar* nourishes the intellectual desire to understand the world in which we live. It is valuable to both the policy maker and the practitioner. It has the potential to promote a common understanding in the realm of inter-agency cooperation between various governmental, as well as commercial entities. It is worth the read. ***IAJ***

Notes

1 Jim Kurose and Keith Ross, "Computer Networking: A Top-Down Approach," 2013, Pearson Education Inc., Addison-Wesley, New Jersey.

2 Timothy L. Thomas, "The Dragon's Quantum Leap: Transforming from a Mechanized to an Information Force," Foreign Military Studies Office (FMSO), Fort Leavenworth, Kansas.

3 Dr. Richard Paul and Dr. Linda Elder, "Fallacies …", The Foundation for Critical Thinking, Dillon Beach, California.



Conflict Management and Peacebuilding: Pillars of a New American Grand Strategy

Edited by Volker C. Franke and Robert H. Dorff

Strategic Studies Institute & U.S. Army War College, October 2013, 420 pages

Reviewed by Major General (Ret.) Michael G. Smith, Australian Army
- Founding Director, Australian Civil-Military Centre

Conflict Management and Peacebuilding: Pillars of a New American Grand Strategy provides an important contribution to understanding the civil-military complexities in responding to, stabilizing, and building sustainable peace and prosperity in conflict and post-conflict environments. The central issues addressed in this volume include the strengths and limits of American military force and diplomatic prowess; the intrinsic melding of soft and hard power ("smart power"); the importance of multinational collaboration; the need for a more comprehensive "whole of government" approach; and the cultural differences within and between American, allied, and host-country state and non-state actors.

Conflict Management is a lengthy read, comprising 14 chapters and 410 pages. The volume could hardly be shorter, however, as it is a compilation of essays from an excellent symposium of a similar title held on February 24, 2012, at Kennesaw State University and the Strategic Studies Institute. In the opening chapter, the editors provide a useful summary of each of the subsequent chapters, but for serious practitioners and theorists alike this summary belies the richness of each of the chapters that follow. The editors advise that the symposium and book reveal a "broad range of viewpoints, a number of overarching themes and tentative agreements", but it is left to the reader to distill these. A concluding chapter that attempted to do this would have been a useful addition to the volume, and helpful for strategic thinkers and planners in determining what the editors call "the future of U.S. grand strategy in an age of austerity".

Most of the volume addresses U.S. perspectives on contemporary peacebuilding and conflict management, but there are also useful European and African perspectives, including on the effectiveness of U.S. approaches in these areas. Given the rise of China and the Obama administration's declaratory intention to pivot more to the Asia-Pacific, the volume, surprisingly, gives little attention to this dynamic in shaping future U.S. grand strategy. An excellent chapter by Liselotte Odgaard partially addresses this by providing a comparison between America's "integrationist" approach and China's practice of "coexistence". Managing this dilemma may well prove to be central to global security in the 21st century, particularly given Odgaard's assertion that "the United States is a great power in decline, with estimates of U.S. GDP at only two-thirds of China's GDP in 2050".

Moving away from more conventional state-centric power politics, several chapters highlight the growing importance of "human security" in shaping America's new grand strategy. These authors advocate for the U.S. to address human security more coherently in both policy and practice. This theme emerges in different ways by different authors, including the two chapters providing African

perspectives, the first by Kwesi Aning and Festus Aubyn, and the second by Abel Esterhuyse. This theme is also included in the chapter on civil-military coordination by Christopher Holshek, the chapter on peacebuilding and development from an NGO perspective by Fouzieh Melanie Alamir, and in Michael Ashkenazi's chapter that calls for a bottom-up approach to address the chronic problems of "individuals and small groups".

In his informative chapter on "smart power", Robert Kennedy contends that "… the greatest challenge for the United States will arise from a continued relative shift in power from the world's predominant political, economic, diplomatic, and military superpower to *primus inter pares* in world affairs". The chapter by Michael Lekson and Nathaniel Wilson supports this view, suggesting that states will remain the main actors in shaping major international security activities and outcomes. Unlike other authors who tend to conflate peacebuilding and conflict management, however, Lekson and Wilson draw a clear distinction and contend that the scarcity of U.S. resources will demand greater priority on conflict management and less on peacebuilding as a pillar of U.S. grand strategy, although they acknowledge that peacebuilding will remain prevalent in international security. Noting the limitations of successive U.S. national security policies, they assert that: "A grand strategy needs to be developed to deal with the future, and not to provide tactical prescriptions for the present".

The decline and limits of U.S. power in relative terms and the return to a more multipolar world is a theme repeated in a number of other chapters. Frederick Smullen contends in his chapter that threats are more global, unpredictable, and persistent than in previous eras and calls for greater U.S. leadership through more rigorous strategic planning to stabilize the current world order—in his words, "America needs to stand out as a beacon of what is right in and for the world." Karl-Theodor zu Guttenberg, the former German Defense and Economics Minister, calls for a new and long-term visionary strategy to strengthen the transatlantic relationship "by promoting a global democratic political culture based on respect for cultural differences".

One of the book's strengths is its focus on practical strategies that could be adopted by the United States to enhance peacebuilding and conflict management. In addition to Guttenberg's call to strengthen transatlantic culture, a number of authors emphasize the need for improved "cultural understanding" of host populations, noting the limitations of imposing American values, particularly when military and civilian deployments provide limited time and opportunity in-country to gain the trust of local populations, underpinned by an appreciation of historical and cultural factors. The fore-mentioned chapters by Alamir, Ashkenazi, Aning and Aubyn, and Esterhuyse all emphasize the importance of greater cultural understanding by the United States. Focusing on the U.S. military contribution to peacebuilding, William Flavin reminds us that successful peacebuilding must reflect true national ownership and address local priorities. Simply put, peacebuilding cannot be imposed effectively by outsiders, and particularly by occupying foreign military forces. In his chapter, Charles Dunlap espouses the importance of "free enterprise and liberal democracy" in building national resilience and international security. To help achieve this, Dunlap advocates that the U.S. should adopt an "off shore" approach based on a light military footprint, claiming that "The efforts to reorient entire societies in Iraq and Afghanistan via a strategy that was manpower-intensive and ground centric has proven to be flawed." Clearly, not everyone would agree with Dunlap's analysis or interpret his off shore option as a viable grand strategy, although his approach would seem to have merit in specific circumstances.

Dwight Raymond's unique chapter on Mass Atrocity Prevention and Response Options

(MAPRO) may have particular relevance for the charting of a new grand strategy for the United States (and other countries). The responsibility to protect civilians is now a core issue for the United Nations and its member states. MAPRO provides useful guidance on how to prevent and respond to these circumstances, both strengthening America's commitment to human rights and international law and requiring the development of new doctrine and training for civilian and military actors. The early introduction of these concepts in new and transforming states could assist in enhancing the prospects for a local peace as well as developing international norms. The international community's current inability to deal with the tragedy in Syria suggests that an alternative MAPRO approach warrants greater attention, although Raymond does not specifically advocate this course of action.

Conflict Management and Peacebuilding: Pillars of a New American Grand Strategy is an important read for scholars and practitioners concerned with the development of America's national security policies. The chapters are rich in facts and ideas, and individual readers will highlight different priorities. In an age of austerity and increasing strategic uncertainty, however, the book does not provide a blueprint or a list of priorities for America's future grand strategy. There is plenty of evidence that the United States should develop a grand strategy that is more joined-up, comprehensive, whole-of-government, and multilateral. A stronger emphasis on enhancing civil-military coordination seems necessary and sensible. Despite this overwhelming evidence, however, it is yet to be seen in the age of austerity if major U.S. security organs will embrace this collective opportunity or retreat to the comfort of their traditional fiefdoms, claiming "core business" as their essential *raison d'etre*. ***IAJ***

The Simons Center
P.O. Box 3429
Fort Leavenworth, Kansas 66027
ph: 913-682-7244
www.TheSimonsCenter.org
facebook.com/TheSimonsCenter

CGSC Foundation, Inc.
100 Stimson Avenue, Suite 1149
Fort Leavenworth, Kansas 66027
ph: 913-651-0624
www.cgscfoundation.org
facebook.com/CGSCFoundation
LinkedIn.com >>CGSC Foundation, Inc.