

University of South Florida

From the Selected Works of Randy Borum

2004

The Role of Operational Research in Counterterrorism

Randy Borum, *University of South Florida*

Robert Fein

Bryan Vossekuil

Michael Gelles

Scott Shumate



Available at: https://works.bepress.com/randy_borum/8/

RANDY BORUM, ROBERT FEIN, BRYAN VOSSEKUIL,
MICHAEL GELLES, and SCOTT SHUMATE

The Role of Operational Research in Counterterrorism

In the post 11 September 2001 security environment, federal, state, and local law enforcement personnel in the United States are asked regularly to maintain a state of “heightened alert.”¹ Intelligence professionals have also been mobilized to increase data collection and information-sharing efforts to prevent terrorist attacks against U.S. interests.^{2,3,4} But understanding the threat of the “new terrorism” and its implications for investigation and

Dr. Randy Borum, an Associate Professor in the Department of Mental Health Law and Policy at the University of South Florida, Tampa, also serves as an instructor with the State and Local Antiterrorism Training (SLATT) program, and is a consultant to federal law enforcement agencies and the United States Intelligence Community.

Dr. Robert Fein, a founder and director of the National Violence Prevention and Study Center, currently serves on the Director of Central Intelligence’s Intelligence Science Board, and works with the U.S. Department of Defense Counterintelligence Field Activity (CIFA) in conducting operational studies of preattack terrorist behaviors with the DoD Criminal Investigative Task Force (CITF), as part of its Behavioral Sciences Consultation Team.

Bryan Vossekuil, a founder and director of the National Violence Prevention and Study Center, is a retired special agent in the U.S. Secret Service. He is currently a consultant to the Department of Defense’s CIFA and CITF operations.

Dr. Michael Gelles, Chief Psychologist at the Naval Investigative Service, serves as the Lead Psychologist of the CITF’s Behavioral Science Consultation Teams.

Dr. R. Scott Shumate, Director of Behavioral Sciences at CIFA, previously served in the Intelligence Community, and has interviewed numerous known and suspected foreign terrorists.

intelligence analysis can be vexing, even for the most thoughtful and experienced professionals.⁵

Those in the law enforcement, defense, and intelligence communities whose jobs have involved anti- and counterterrorism efforts are now confronting a new type of adversary.⁶ From the end of World War II through the end of the Cold War, terrorist groups and activities were driven primarily by nationalistic interests. Most of these terrorists had similar, classic patterns: they belonged to discreet groups with hierarchical command structures; clearly defined ideology and objectives; were relatively small in number; and struck selectively and primarily at targets selected for their symbolic value, rather than their potential to maximize casualties. After an attack, the group responsible would most often identify itself and state the reason for the violent act. As Bruce Hoffman has so aptly stated: “However disagreeable or repugnant the terrorists and their tactics may have been, we at least knew who they were and what they wanted.”⁷

Al-Qaeda and the transnational terrorist groups of the present, however, are motivated and operate much differently than the stereotypical groups of the past.⁸ There is a command structure for al-Qaeda’s small, but effective core, and a decentralized outer band, that is level and variant to control and autonomy. Unlike past terrorist groups, al-Qaeda has the strength of numbers, with cells represented in multiple countries worldwide, and their technical training and sophistication are far greater. Targets are selected with varying discrimination, from symbolic to economic and opportunistic, and accessibility and tactics are chosen to increase the magnitude and scope of lethality.⁹ Al-Qaeda’s leadership has gone to great lengths to adopt the linear model of thinking and problem solving that is readily found in Western doctrine, and which counters their otherwise more natural associative thinking patterns. Killing is no longer the incidental outcome of an attack; it is the central purpose of the attack.¹⁰ Al-Qaeda’s objectives and ideologies remain much more elusive, in that there is less attributed connection between the chosen action and the stated cause.¹¹

Just as war planners must adapt to the evolving threats of combat, so too must those concerned with national security recognize that these new terrorist threats are not just another handful of nails waiting to be driven by the nation’s trusty hammers of force and diplomacy.¹² The threat of terrorism to national and international security has evolved and is continuing to evolve. Efforts to contain and effectively terminate this threat must transform to adapt to these changes.

CONTEMPORARY THREAT ENVIRONMENT

In analyzing the threat from the new transnational terrorists, some scholars of military operations have drawn parallels with elements of “fourth

generation warfare”¹³ and “asymmetric warfare.”¹⁴ Briefly, the concept of fourth generation warfare (4GW) comes from an analysis that modern warfare (post-Industrial Revolution) has evolved through four phases.¹⁵ The first phase was characterized by dominant use of the smoothbore long gun deployed with “line and column” tactics. Combat effectiveness depended on mass of manpower and rate of fire. A second generation emerged with the development of the rifle-barrel musket, and was enhanced by automatic machine guns and artillery. As a result of these technological advances, the firepower of an assault no longer depended on massive manpower. Tactically, troops would advance—usually now in small groups—after an infusion of firepower attacks. This shifted the mode of confrontation. Battles were no longer waged between two lines of armed combatants standing face-to-face, engaging in direct fire on the battlefield. The foundation for (but not implementation of) third generation warfare was firmly in place by World War I. Armament technology continued to advance; but significantly, ideas and strategy also gained ascending importance in operational planning.

The major third generation of development was a shift toward maneuver warfare. That is, troops gained advantage over an enemy not simply by destroying them and reducing their numbers (attrition), but rather by maneuvering around their defenses and infiltrating with less direct confrontation.

The fourth generation trends are driven largely by ideas, with radical changes to the concepts of both combat and combatants. Lind, Nightengale, Schmitt, Sutton, and Wilson, authors of the seminal work on 4GW, state that the goal is to collapse the enemy internally, rather than to defeat him physically. They describe its manifestation as follows:

In broad terms, fourth generation warfare seems likely to be widely dispersed and largely undefined; the distinction between war and peace will be blurred to the vanishing point. It will be nonlinear, possibly to the point of having no definable battlefields or fronts. The distinction between “civilian” and “military” may disappear. Actions will occur concurrently throughout all participants’ depth, including their society as a cultural, not just a physical, entity.¹⁶

Although written in 1989, this formulation describes the contemporary operational mode of al-Qaeda and other contemporary transnational terrorist groups.¹⁷ In fact, in a remarkably prescient hypothetical, Lind et al. ponder the potential challenges to the U.S. were terrorists to use existing technology combined with the following elements:

- A non-national or transnational base, such as an ideology or religion.
- A direct attack on the enemy’s culture.

- Highly sophisticated psychological warfare, especially through *manipulation* of the media, particularly television news.¹⁸

Fourth generation warfare is not necessarily terrorism, but terrorists do appear to be using 4GW strategy and tactics.¹⁹ An effective counterterrorism response will need to be driven by good intelligence.²⁰

Intelligence has been defined broadly as “the product resulting from the collecting and processing of information concerning actual and potential situations and condition relating to domestic and foreign activities and to domestic and foreign or US and enemy-held areas.”²¹ Among its objectives are the acquisition of facts about, and an understanding of the adversary’s goals, intent, methods, and capacities. This new framework for action calls for new strategies from intelligence agencies that monitor and assess extremists; from law enforcement agencies that observe, record, and investigate their behavior; and from military and defense agencies attempting to contain or eliminate them. In countering operational tactics that rely heavily on strategic analysis and psychological effect, behavioral research has a clear role to inform those efforts, but only if those research products are operationally relevant.

PSYCHOLOGICAL VS. OPERATIONAL RELEVANCE

While much has been written about the “psychology of terrorism,” many questions remain.²² Particularly important are questions that have operational relevance—those that can influence the thinking and action of organizations and individuals with responsibility to disrupt and destroy terrorists networks. For example, terrorism expert Martha Crenshaw notes that tensions have arisen from policymakers’ insistence on the possibility of a fixed and unambiguous “terrorist profile,” a list of characteristics that permit identification of actual or potential terrorists.²³ There is also debate about whether terrorism is best understood as a form of psychopathology or as a strategic choice.²⁴ Numerous mental health professionals have sought to explain terrorist behavior in conventional psychiatric terms, mainly by posing theory-laden hypotheses.²⁵

Whether terrorists collectively suffer from paranoia or wallow in narcissism seems, however, to be of little operational significance to investigators, intelligence analysts, case officers, military operatives, or defense planners. The guiding principle for any behavioral research that seeks to inform questions of homeland or national security is not whether the study question is *psychologically* interesting or relevant, but whether it is *operationally* relevant. Viewed this way, behavioral research may be responsive to the needs of those with operational responsibilities.

An Example of Operationally Relevant Research in Practice

In the early 1990s Robert Fein and Bryan Vossekuil—working at the time for the U.S. Secret Service—pioneered a strategy for conducting operationally relevant behavioral research. Around that time, several cases had come to the attention of the Secret Service that raised questions about conventional wisdom regarding assassins and assassination behavior. For example, the frequent assumption was that a person seeking to assassinate a U.S. President would be (a) motivated by mental illness; (b) first communicate a threat to the target; (c) have a grievance or feelings of animosity toward the target; and, therefore, (d) have a focused, single direction of interest. But the cases that had come to attention, although quite serious, did not fit that preconceived pattern. This led the Secret Service to reexamine its assumptions about assassination behavior and the way in which it assessed potential threats to its protectees.²⁶

Fortunately, assassination is a very rare phenomenon, so the initial research challenge was to determine how to systematically study such an infrequent event. Fein and Vossekuil chose to focus on incidents in which one or more individuals had attacked—or approached with lethal intent—a public figure, chosen for the attack because of his/her public status. For the method of inquiry, they developed a modified, intensive case study approach. Using a structured codebook, they examined the patterns of thinking and behavior of all 83 persons known to have attacked or come close to attacking a person of public status in the U.S. over the preceding fifty years. The choice to focus on “patterns of thinking and behavior” was deliberate. The objective was not to determine “what makes people become assassins”; rather, it was to examine whether there were discernible behaviors that were known, or knowable in advance, that could have marked a pathway toward a planned violent act. If so, these markers might help investigators prevent future attacks. The study, called the Exceptional Case Study Project (ECSP), focused on seven operationally relevant questions:²⁷

- How do attackers develop the idea to assassinate a public official or public figure, and move from idea to action?
- What is the range of motives for assassination?
- How do attackers select their target(s)?
- How do attackers plan for the attack?
- What do attackers communicate to anyone about their ideas or intent prior to the attack?
- What role, if any, does mental illness play in motivating or implementing an attack?
- Are there key life factors that play any role in motivating or implementing an attack?

A systematic investigation of these questions produced several surprising findings that challenged the prevailing assumptions about assassination. Mental illness was not a critical factor. Most attackers and near-attackers did not harbor a grievance or animosity toward the target. Many had considered multiple targets (multiple directions of interest). And none of the persons who actually mounted an attack against a public figure had communicated a prior threat to the target. The findings called for a radically different approach to assessing and managing threats to public figures, including Secret Service protectees.²⁸ Conceived in an operational environment, translating ECSP findings into recommendations for how that process could be improved was not difficult.

Principles of Operationally Relevant Research

The ECSP and its approach were distinguished by the fact that the empirical inquiry was driven by a need to inform key investigative and protective—rather than scientific, psychological, or sociological—questions. The same method can be applied to other acts of planned, lethal aggression, including those that pose a threat to homeland or U.S. national security. Fein and Vossekuil coined the term “targeted violence” to describe those situations where an identified or identifiable perpetrator has come to official attention, raising the question of a potential threat to an identified or identifiable target(s).²⁹ Many diverse acts of violence fall within that broad definition. In fact, some of the horrific shootings occurring in schools in recent years could also be viewed as a form of targeted violence. Consequently, the operationally relevant ECSP methodology was applied to those incidents, again leading to some compelling and illuminating results, with direct implications for school safety.³⁰ To achieve this level of relevance, however, requires rigorous adherence to certain principles in the design, implementation, and analysis of the research study.

First, the research endeavor must be operationally informed. The design of the inquiry must begin with an understanding of the key ultimate questions that end users (e.g., investigators, intelligence analysts, defense, and security decisionmakers, etc.) routinely are required to answer, the threshold decisions they are required to address, and the environment in which that process occurs. For example, an investigator may need to know: “Does this person (or groups) pose a threat to U.S. assets or interests, and if so, what kind of threat?” That analysis may occur in an operational context where the investigator is aware of many persons and groups in the jurisdiction that espouse some kind of extremist ideology and potentially violent rhetoric. Having extreme beliefs and ideas, *per se*, is not uncommon, nor is it a crime. Moreover, all people with extremist ideas cannot be assumed to pose a similar type and level of threat to U.S. interests. Therefore, generating knowledge that an investigator can use and

apply to answer a key question of threat assessment requires an understanding of the operational context.

Similarly, the research plan should take into account the *process* of investigation and analysis typically applied to the problem, including what kinds and sources of data or information are available to the decisionmaker.³¹ Because the goal is to develop information that will inform operational questions and activities, the study should be conceived and crafted in a way that is consonant with the procedures and language of those who will use or apply it.³² Accordingly, having operational personnel involved at every phase of the study plan and implementation is helpful.

Second, the study should maintain a behavior-based focus. When exploring the realm of terrorism or other violent behavior, speculating about the personality or internal dynamics of the actors may seem intriguing or even tempting.³³ These questions, though perhaps having some theoretical or even scientific merit, are unlikely to produce operationally relevant findings, for at least two reasons:

- (1) Individual personality factors tend not to be the causes that best explain violent behavior, nor do they help reliably to distinguish “terrorists” from “non-terrorists,” and
- (2) This type of information tends not to be routinely known or “knowable” to investigators or analysts examining a potential threat.

For example, in the past, some experts have argued that one form of “terrorist psychopathology” arises from an individual’s developmental failure to psychologically separate and individuate from his or her parents.³⁴ Even if investigators and analysts could reliably determine what that means, information would not likely be readily available about whether a person of investigative interest has successfully navigated the developmental task of separation-individuation. Maintaining a behavioral focus in the study, therefore, enhances operational utility and leads to more specific threat assessment indicators.

Third, the interpretation or lessons from the study must derive from an analysis of incident-related behaviors. This means that facts should drive conclusions. Those designing and analyzing the research should recognize that preconceived notions, assumptions, or conventional wisdom may be wrong. A major objective of research is to submit ideas and hypotheses to critical scrutiny. Operational research should set aside preconceptions about what “causes” the behavior, and redirect interest to what behaviors precede the outcome. The approach used in ECSP and related studies was to “work backwards from the incident to the idea.” By beginning with the outcome—such as an attack incident—it is possible to trace backwards the progression of tasks and behaviors that were necessary to accomplish

the act. These incident-related behaviors will be the most specific and reliable indicators of planning or preparing for an attack.

ADVANTAGES OF A RESEARCH-BASED APPROACH

To believe that one can learn from experience is not difficult or particularly controversial. Accepting that premise, the question then becomes: What kind of experience will lead to prevention and how can lessons best be learned and developed from that experience? Anecdotes and case studies are used routinely in law enforcement, military training, and in the academic field of strategic studies.³⁵ Some distinct advantages can be gained from relying on a methodical analysis of multiple cases, rather than drawing general conclusions based on a single case.³⁶

The first advantage is that the analysis is systematic.* With anecdotal accounts, knowing how best to extract the lessons from the narrative is often difficult. This is true even if multiple cases are anecdotally examined. Different preincident behaviors or contextual factors may be more readily apparent in some cases than in others. For example, a terrorist target may appear to be drawn directly from the al-Qaeda training manual, while another may not. But the common behavioral element may have been that all potential targets of a particular type or in a particular region were surveilled and assessed prior to selection. Clearly, that lesson would have implications beyond a conclusion that consulting the training manual to determine which targets should be hardened or monitored is advisable. Systematic observation across multiple incidents facilitates this broader view.³⁷

The second advantage, a result of systematic observation, is that the analysis can reveal patterns, deviations, and possible cluster or typologies of the studied behavior. Explaining and applying findings from behavioral research is easier when they can be analyzed and presented within some type of conceptual framework. Gathering the same information, on the same behaviors, defined in the same way, across different cases, allows enough variability that the phenomenon (e.g., terrorists attacks) more generally can be deconstructed into its component parts. Single cases may

*The ECSP and related case-series studies of relatively rare events are based on a systematic method of empirical inquiry. We draw a distinction between a systematic method of inquiry and the more traditional scientific method. The scientific method aspires to derive knowledge from true experimental studies with random assignment and proper controls for all potentially confounding variables. Given the nature of the events of interest in an operational context, it is often impossible or impractical to design and conduct a study within such narrow parameters.

be idiosyncratic and anomalous, not lending themselves well to inference of trends or more general principles.³⁸

APPLICATIONS OF BEHAVIOR-BASED OPERATIONAL RESEARCH

Once a study has been conducted, how might the findings and lessons be applied to operational tasks? The National Commission Report on Terrorism concluded that: “the best weapon against international terrorism is good intelligence.” Information from operational research can best be used to inform the collection, analysis, and dissemination of protective intelligence, and the assessment and management of potentially threatening situations.

Information Gathering

An operational research analysis can identify specific behaviors that might suggest planning or preparation for an attack. State and local law enforcement personnel, serving on the front line of America’s homeland defense, have as one of their many roles to serve as the “eyes and ears” of the intelligence community.³⁹ They often are in a better position than federal officials to observe suspicious and attack-related behaviors in the community. To execute that role effectively, however, they need to know what specific behaviors to look for and what should be a source of concern.⁴⁰ A behavior-based, operational analysis of past attacks and attempts can identify mechanisms for target selection, surveillance, communication, intelligence gathering, subverting security, and acquiring and preparing weapons to help front-line data gatherers focus and organize their observations.⁴¹

Intelligence Analysis

Research results can suggest not only specific behaviors to look for, but also ways to organize the incoming information. As noted, an advantage of research—defined here as systematic observation across multiple cases—is that it can reveal patterns of activity and deviations from those patterns. By understanding the patterns and sequences of preattack activity, investigators will have a refined set of guiding questions that frame the analysis of threat-related information. Questions arising from research might include: How are targets selected? What information is gathered about potential targets prior to the attack? How is that information gathered? How are the means of the attack chosen? How are they acquired? How many people are involved? What are their roles? How do they communicate? In this way, analysts can interpret incoming information in relation to other information, patterns, and past events.

Resource Deployment

A key challenge in homeland security planning is to determine how best to deploy limited resources. All persons or groups of potential concern cannot be constantly monitored. All potential targets cannot be maximally hardened and continuously watched. Planners must decide what kind of preventive resources have the greatest likelihood of deterring certain types of attacks against certain types of targets.⁴²

Operational research can help to guide these resource deployment decisions. Research results point to patterns in terrorist target selection and attack planning that can be combined with data from vulnerability assessments to produce a more comprehensive plan of defense and asset protection. Homeland defense strategies and activities are dynamic, and should change constantly to adapt to the evolving threat environment.⁴³ Defensive maneuvers should track and lead these offensive/attack maneuvers. A systematic knowledge of enemy (terrorist) planning and operations can lead to more informed security plans and decisions.

Identification of Critical Inter-System Relationships

Operational research, as described here, focuses on facts and behaviors that are known or knowable prior to the attack. But different facts can come from different sources. A third application of research results is to identify the source of critical information. Knowing this source helps national security and homeland defense planners identify the key agencies and systems to involve in information sharing, intelligence analysis, and security development.⁴⁴

Information Integration

Sometimes, after a terrorist attack has occurred, and the incident has been thoroughly and critically reviewed, the evidence of planning and preparation seems abundantly clear. Comprehending why the attack was not foreseen and prevented may be difficult. A distinct advantage of retrospective analysis, however, is that, after the fact, all critical information is known, collated, and analyzed in light of the known outcome. This, typically, is not the case in an ongoing investigation or threat assessment. Some pieces of the puzzle may be missing. Some pieces may be held by persons or agencies that are not sharing or even communicating with others.⁴⁵ And, at this early stage, no one with any of the pieces knows the outcome or what the end product will look like.

Operational research can capitalize on those retrospective advantages and apply them to prospective analyses. It can suggest better questions to direct the investigation. It can give guidance to investigators and analysts about

what kind of relevant information may be known or knowable prior to an attack, where such information may be located and corroborated, and how pieces of information may fit together. For example, an analysis of past attacks by a particular group may ascertain that a certain level of chatter between individuals of investigative concern was often followed by a transfer of money in certain increments into known accounts. This monetary transfer was followed closely by activity that built capacity for the attacks, such as weapons acquisition, technical training, production of false documents, etc. A piece of information integrated with other information often takes on a new—and perhaps more significant—meaning. One way that research findings can be used as an operational tool is to help specify the relevant pieces of the puzzle, point to where they might be found, and how they might relate to one another.

THE NEED FOR RELEVANCE

The current threat to United States interests posed by terrorism is considerably different—and arguably more lethal—than in the past. Terrorists are taking advantage of new technology and becoming more strategically sophisticated, often intentionally applying asymmetric maneuvers and elements of fourth generation warfare. The nature of this threat requires a U.S. response that is intelligence-driven and uses information effectively.

Research analyses of past plans, operations, and attacks can assist in this effort, but only if the studies are planned and conducted with an emphasis on operational relevance. That requires that research questions, design, and analyses be informed by a thorough understanding of the key issues and tasks that end-users (e.g., investigators and analysts) are required to address and the process by which their inquiries are conducted.

The study approach developed by Fein and Vossekuil in their operational analysis of assassination behavior—the Exceptional Case Study Project—serves as both an exemplar and a road map for examining other acts of aggression against U.S. assets and interests. Using that operational research approach over the more traditional single case study allows the examination to be more systematic and perhaps identify patterns, trends, and deviations that may not otherwise be apparent.

Applying this research method to cases of terrorism could produce findings that would help to guide information gathering, intelligence analysis, resource deployment, identification of inter-systems relationships, and information integration. Those advances should lead to a more effective use of information in the intelligence-driven war against the new terrorism.

REFERENCES

- ¹ “Washington Dateline: Heightened Alert,” Associated Press Online, 10 September 2002.
- ² U.S. Senate Select Committee on Intelligence, *Hearing on Current and Projected National Security Threats to the United States, 6 February 2002* (Washington, D.C.: Superintendent of Documents).
- ³ Robert Bryant, John Hamre, John Lawn, John MacGaffin, Howard Shapiro, and Jeffrey Smith, “Special Report: America Needs More Spies—Intelligence and Security,” *The Economist*, U.S. edition, 12 July 2003, p.3.
- ⁴ Bruce Berkowitz, “Better Ways to Fix U.S. Intelligence,” *Orbis*, Vol. 45, No. 4, 2001 pp. 609–619. John Deutch and Jeffrey Smith, “Smarter Intelligence,” *Foreign Policy*, Vol. 128, January/February 2002, pp. 64–69. Robert David Steele, “Crafting Intelligence in the Aftermath of Disaster,” *International Journal of Intelligence and CounterIntelligence*, Vol. 15, No. 2, Summer 2002, pp. 161–178. U.S. Senate and U.S. House of Representatives, Final Report, *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001: The Context, Part I: Findings and Conclusions*, 10 December 2002 (Washington, DC: Government Printing Office), pp. 60–70.
- ⁵ Eugene R. Bertolli and Constantine J. Forkiotis, “Recognizing Unconventional Terrorists Attacks,” *International Journal of Counterterrorism and Homeland Security*, Vol. 8, No. 3, pp. 20–22.
- ⁶ Joseph Cirincione, “Defending America,” *Georgetown Journal of International Affairs*, Vol. 3, No. 1, 2002, pp. 127–153. Bruce Hoffman, “Rethinking Terrorism and Counterterrorism Since 9/11,” *Studies in Conflict and Terrorism*, Vol. 25, No. 5, pp. 303–316.
- ⁷ Bruce Hoffman, “Lessons of 9/11.” Paper submitted on 8 October 2002 for the Committee Record, U.S. Congress Joint Inquiry into Intelligence Activities Before and After the Attacks of September 11, 2001.
- ⁸ Ed Blanche, “Al-Qaeda Recruitment Targets the Intelligent, Disciplined and Devout,” *Jane’s Intelligence Review*, No. 14, 2002, pp. 27–28. James Stinson, “Al-Qaeda,” Paper presented to the Mid-Atlantic/Great Lakes Organized Crime Law Enforcement Network Conference, Cleveland, Ohio, 25 April 2002.
- ⁹ Jane Corbin, *The Base: Al-Qaeda and the Changing Face of Global Terror* (London: Pocket Books, 2003), pp. 41–53.
- ¹⁰ Sharad Chauhan, *The al-Qaeda Threat* (New Delhi: A. P. H. Publishing Corp., 2003).
- ¹¹ Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Columbia University Press, 2002). Paul J. Smith, “Transnational Terrorism and the al-Qaeda Model: Confronting New Realities,” *Parameters*, Vol. 32, No. 2, pp. 33–46.
- ¹² Donald Rumsfeld, “A New Kind of War,” *The New York Times*, 27 September 2001 at www.defenselink.mil/speeches/2001sz0010927-secdef.

- ¹³ Gary I. Wilson, "The Next Conflict," *Marine Corps Gazette*, Vol. 85, No. 11, November 2001, pp. 73–76.
- ¹⁴ Stephen C. Small, "Small Arms and Asymmetric Threats," *Military Review*, Vol. 80, No. 6, November/December 2000, pp. 33–41.
- ¹⁵ William S. Lind, Keith Nightengale, John F. Schmitt, Joseph Sutton, and Gary I. Wilson, "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette*, October 1989, pp. 22–26.
- ¹⁶ Ibid.
- ¹⁷ Jane Corbin, *The Base: al-Qaeda and the Changing Face of Global Terror*, pp. 41–53.
- ¹⁸ William S. Lind et al., "The Changing Face of War," pp. 22–26.
- ¹⁹ Harold A. Gould and Franklin C. Spinney, "Fourth-Generation Warfare Is Here," *Defense Week*, 15 October 2001. William S. Lind, Major John F. Schmitt, and Colonel Gary I. Wilson, "Fourth Generation Warfare: Another Look," *Marine Corps Gazette*, December 1994, pp. 34–37.
- ²⁰ Ely Karmon, "The Role of Intelligence in Counter-terrorism." Paper presented at the Conference on Intelligence in the 21st Century, Center for Advanced Studies of Terrorism and Political Violence, Priverno, Italy, 2001.
- ²¹ Leo Carl, *International Dictionary of Intelligence* (McLean, VA: Maven Books, 1990).
- ²² Chris E. Stout, ed., *The Psychology of Terrorism: Vols. I–II* (Westport, CT: Praeger/Greenwood Publishing, 2002). Jerrold M. Post, "Individual and Group Dynamics of Terrorist Behavior," in *Psychiatry: The State of The Art* (New York: Plenum 1985), Vol. 6. Rex A. Hudson, *The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why?* (Washington, DC: Library of Congress, Federal Research Division, 1999), pp. 1–60.
- ²³ Martha Crenshaw, "The Psychology of Terrorism: An Agenda for the 21st Century," *Political Psychology*, Vol. 21, No. 2, June 2000, pp. 405–420, at p. 407.
- ²⁴ Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind* (Washington, DC: Woodrow Wilson Center Press, 1998).
- ²⁵ Charles Ruby, "Are Terrorists Mentally Deranged?," *Analyses of Social Issues and Public Policy*, Vol. 2, No. 1, 2002, pp. 15–26. Andrew Silke, "Cheshire–Cat Logic: The Recurring Theme of Terrorist Abnormality in Psychological Research," *Psychology, Crime & Law*, Vol. 4, No. 1, April 1998, pp. 51–69.
- ²⁶ Robert A. Fein and Bryan Vossekuil, *Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials* (Washington, DC: U.S. Department of Justice, 1998). NIJ/OJP/DOJ Publication No. 170612, available on World Wide Web at <http://www.nvpsc.org>
- ²⁷ Robert A. Fein and Bryan Vossekuil, "Assassination in the United States: An Operational Study of Recent Assassins, Attackers, and Near-Lethal Approaches," *Journal of Forensic Sciences*, Vol. 50, 1999, pp. 321–333.
- ²⁸ Ibid.

- ²⁹ Robert A. Fein, Bryan Vossekuil, and Gwen A. Holden, "Threat Assessment: An Approach to Prevent Targeted Violence," *Research in Action*, National Institute of Justice, 1995, pp. 1–7.
- ³⁰ Bryan Vossekuil, Robert A. Fein, Randy Borum, and William Modzeleski, *The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States* (Washington, D.C.: U.S. Department of Education, Office of Elementary and Secondary Education, Safe and Drug-Free Schools Program, and U.S. Secret Service, National Threat Assessment Center, 2002).
- ³¹ Robert David Steele, "Crafting Intelligence in the Aftermath of Disaster."
- ³² *Intelligence 2000: Revising the Basic Elements* (Richmond, VA: International Association of Law Enforcement Intelligence Analysts/Law Enforcement Intelligence Unit (IALEIA/LEIU), 2000).
- ³³ See reference no. 22.
- ³⁴ Jerrold M. Post, "Individual and Group Dynamics of Terrorist Behavior."
- ³⁵ David Collier and James Mahoney, "Insights and Pitfalls: Selection Bias in Qualitative Research," *World Politics*, Vol. 49, No. 1, October 1996, pp. 56–91. Alexander L. George, "Case Studies and Theory Development: The Method of Structured, Focused Comparison," in Paul G. Lauren, ed., *Diplomacy: New Approaches in History, Theory, and Policy* (New York: The Free Press, 1979), pp. 43–68. Stephen Biddle, "Victory Misunderstood: What the Gulf War Tells Us About the Future of Conflict," *International Security*, Vol. 21, No. 2, Fall 1996, pp. 139–179. Stephen Biddle, "The Past as Prologue: Assessing Theories of Future Warfare," *Security Studies*, Vol. 8, No. 1, Fall 1998, pp. 1–74. Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, NJ: Princeton University Press, 2004).
- ³⁶ Timothy McKeown, "Case Studies and the Statistical Worldview," *International Organization*, Vol. 53, No. 1, Winter 1999, pp. 161–190.
- ³⁷ David Collier and James Mahoney, "Insights and Pitfalls: Selection Bias in Qualitative Research," pp. 56–91, and Timothy McKeown, "Case Studies and the Statistical Worldview," pp. 161–190.
- ³⁸ Timothy McKeown, *ibid.*, pp. 170–175.
- ³⁹ Douglas Bodrero, "Confronting Terrorism on the State and Local Level," *FBI Law Enforcement Bulletin*, Vol. 68, No. 3, 1999, pp. 11–18.
- ⁴⁰ *Possible Indicators of al-Qaeda Surveillance*, Information Bulletin 03–004 (Washington, DC: U.S. Department of Homeland Security, 2003). *Terrorist Pre-Incident Indicators* (Tallahassee, FL: Institute for Intergovernmental Research, State and Local Antiterrorism Training Program, 2002).
- ⁴¹ Joshua Sinai, "How to Forecast Intentions, Capabilities and Likelihood of Terrorist Groups Resorting to Low Impact Catastrophic Warfare," *International Journal of Counterterrorism & Homeland Security*, Vol. 9, No. 1, 2003, pp. 19–22.
- ⁴² Jonathan White, *Defending the Homeland: Domestic Intelligence, Law Enforcement and Security* (Belmont, CA: Wadsworth Publishing, 2004), pp. 63–102.

- ⁴³ Chris Demchak, “Un-muddling Homeland Security: Design Principles for National Security in a Complex World,” *The Forum*, Vol. 1, No. 2, 2002.
- ⁴⁴ From: Office of Justice Programs, Global Intelligence Working Group, 12 June 2003, at http://it.ojp.gov/topic.jsp?topic_id=56. *Interim Report: Development of the National Criminal Intelligence Sharing Plan*, at <http://it.ojp.gov/documents/intellplan.pdf>
- ⁴⁵ U.S. Senate and U.S. House of Representatives, Final Report, *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, pp. 76–96.