NATIONAL DEFENSE RESEARCH INSTITUTE

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Purchase this document
Browse Books & Publications
Make a charitable contribution

For More Information

Visit RAND at www.rand.org
Explore the RAND National Defense Research Institute
View document details

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND PDFs to a non-RAND Web site is prohibited. RAND PDFs are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see RAND Permissions.

This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

Analytic Support to Intelligence in Counterinsurgencies

Walter L. Perry, John Gordon IV

Prepared for the Office of the Secretary of Defense

Approved for public release; distribution unlimited

NATIONAL DEFENSE RESEARCH INSTITUTE

The research described in this report was sponsored by the Office of the Secretary of Defense (OSD) and conducted within the International Security and Defense Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the OSD, the Joint Staff, the Unified Combatant Commands, the Department of the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community under Contract W74V8H-06-C-0002.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN 978-0-8330-4456-3

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

Cover photo by U.S. Air Force Technical Sergeant John M. Foster; courtesy of the Department of Defense

© Copyright 2008 RAND Corporation

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from RAND.

Published 2008 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

Insurgency is one of the oldest forms of conflict. Records of ancient regimes show how their rulers were frequently faced with revolts and insurrection. The reality that insurgency is a continual problem has persisted into the modern era. The United States Army spent decades conducting what was, essentially, a counterinsurgency in the American West during the period after the Civil War; the British Army was faced with multiple insurgencies during the period of Empire in the nineteenth and early twentieth centuries; and as the colonial era came to an end in the post–World War II period, the Western militaries—especially their armies—continued to face this challenge. Today, the problem of combating insurgencies continues to loom large for the armed forces of several western nations.

Yet despite this, the preference of most Western militaries has been to focus on conventional combat operations against the armed forces of another nation state. This is reflected in the spending patterns of the NATO nations today. Compared with the money devoted to new systems for high-intensity combat, the amount invested in the preparation for irregular warfare pales. Of course, quality does not equal quantity, and a strict resource metric does not necessarily gauge emphasis. However, when we couple the money spent with the relative ability of nations to conduct conventional and counterinsurgency operations, it is clear that the emphasis is on conventional forces.

What is the reality that faces the Western militaries today? Iraq provides a useful example. Whereas the major combat operations phase in Iraq lasted some 23 days (from the time U.S. and UK forces crossed

the border from Kuwait into Iraq to the last major battle in Baghdad on April 10, 2003) the counterinsurgency period has lasted some 1,700 days as of this writing. This is consistent with the norm of post-World War II insurgencies.

Although Iraq and Afghanistan will probably reduce the appetite of Western nations to engage in similar events without vigorous domestic debate, a strong case can be made that the Western militaries simply cannot turn their back on the study of and preparation for counterinsurgency in a manner similar to the way the conventional U.S. military turned its back on the study of low-intensity operations in the aftermath of the unfortunate experience in Vietnam. A major part of enhancing our ability to conduct counterinsurgency is improving our ability to analyze how insurgencies get started, the different nature of each individual insurgency, and the actions required by the security forces that are attempting to counter the movement.

This monograph examines the nature of the contemporary insurgent threat and provides insights on the need for better analysis of insurgency. It focuses on the security portion of a counterinsurgency effort. Other elements of counterinsurgency, such as efforts to improve governance in countries threatened by insurgency, are also critically important. However, those nonsecurity portions of counterinsurgency are beyond the scope of this analysis.

The Nature of Modern Insurgency

Today, theorists and doctrine writers, those in charge of training and equipment purchases, and the political leaders of the nations faced with insurgencies and other nations considering coming to their assistance must all consider the nature of modern insurgency. This is a profoundly important issue, since how nations view *insurgencies* will have significant influence on how their militaries and governments prepare for future *counterinsurgency* missions.

There is considerable discussion today about "what has changed." Does the modern, interconnected, networked, cable-television world obviate the lessons from past counterinsurgency campaigns? Or is the

nature of insurgency so enduring as to render the recent phenomena of *jihad* just another chapter in what is a rather consistent story of how insurgencies develop and how they are countered? The reality is that there are important elements of truth in both views.

Whereas, in some respects, insurgencies have become slicker, quicker, and enabled by modern information technology, many of the principles of counterinsurgency operations remain fundamentally the same. This reality should strongly influence how today's Western militaries prepare themselves for the challenge. In all of this, we see the need for sound analysis in order to determine what capabilities and what mixture of new and old techniques are most appropriate for a particular insurgency.

Most insurgencies evolve over time. While occasionally an insurgency suddenly springs forth in a matter of months (this is essentially what happened in Iraq), in most cases insurgencies gradually gather strength—assuming they survive their initial, weak, proto-insurgency phase. In this early phase, the most effective government counters to the insurgents are generally intelligence services and the police. There may be little, if any, role for the military at this point.

If an insurgency survives past this initial stage, it can evolve into a small-scale insurgency. Now the insurgents start to make their presence felt with more-open propagandizing and occasional attacks against government forces and facilities. While the police and intelligence agencies remain in the lead to combat the insurgents, at this point there may be a need to involve the military in the effort, since the police may need help in some areas.

Should the rebels continue to grow in numbers and capability, it could become a large-scale insurgency. At this point, major portions of the country could be under insurgent control and a large portion of the population will have sided with the rebels. If the problem has reached such proportions, the insurgents stand a good chance of prevailing. On the government side, the military has by now probably taken the lead, since the insurgency is so strong that it is now beyond the ability of the police to control.

The Dominance of Intelligence

Although there are some similarities, the role of intelligence in conventional combat operations differs considerably from its role in support of irregular warfare, including insurgencies. Because the enemy in an insurgency is elusive, unknown, and most likely indistinguishable from the general population, intelligence operations are crucial.

Intelligence Operations in Support of Conventional Combat

In conventional combat operations, the intelligence mission is primarily to respond to the requirements imposed by the campaign plan—in essence, military intelligence. In this case, intelligence tends to support operations. Commanders decide what objectives they will seek to attain, and intelligence supports both the decisionmaking process and additional information needed to support the selected course of action.

Analysis in support of conventional operations is generally well understood. For example, operational analysis can help commanders sift through the intelligence data by systematically applying systems analysis techniques to the process of selecting the best course of action.

Intelligence in Support of Counterinsurgencies

Insurgent groups rarely resemble conventional force formations until they have wrested control of large amounts of territory from the government. They are usually made up of clandestine groups operating in the shadow world, disrupting activities of the government in ways that resemble criminal gangs. Little, if anything, is generally known about their order of battle, equipment, strategic goals, or tactics. In fact, their disruptive behavior can resemble the activities of ordinary criminals.

Successful intelligence operations in support of counterinsurgencies therefore resemble those of law enforcement agencies. Operations against these insurgent cells must depend upon the development of intelligence aimed at identifying cell members and their location. Insurgent command structures are also likely to be unconventional,

and much effort must be expended on understanding the relationships among the members of the various groups involved in the insurgency.

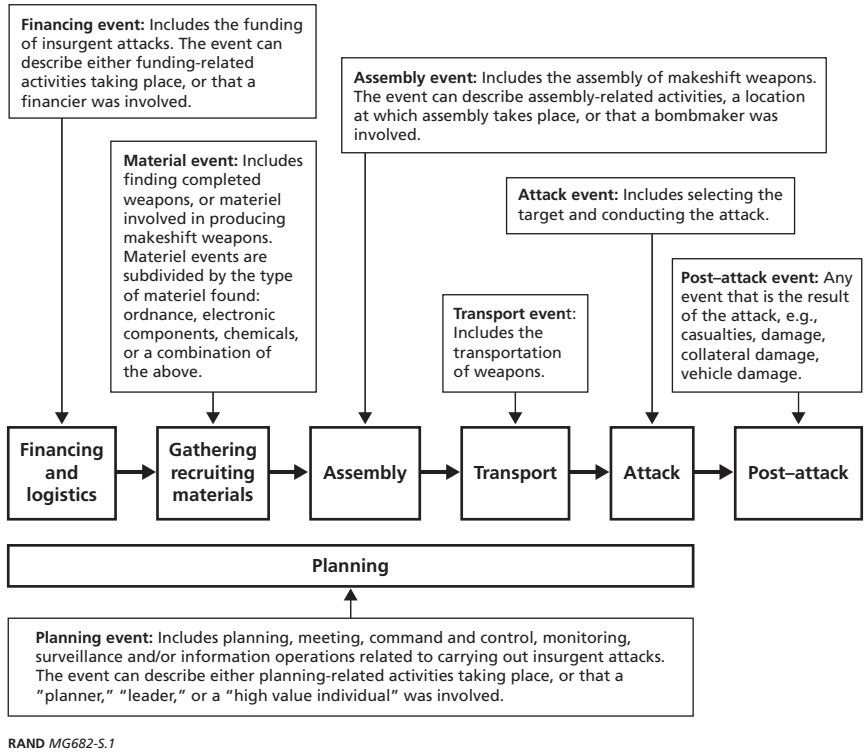
Insurgents generally conduct acts of violence against the established government. Assassinations, bombings, kidnappings, and other forms of violence are common. Seemingly random acts against innocent civilians are conducted by insurgent gangs to intimidate and underscore the government's inability to protect the population. In investigating these incidents, considerable emphasis is placed on crime scene analysis, social network analyses, interrogation of detainees, forensics and biometrics. Military intelligence begins to resemble police intelligence.

Analysis in support of these police-like operations is likely to be considerably different than analysis to support conventional military operations. In supporting counterinsurgency operations, we need to apply existing, and perhaps new, analytic techniques to answer such questions as the following: Who are the insurgents? What are their objectives? Where will they strike next? How are they organized? Notice that answers to most of these questions are already known in conventional military operations. The law enforcement community often employs pattern analysis techniques, such as geographic profiling, to understand past criminal behavior and to predict where criminals are likely to strike next. This is something we explore here as well.

The Analytic Questions

Analysis in support of counterinsurgencies (indeed, in support of most unconventional wars) centers on contributing to intelligence production by focusing on required information elements. Because this is a unifying theme, we refer to analytic support in these cases as *intelligence analysis*. It is therefore important that we fully understand the anatomy of insurgent attacks. Figure S.1 depicts a typical sequence, from financing operations to conducting the attack. At each event in the chain, the insurgents are vulnerable to government detection and attack, but to varying degrees.

Figure S.1
The Insurgent Attack Event Chain



RAND *MG682-S.1*

The analytic questions at each stage in an insurgency therefore center on understanding what is needed to interrupt insurgent attacks at each point in the event chain. Some of these questions are the following:

- **Signs of a Nascent Insurgency.** What is the typical signature of a nascent insurgency—in terms of actions, pronouncements, and so on?
- **Leadership and Membership.** Who are the leaders and principal deputies of each insurgent group? Where are they located? What is the relation among the group members and between groups?

- Insurgent Goals. Are the insurgents striving to overthrow the existing government or to gain autonomy for a region? How can the government take advantage of each goal?
- **The Nature of Insurgent Attacks.** Where are the weapons caches used by the insurgents? Where are the next attacks likely to occur? What is the nature of the attack "event chain"? What foreign entities (governments or groups) are assisting in the attacks in some way?
- **Intelligence Sources.** How can we best leverage information obtained from detainees? How can we use forensic and biometric evidence to locate insurgents?
- **Financing and Recruitment.** Who is financing the insurgency? How are the insurgent groups recruiting members? What part of the population is susceptible to recruitment? What are the inducements to join?
- **Weapons.** What types of weapons are being used? Where do they come from? Where are they cached? Where are the assembly facilities for makeshift weapons? How are weapons delivered to attackers? Which groups are conducting the attacks?
- **Friendly-Enemy Interactions.** What operational patterns are friendly forces exhibiting? How is this behavior being exploited by the enemy? How can a friendly force alter its behavior to make its patterns more difficult to discern? If its patterns are discerned, how can a friendly force make it more difficult for the enemy to exploit?

For the United States and other friendly nations to come to the aid of a neighbor threatened by insurgents, it is important to answer these questions. To do so, we turn to intelligence analysis using some of the traditional tools of operational analysis and adding a few new tools.

In the process of applying these techniques, it is important to keep in mind two distinguishing characteristics of insurgencies: (1) When carrying out operations, insurgents are likely to subordinate global objectives to local objectives, and (2) any attempts by the friendly

forces to counter insurgent attacks are generally met with counters to the counters—that is, insurgents are adaptive.

Analysis

The analytic tools needed to answer the research questions will be a mix of existing methods of analysis, some new approaches and perhaps different ways to apply existing methods. We suggest several analytic techniques based on our experience supporting operations in Iraq and Afghanistan. Not all have proven successful, but in some cases that may be because they have not yet been applied.

All analysis depends on data, and analytic support to counterinsurgency operations is no exception. The major source of information on enemy activities is generally a report that records "significant" activities. A significant activity can be any incident deemed important. For example, locating a weapons cache is a significant activity as is an enemy attack on a friendly convoy. In many cases, the most important pieces of information are recorded in narrative remarks sections—and not in the more structured data entries. Reports therefore are dependent upon the diligence of the individual soldier preparing the entry. In addition, there are other issues relevant to the usefulness of the data.

- **Data Collection.** Most data are collected to support operations—not to inform analysis.
- **Unevenness in Reporting.** Which incidents are considered "significant" can vary with the experience of the reporting unit.
- **Multiple Databases.** In Iraq and, to some degree, Afghanistan, the several databases are not linked or cross-referenced. Many are stored locally and not easily accessed.
- **Lack of a Standard Lexicon.** A critical requirement for database searches is that the terms used be consistent. Unfortunately, only recently have standard definitions begun to be applied to data entries in Iraq.

- **Friendly Data Generally Not Captured.** Most of the data collected in Iraq and Afghanistan are associated with enemy activities—little information is recorded about friendly operations.
- **Sharing Intelligence Data Among Agencies.** All too often, bureaucratic procedures inhibit or prohibit the sharing of information—much of which may be time-sensitive—between the organizations that are attempting to deal with the insurgency. Sharing intelligence information among allied nations is also difficult. This is particularly problematic for analysis.

Finally, we address some of the techniques that appear to show some promise of being useful to intelligence analysis in support of counterinsurgencies.

- **Discerning Patterns.** Some of the research questions can be answered only in terms of what we refer to as indicators—that is, what friendly units should look for when searching for enemy activity. The most frequently used methods to develop indicators are pattern classification methods, hierarchical decision trees, and linear discriminant analysis. All these methods examine factors associated with the occurrence of an event and then examine evidence in the form of training vectors to narrow the factors to a few strong indicators.
- **Predictive Analyses.** Predictive analyses aim at forecasting where (and sometimes when) the enemy will strike next. In the absence of data on friendly behavior, these techniques invariably depend upon statistical analysis of past insurgent behavior under the assumption that the past is prologue. The predictions therefore are based solely on what the enemy forces have done in the past—not on any interaction between friendly and enemy forces. Most assume an underlying randomness associated with enemy behavior. Although several of these predictive methods exist, very few are currently being used in Iraq or Afghanistan. Local commanders therefore resort to heuristic methods that rely on the location and timing of past insurgent attacks plotted on maps. To be effective (and accepted by commanders in the field), predictive meth-

ods should (1) recognize that insurgent attacks are not random, (2) provide a mechanism for grouping historical events, (3) account for an adapting enemy, (4) benefit from input from local commands, (5) recognize that analysis is local, like the insurgency, and (6) be better than what the command is presently using.

- **Analyzing Insurgent Networks.** Much of what commanders face across all phases of an insurgency consists of clandestine groups of loosely connected individuals carrying out criminal acts against the government and the friendly forces supporting it. In Iraq, commanders at all levels devote considerable time understanding the relationships among key people in the cities, towns, and villages within their areas of operation. For insurgents to successfully carry out the activities depicted in Figure S.1, they must be in contact through some form of network. Understanding the structure of these networks is therefore a primary goal of counterinsurgency operations. A possible solution is the development of an intelligence-based common picture of the insurgent networks that (1) uses the most current intelligence estimates, (2) is automated so as to provide access to multiple commands, and (3) can be easily updated.
- **Friendly-Enemy Interactions.** In general, friendly forces are attacked because they are exposed in some way. In an insurgency, unlike in conventional combat, there are no "lines of contact" behind which friendly forces are secure. Typically, friendly forces create safe enclaves from which to mount operations. Once out of the enclave, friendly forces are exposed and therefore vulnerable to enemy attack. Because friendly forces cannot hide their activities, the enemy is free to attack—provided it has the resources and sufficient time to plan. We explore two closely connected methods to examine the research question associated with friendly-enemy interactions: game theory and change detection.
- **Enemy-Friendly Interaction Analyses: A Game Theory Approach.** One advantage of using game theory is that the mental process involved in determining the payoffs forces us to assess enemy objectives: a favorable payoff to the enemy (Red) implies that it has achieved some part of its objectives. In a counterinsurgency,

friendly forces (Blue) make many decisions when planning and executing missions. They choose routes, times, travel speeds, and so forth. The set of Blue strategies corresponds to the set of possible realizations of these choices. Insurgent elements (Red) make their own decisions about attacking Blue. In general, the success of a Blue mission and the outcome of a Red attack depend on how well-matched Red's strategy is to Blue's strategy. Red must attack when and where Blue will travel, and may need to adjust its tactics in a way that is tuned to the given Blue mission. We assume that the outcome of the game for Red can be measured in terms of the expected payoff to be derived from the consequences of Red propaganda, friendly casualties, etc. Crucially, the analysis does not depend on actually measuring the payoffs. One approach is to examine relative payoffs. For example, Red may conclude that it has achieved its objective better with more Blue casualties than with fewer. The assumption is merely that the payoffs could be evaluated on some ordinal scale.

- **Enemy-Friendly Interaction Analysis: Response Detection.** A study currently being led by the Center for Naval Analyses (CNA) examines a unit's historical movement patterns using archived Blue Force Tracker (BFT) data.[1] This is generally a graphical process whereby BFT data are plotted on a map of the unit's area of operation—outside its forward operating base. This is repeated for a subsequent time period of equal length, and the difference is calculated. In areas where significant change is observed, the analysis focuses on enemy activity to see how the enemy has exploited (responded to) the change in friendly behavior. Next, area density changes are computed within grids overlaid on the area of operations, and along road segments within those grids if more resolution is needed. An important aspect of this type of analysis is the development of suitable measures and metrics that reflect the level of Red-Blue interaction from one time period to the next. For the friendly forces, operational density is appropriate, i.e., the

[1] The work presented here summarizes research conducted by Dr. Caryl Catarious, a research analyst at CNA.

levels of Blue force activity per unit area or per unit kilometer. For Red, the metrics are simply the activity of interest for the analysis being conducted: the number of friendly-force casualties per time period, the number of attacks of specific types or all types per time period, the number of weapons caches found and cleared per time period, and so forth. The goal of the response detection analysis is to focus on areas where (1) a significant change in Blue force activity has been observed, and (2) insurgents have either successfully taken advantage of the change or have failed to do so.

Conclusion

Our goal in this monograph has been to examine how operational analysis can be used to support the security portion of counterinsurgency operations. Insurgencies evolve over time. Normally starting as a small, clandestine movement of "true believers," insurgent movements are usually very weak and vulnerable in their early stages. If the movement survives and begins to grow, it can become a large-scale insurgency that has a reasonable chance of succeeding.

Our understanding of modern insurgency is evolving and improving. In some respects, the lessons and techniques used in past counterinsurgency efforts remain valid today. In other areas, important changes have taken place, especially in the ability of insurgents to use modern global information and communications networks to recruit, spread propaganda, organize, and control their operations.

As analysts engaged in trying to understand and assess modern insurgencies, we must realize that this is a different form of conflict from what we grew accustomed to during the Cold War and the 1990s, when most of us focused on the interaction of conventional military forces. Instead of merely conducting operational analysis, we are really engaged in using operational analysis techniques to support intelligence operations.