

Psychological Support to Defense Counterintelligence Operations

Scott Shumate

*Counterintelligence Field Activity
United States Department of Defense
Washington, DC*

Randy Borum

*Department of Mental Health Law & Policy
University of South Florida*

The practice of providing psychological or behavioral science support to counterintelligence operations is relatively new, but actively evolving. Psychologists—some of whom refer to themselves as operational psychologists—provide assessments for, and consultations to, operators, case officers, service members, and others on psychological or behavioral issues relevant for planning, managing, or terminating elements of an operation and handling human assets. Specifically, they may conduct direct or indirect risk assessments, offer perspectives on source recruitment and handling, or support interrogations and other information-gathering activities. Counterintelligence's focal areas, currently, are counterespionage and counterterrorism. We describe how psychologists have provided value-added support to each of those Department of Defense missions.

Psychologists in the U.S. Armed Forces and the U.S. Department of Defense (DoD) are often required to function both as generalists and as specialists (Cronin, 1998). They are frequently called on to provide a wide range of nontraditional services in an even wider range of nontraditional contexts (Page, 1996). Military psychologists may even be asked to perform specialized assessments or interventions or to render professional opinions on issues with which they have no prior formal training or experience (Johnson, 1995). A clinical psychologist, who may be “the only game in

Correspondence should be addressed to Randy Borum, Department of Mental Health Law & Policy, Florida Mental Health Institute, University of South Florida, 13301 Bruce B. Downs Boulevard, Tampa, FL 33612. E-mail: borum@fmhi.usf.edu

town” may be asked to assess the suitability of a present or prospective operator to infiltrate enemy borders, under cover, collecting information to provide to U.S. forces. Another may be asked by a case agent or investigator to review files on a service member who is suspected of espionage. Faced with these and similar situations, most clinicians try to plant their feet firmly in basic ethical principles, attempting to be both responsive and responsible as they apply their skills while navigating in new terrain (Ewing & Gelles, 2004; Johnson, 1995, 2002).

Psychologists may, indeed, have insights and information of value on these and other counterintelligence (CI)-related questions. However, as with any area of specialized psychological knowledge, the better one knows the substantive landscape, issues to anticipate, and the relevant professional knowledge base (or lack thereof), the better able one is to provide competent and useful consultation to the person or agency making the request. The art of providing psychological or behavioral science support to counterintelligence operations is actively evolving. Although operational psychology (perhaps more appropriately called “national security psychology”) is a relatively new area of expertise, a cadre of behavioral science experts in the U.S. Department of Defense (DoD)—experienced in operational consultation—are striving to make their expertise available to support both specialized operational psychologists and the general military psychologist in responding to a range of requests from the CI community. This article describes an effort to bring state-of-the-art psychological support to CI operations and investigations in the U.S. defense community. We begin by introducing the nature and role of counterintelligence in the U.S. DoD, and a relatively new specialized psychological support unit developed for Defense CI operations. We then discuss potential roles and functions for psychologists who support CI operations, with some elaboration on the core areas of counterespionage and counterterrorism.

COUNTERINTELLIGENCE IN THE U.S. DEPARTMENT OF DEFENSE

Counterintelligence refers to

information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document or communications security programs. (Executive Order 12333, 1981, p. 1)

CI has long been a critical element in intelligence operations and national security policy. Like other intelligence elements, it has both analytic and operational functions. Although psychologists may support both functions, we focus here on their role in CI operations.

As Lowenthal (2003) suggested, there are three main categories of CI, and arguably of CI operations:

Collection: gaining information about an opponent's intelligence collection capabilities that might be aimed at you. Defensive: thwarting efforts by hostile intelligence services to penetrate your service. Offensive: having identified an opponent's efforts against your system, trying to manipulate these attacks either by "turning" the opponent's agents into double agents or by feeding them false information they will report home. (p. 113)

Because DoD and its affiliated entities control the majority of U.S. intelligence community resources and command the largest number of personnel, it is a major force in U.S. CI operations. Historically, each service component of the U.S. Armed Forces has managed the CI function for its own branch. In the Department of the Navy, that function is handled principally by the U.S. Naval Criminal Investigative Service (NCIS), in coordination with U.S. Marine Corps CI elements. In the Department of the Army, CI activities are centralized in the Army Intelligence and Security Command (INSCOM), and the Department of the Air Force is protected through the CI activities of the Air Force Office of Special Investigations (OSI).

Each CI entity has also been responsible for finding its own source of operational behavioral science and psychological support. NCIS uniquely has a stable core of civilian psychologists (and at least one uniformed service psychologist) on staff in their Psychological Services Unit (Code 02D) who specialize in operational support. Historically, INSCOM and OSI have relied exclusively on uniformed service psychologists, assigned to serve a tour in those commands, to provide behavioral science support. Those psychologists may or may not have had the opportunity for extensive training or experience with CI activities prior to their arrival. Over the years, informal sharing of resources, information, and even personnel between service components has allowed psychologists to collaborate in responding to requests for operational consultation or assistance.

In 2002, the DoD created Counterintelligence Field Activity (CIFA) as an umbrella combat support agency to coordinate all CI efforts throughout the DoD Community (DoD Directive 5105.67, 2002). CIFA's vision and implementation included a substantial infrastructure for operational psychological support. Within the first year, CIFA's organizational structure included a Directorate of Behavioral Sciences (DB) to be led by an experienced Senior Executive Service psychologist. At present, DB is staffed by a cadre of psychologists as well as analysts and former special agents. The Directorate also sponsors several contract psychologists to provide embedded support for INSCOM and OSI to supplement and collaborate with the uniformed psychologists. To be clear, DB's mission in relation to the service components is to support, not to supersede or replace, existing psychological resources.

CIFA's commitment to behavioral sciences has been realized not only in planning, but also in practice. Any CI operational plans originating in CIFA are sent to

DB for review and behavioral input before final approval. In addition, DB psychologists are available to CIFA operators for ongoing case consultation.

PSYCHOLOGICAL SUPPORT FOR COUNTERINTELLIGENCE OPERATIONS: ROLES AND FUNCTIONS

CIFA's DB has carved out a variety of roles to support DoD CI investigations and operations, both directly and indirectly. Indirectly, they train, advise, assist, and support military and civilian psychologists in the DoD service components in their consultation on CI operational activities. They have taken on training and coordination as the core of their indirect support functions to enhance the sharing and dissemination of information on practicing in CI contexts and, more generally, to encourage best practices in psychological support to CI operations, particularly those in DoD. Their vision for the future includes helping to advance the base of knowledge in operational psychology through systematic inquiry and operationally relevant research (Borum, Fein, Vossekul, Gelles, & Shumate, 2004).

More directly, DB psychologists provide assessments for, and consultations to, operators, case officers, service members, and others on psychological or behavioral issues relevant for planning, managing, or terminating elements of an operation and handling human assets. These include the four functional CI issues discussed in the following sections.

Risk

Psychological risk assessments are a core support function before, during, and after a CI operation. CIFA DB has assembled and hosts a Risk Assessment Working Group (RAWG), with an open invitation to psychologists throughout the DoD and the U.S. intelligence community who conduct psychological screenings for sensitive and high-risk national security positions. The nature of the positions can be quite diverse, ranging from administrative and clerical personnel who simply hold security clearances to potential agents and case officers. The objective is to share information, challenges, solutions, and lessons learned in an effort to work toward best practice models.

The nature of CI risk assessment questions and methods also varies considerably. Preemployment evaluations often seek to screen out persons with undesirable characteristics that may place them at undue risk for security compromise or for job-related performance problems (Borum, Super, & Rand, 2003). During an operation, however, a concern may emerge about the psychological condition of an asset (case officer or agent), and whether—and the extent to which—any impairment could compromise the operation's success. Because the mission in CI operations is

of primary importance, these risk assessments also carry an implicit—if not explicit—mandate to generate interventions or risk management strategies to potentially contain, suppress, or delay psychological impairments until mission objectives have been accomplished. These risk assessments may be conducted using an approach that is either direct (i.e., face-to-face evaluations where the purpose of the encounter typically is known to the examinee) or indirect (i.e., an assessment without a face-to-face encounter, typically based on writings, records, reports, collateral interviews, and perhaps even observations. The “subject” of the assessment is usually unaware that he or she is being assessed; Ewing & Gelles, 2004). Finally, after an operation, the psychologist may need to assess risk in the context of debriefing or repatriation efforts. Among the psychological support functions for CI operations, psychological risk assessments (at least direct ones) are probably the most similar to typical psychological services, although the criteria for success, tools available, and mandates for recommendations plainly call for a supplemental, specialized body of knowledge and skills.

Recruiting

CI operations often—although not always—involve the use of human assets who are affiliated in some way with an enemy or adversary. Whether these assets self-identify as “walk-ins,” or are spotted and approached by a U.S. contact, there is a necessary assessment and vetting process that must attend a decision about whether this person can and should be recruited to collect information for the United States. Psychologists may consult in a variety of ways at any stage of asset identification and recruiting activities from prerecruitment, through targeting, assessing, and developing the asset.

The operational judgments to be made here are critical to the success of the mission, but are not easily accomplished. Traditional psychometric tests are not designed to discern an individual’s responses to competing identities and loyalties or ability to follow rules of tradecraft. Psychologists in the intelligence community have developed, and are continuing to refine and generate, some guides and tools that relate more specifically to capacities and traits of interest in operational assessments, such as split loyalties and competing identities. Many of these products are not psychometric tests, but rather guides to enhance information collection and to facilitate communication among agents, analysts, and psychologists as they consider behavioral aspects of an operation (Gelles, Palarea, Arita, & Hawkes, 2005). These nascent tools remain sensitive, but efforts to develop and standardize tools and procedures represent an important advance in operational assessment methodology.

In addition to assessing personality and motivational variables that may affect an asset’s performance, considering the impact of cultural factors may also be significant. Many assets—particularly in current counterterrorism-related opera-

tions—come from cultures that are markedly different from those of their (typically) Western handlers or case officers. These differences can affect relationships, trust, clarity of communication, interpretation of behavior, delivery of instructions, and a host of other behavioral issues (Matsumoto, 2001; Saraswati, 2004). The psychologist can sometimes bring a degree of objectivity or cross-cultural insight to the observations and impressions of those directly involved in the case.

During initial stages of operational planning, a psychologist can sometimes identify or anticipate a particular behavioral issue or challenge to bring to the attention of the case officer and suggest some potential strategies for managing them in an operational context. The behavioral science consultant may even be able to offer insights or help brainstorm about asset vetting processes around key areas of concern including possible “tests” or exercises and subsequent interpretation of performance.

Handling

Successfully managing or running an asset in a human intelligence (HUMINT) CI operation rests heavily on managing the relationship. Psychologists can provide consultation, assistance, and support to a case officer running an asset, including, for example, ongoing credibility assessments, problem solving, and monitoring and managing an asset’s vulnerabilities and mental condition.

Psychologists may make handling recommendations based on a direct or indirect assessment. In direct assessment, the psychologist would meet with the source, and conduct an examination or gather data that would be relevant to the questions the case officer has posed. Many times, this encounter would be structured like most any other psychological evaluation, although in some circumstances, elements of the situation may be need to be modified or veiled for security reasons. In indirect assessment, the psychologist would gather data only from places and people other than the source himself or herself. The sources of information may include case officer notes and records, collateral interviews, video observations, and historical information. A request for source-handling consultation may be prompted by concerns about a source’s competing identities; changes in the source’s behavior, productivity, or performance; perceived personality conflicts; or an anticipated change in the tasking with which the source may be charged. The selection of assessment methods is determined by the nature of the referral questions, sensitivity of the case, and demands of the mission.

Elicitation

Many CI operations ultimately require that critical information is retrieved from a human source who is often unwilling to cooperate. Eliciting (or retrieving) accurate, useful, and complete information from an uncooperative source is one of the most vital and challenging tasks in a CI operation (Fein, 2006). Psychologists can

offer unique incremental value in support of interrogations and other HUMINT collection efforts.

Recent events have made it clear that operational interrogation support is an enterprise fraught with potential pitfalls. It is absolutely possible, however, for a trained psychologist to offer assistance with interrogation in an ethical manner. The American Psychological Association (2005) Presidential Task Force on Psychological Ethics and National Security concluded:

Psychologists may serve in various national security-related roles, such as a consultant to an interrogation, in a manner that is consistent with the Ethics Code. ... The Task Force noted that psychologists have served in consultant roles to law enforcement on the state and federal levels for a considerable period of time. Psychologists have proven highly effective in lending assistance to law enforcement in the vital area of information gathering and have done so in an ethical manner. (p. 6)

One fact that has become clear amid coverage and scrutiny of HUMINT collection efforts in the global struggle against violent extremism is that no single technique or set of techniques is uniformly effective in eliciting information from every uncooperative source (Gelles, McFadden, Borum, & Vossekuil, 2006). Psychologists researching psychotherapy outcomes ultimately concluded that the central question was not “Does psychotherapy work?” but rather “What kinds of psychotherapy are most effective for what kinds of individuals with what kinds of disorders in what contexts?” A similarly nuanced approach is necessary to advance effective interrogation research and practice (Borum, 2006).

Psychologists may observe a source’s behavior, providing input into its interpretation as well as whether and how the source is responding to the interviewer or particular strategy or line of questions. They may be able to provide information to the case officer and interviewers about the effects of certain stressors on the source’s cognitive functioning or about the nature of human memory. Psychologists can draw on the empirical literature bearing on persuasion and interpersonal influence to suggest potential strategies to counter and overcome a source’s resistance (Borum, 2006). They may provide counsel on the source’s motivation or help to assess his or her credibility or attempts at deception.

PSYCHOLOGICAL SUPPORT FOR COUNTERINTELLIGENCE OPERATIONS: APPLICATIONS

As the foregoing discussion suggests, CI is a multifaceted field. For virtually every intelligence discipline, there is a corresponding CI application. HUMINT, however, historically has been, and remains, the primary mode of information collec-

tion. It is, in part, because of this that psychology has the potential to make such a significant operational contribution.

Two of the leading contemporary applications of CI technology and activity are counterespionage and counterterrorism. Counterespionage has always been a core CI focus, and in the post-Cold War security environment, countering terrorism has also gained prominence. In fact, a recommendation to extend strategic CI to the Global War on Terrorism was the first of seven “pillars of counterintelligence” advocated by National Counterintelligence Executive (NCIX) in developing the National Counterintelligence Strategy of the United States (Office of the National Counterintelligence Executive, 2005). In the sections that follow, we briefly discuss how psychological consultation might be utilized in counterespionage and counterterrorism operations.

Counterespionage

Fundamentally, espionage is about stealing secrets. The United States and most other nations routinely classify and safeguard certain information that is considered vital to national security. The objective is to protect information that, if known to enemies, adversaries, or those with hostile intention, could expose weaknesses and vulnerabilities or mitigate a strategic advantage. Defensive counterespionage activities are designed to thwart the efforts of those seeking to steal our secrets or to use them for unauthorized purposes. Offensive counterespionage operations seek to coopt individuals who have access to others’ secrets.

Members of any foreign intelligence service (FIS) are presumed to be hostile to U.S. security interests; it is sometimes said that there are friendly nations but no friendly intelligence services (Olson, 2001). For the FIS or hostile nonstate faction looking to infiltrate or compromise the United States, in many cases, the most direct way for them to steal our secrets is to get them from someone who has legitimate access (National Security Agency, 2001). This raises one of the most serious and vexing problems in contemporary counterespionage, the insider threat (Kipp, 2001; Smith, 1990). A recent analysis of U.S. espionage cases by DoD’s Personnel Security Research Center (PERSEREC) suggests that the threat posed by internal espionage, for a variety of reasons, has increased in recent years (Kramer, Heuer, & Crawford, 2005). This threat presents both a risk and an opportunity to CI efforts. Operations may be conducted to identify a suspected “mole” or insider providing information to hostile parties, but they may conversely involve the use of an insider to provide false leads and information to those parties. Psychologists can and do help support operations of both types.

In counterespionage operations assessing motivations is essential. According to a 2002 PERSEREC study of 150 espionage cases directed against the United States by U.S. citizens, insiders who betray their country’s secrets rarely seek or enter their security position with intent to do so (Herbig & Wiskoff, 2002). This is

true both for civilian and military cases. The idea or intent to engage in espionage usually comes some time after they are in their official position. Those in intelligence and communication-related positions were particularly well represented, comprising approximately a third of all cases.

That internal spies are developed only after they are cleared and hired has some significant implications for both offensive and defensive counterespionage operations. It suggests the central importance of understanding vulnerabilities to seeking or being recruited by a FIS or other hostile entity (Crawford & Bosshardt, 1993). It also suggests that there are typically approach and avoidance forces that operate to varying degrees in the individual's decision making. Motivations in espionage cases are typically multiple and often complex, frequently rife with ambivalence and competing needs and incentives. PERSEREC's research suggests that, over the past 70 years the motivational profile of those committing treason may have changed from a dominant focus on ideology to a dominant focus on money (Thompson, 2001).

Shaw, Ruby, and Post (1998), for example, applied some of the findings from another government-sponsored study of insider spies, called Project Slammer, to portray a "pathway" to espionage. They did not conduct the Slammer study, but merely framed its findings. Their proposed pathway is composed of the following events: (a) predisposing personal traits, (b) an acute situational stressor, (c) emotional fallout, (d) biased decision making or judgment failures, and (e) failure of peers and supervisors to intervene effectively (Shaw et al., 1998).

The basic idea here is that there are often discernible precipitating events that produce observable changes in behavior before and during the period of actual betrayal. This is consistent with findings from the PERSEREC study, in which a quarter of betrayers were known to have a major life crisis in the months before turning to espionage, and 80% were known to demonstrate one or more conditions or behaviors of security concern (Herbig & Wiskoff, 2002). Knowing the nature and frequency with which suitability concerns emerge in cases of insider betrayal before the espionage occurs can help to identify persons who may deserve greater interest in an investigation or to portray a credible scenario of a "false flag," vulnerable to exploitation. The following case study offers an example of how operational psychology may play a salient role in counterespionage operations.¹

Case study: Consultation in a counterespionage operation. A longstanding, credible source who worked inside a FIS advised his U.S. case officer that his home service was acquiring information from a person inside the Pentagon. When an insider is working for a FIS, that person is commonly referred to as a "penetration." The source did not know the identity of the penetration, but was able to provide

¹The scenarios provided here for counterespionage and later for counterterrorism are illustrative, not factual. They are fictionalized to avoid compromising classified information.

a few details of known demographics and operational travel patterns that allowed investigators to narrow the list of likely suspects from 2,300 to about 175. Investigators knew that investigating each potential suspect would be inadvisable. That effort would be time consuming, allowing opportunity for further breach. Furthermore, an open investigation of that scope could rouse the penetration's suspicion, making him or her nearly impossible to catch.

Investigators consulted an operational psychologist to explore whether any behavioral information or strategies might be used to further narrow the list and focus the investigation. At that time, PERSEREC was conducting a research study on security procedures that was widely known in the defense community. The psychologist raised the possibility that the study could provide cover for briefly interviewing select officials on security practices. He recommended a strategy sometimes used in psychological research on deception. The basic premise is that when a person wishes to not respond to, or to be associated with, a particular stimulus, she or he will avoid it so consistently that her or his response pattern is statistically anomalous. On that basis, the plan was to try to classify respondents into three categories of likely deception (e.g., high, moderate, and low) based on their responses to the index question.

After all responses were analyzed, interestingly, the answers of one respondent were markedly distinct from those of all others interviewed. This did not necessarily indicate that he was the penetration, but he continued to be of significant investigative interest. After months of intensive observation and analysis of additional forensic and investigative evidence, the individual was arrested for espionage. The original, realistic objective was not that the interview strategy would pinpoint the informant, but rather that this behavioral methodology might help investigators to more efficiently and surreptitiously identify cases with higher and lower indexes of suspicion to focus their investigation.

Counterterrorism

There is general consensus in the intelligence, defense, and diplomatic communities that transnational terrorism currently poses one of the most serious threats to U.S. national security. CI activities are a vital part of the overall U.S. strategy to combat terrorism, and DoD is at the heart of those efforts, including, but not limited to, force protection (Graham, 2002). Since 9/11, and throughout the Global War on Terrorism, U.S. military, intelligence, and law enforcement forces have had to reorient and redeploy resources to combat a nonstate adversary whose structure and operations are different from those of our past opponents and that are constantly evolving (Borum, 2004; Borum & Gelles, 2005). Plainly, this requires a different type of operation and a different strategy for attack (Wettering, 2000).

The most aggressive and proactive of these operations typically require recruiting or inserting a source inside an operational terrorist cell. CI-driven source operations against terrorist targets can prevent specific attacks, interrupt forward

motion, and sometimes yield valuable information. It is difficult, however, to access and infiltrate a security-conscious collective. To do so requires an understanding of behavior, interpersonal relationships, interpersonal influence, and group dynamics (Gelles, Borum, & Palarea, 2005). These conditions offer ample opportunity for psychological input. The following case study offers an example of how operational psychology may play a role in counterterrorism operations.

Case study: Consultation in a counterterrorism operation. DoD investigators were monitoring the recruitment activity of a local cluster (cell) of extremists suspected of planning a terrorist attack. Their investigation revealed that one extremist had a relationship with a U.S. Armed Forces service member that dated back to their youth. They continued to have contact, but it was suspected that the service member was unaware of his friend's extremist connections and activity. Investigators proposed recruiting the service member as a possible "access agent" into information about the friend specifically, and the cell more generally. The operational planners asked for psychological consultation to assess the member's suitability for such a task, to provide behavioral information about him that would assist case officers in his management, and to support the case handlers' ongoing assessment and monitoring of the operation's dynamics.

One feature of the operation that made it more precarious was the long-term friendship that existed between the member and the extremist target. One behavioral suggestion was to do a "trial run" using the serviceman as a covert source in another smaller operation, involving no people previously known to him. This approach had several benefits. It allowed the operations team and psychologist an opportunity to assess the serviceman's willingness to cooperate, ability to follow instructions and adhere to tradecraft, and capacity to cope with stress and uncertainty in a covert role. It also provided a mechanism to develop the relationship between the serviceman and case officer and to establish mutual trust and confidence.

The service member performed well—tactically and psychologically—in his trial operation and the case officer decided to approach him about the possibility of acting as an access agent against his old friend. A formal operational psychological assessment supported this decision. The case officer and psychologist jointly developed a plan about how best to present information and proceed with the recruitment meeting. During the meeting, the service member expressed a strong desire to assist and related his own concerns about some of his old friend's changing attitudes and associations.

The service member agreed to be an access agent to his friend and to slowly introduce probing questions, but only in a manner and time frame that the case officer felt was appropriate. The operation yielded important information as it unfolded over the year. During that time, the psychologist met twice with the access agent to monitor his coping and psychological status. When the operation concluded, the service member was deactivated from his role as a clandestine source. The psychologist and case officer had anticipated the serviceman might

subsequently experience some feelings of depression and let down, so they built into the operational plan a termination phase that helped him readjust to his nonoperational role as a productive service member.

CONCLUSION

CI activity is a vital part of U.S. national security. Psychologists bring a wealth of skills and expertise that can add unique value to CI activities generally, and to CI operations specifically. There are opportunities to assess risks; to provide consultations to case officers recruiting and running HUMINT collection operations; and to support civilian, military, and law enforcement elements conducting interrogations. The opportunities are plentiful, but qualified operational psychologists are in short supply.

Although many defense CI operations (and behavioral consultations) involve attempts to detect or thwart espionage, operations focused on countering terrorism are also increasingly common. As CI operations continue to expand in the ongoing global struggle against violent extremism, opportunities will become increasingly available for psychologists in the military and defense community to provide operational support in matters of national security.

What are the implications of this trend? First, a DoD-wide collaborative effort should emerge to assemble the collective wisdom of experienced practitioners and move toward a collection of best practices for the major CI-behavioral functions. Second, practitioners and researchers working in CI should jointly create an agenda for needed behavioral research to inform operationally relevant CI questions; develop cooperative methods and protocols for conducting the research; and with those findings, craft the foundation for a discipline-specific knowledge base. Third, psychologists supporting CI operations throughout DoD must look to, and prepare for, the future of this applied discipline. It is vital that psychology find a way to attract the next generation of the best and the brightest to direct their careers to CI-related endeavors, to thoughtfully confront the myriad ethical challenges certain to arise in any new practice arena, and to nurture and guide this fledgling field into its next stage of development.

REFERENCES

- American Psychological Association. (2005). *Report of the presidential task force on psychological ethics and national security*. Washington, DC: Author.
- Borum, R. (2004). *Psychology of terrorism*. Tampa: University of South Florida.
- Borum, R. (2006). Approaching truth: Behavioral science lessons on educing information from human sources. In R. Fein (Ed.), *Educing information: Science and art in interrogation—Foundations for the future* (Intelligence Science Board Study on Educing Information Phase 1 report). Washington, DC: National Military Intelligence College Press.

- Borum, R., Fein, R., Vossekuil, B., Gelles, M., & Shumate, S. (2004). The role of operational research in counterterrorism. *International Journal of Intelligence and Counterintelligence*, 17, 420–434.
- Borum, R., & Gelles, M. (2005). The operational and organizational evolution of Al-Qaeda: A behavioral perspective. *Behavioral Sciences & the Law*, 23, 467–483.
- Borum, R., Super, J., & Rand, M. (2003). Forensic assessment for high risk occupations. In A. Goldstein (Ed.), *Comprehensive handbook of psychology: Vol. 11. Forensic psychology* (pp. 133–148). New York: Wiley.
- Crawford, K. S., & Bosshardt, M. J. (1993). *Assessment of position factors that increase vulnerability to espionage*. Monterey, CA: Defense Personnel Security Research Center.
- Cronin, C. (Ed.). (1998). *Military psychology: An introduction*. Needham Heights, MA: Simon & Schuster.
- DoD Directive 5105.67. (2002, February 19). *Department of Defense Counterintelligence Field Activity (DoD CIFA)*. Washington, DC: Department of Defense.
- Ewing, C., & Gelles, M. (2004). Ethical concerns in forensic consultation regarding national safety and security. *Journal of Threat Assessment*, 2, 95–107.
- Executive Order 12333. (1981, December 4). United States Intelligence Activities, Section 3.4(a). EO provisions found in 46 FR 59941, 3 CFR, 1981 Comp., p. 200.
- Fein, R. (Ed.). (2006). *Educing information: Science and art in interrogation—Foundations for the future* (Intelligence Science Board Study on Educting Information Phase 1 report). Washington, DC: National Military Intelligence College Press.
- Gelles, M., Borum, R., & Palarea, R. (2005). *Fundamentals of Jihadism: Behavioral considerations for developing and managing counterterrorism sources*. Washington, DC: Naval Criminal Investigative Service.
- Gelles, M., McFadden, R., Borum, R., & Vossekuil, B. (2006). An approach to the interrogation of subjects of al Qa'ida-related investigations: A perspective for law enforcement personnel. In T. Williamson (Ed.), *Investigative interviewing: Developments in research, rights and regulation* (pp. 23–41). Cullompton, England: Willan.
- Gelles, M., Palarea, R., Arita, A., & Hawkes, C. (2005). *Operational assessment in a changing world: A guide for special agents*. Washington, DC: Naval Criminal Investigative Service.
- Graham, J. (2002). *What the U.S. military can do to defeat terrorism*. Lincoln, NE: Writer's Club Press.
- Herbig, K. L., & Wiskoff, M. F. (2002). *Espionage against the United States by American citizens: 1947–2001*. Monterey, CA: Defense Personnel Security Research Center.
- Johnson, B. (1995). Perennial ethical quandaries in military psychology: Toward American Psychological Association–Department of Defense collaboration. *Professional Psychology: Research and Practice*, 26, 281–287.
- Johnson, B. (2002). Consulting in the military context: Implications of the revised training principles. *Consulting Psychology Journal: Practice and Research*, 54, 233–241.
- Kipp, S. (2001). *Espionage and the insider*. San Francisco: SANS Institute.
- Kramer, L., Heuer, R., & Crawford, K. (2005). *Technological, social, and economic trends that are increasing U.S. vulnerability to insider espionage*. Monterey, CA: Defense Personnel Security Research Center.
- Lowenthal, M. (2003). *Intelligence: From secrets to policy*. Washington, DC: CQ Press.
- Matsumoto, D. (Ed.). (2001). *The handbook of culture and psychology*. New York: Oxford University Press.
- National Security Agency. (2001). *Espionage: The threat is real*. Washington, DC: Author.
- Office of the National Counterintelligence Executive. (2005). *National counterintelligence strategy of the United States*. Washington, DC: Author.
- Olson, J. (2001). The ten commandments of counterintelligence. *Studies on Intelligence*, 11, 81–87.
- Page, G. (1996). Clinical psychology in the military: Developments and issues. *Clinical Psychology Review*, 16, 383–396.

- Saraswati, T. (Ed.). (2004). *Cross-cultural perspectives in human development: Theory, research, and practice*. Thousand Oaks, CA: Sage.
- Shaw, E. D., Ruby, K. G., & Post, J. M. (1998). *The insider threat to information systems* (Security Awareness Bulletin No. 2-98). Washington, DC: Department of Defense Security Institute.
- Smith, E. (1990). The spies among us: Trends in military espionage. *American Intelligence Journal*, 11, 1-3.
- Thompson, T. (2001). Security and motivational factors in espionage. *American Intelligence Journal*, 20, 47-56.
- Wettering, F. (2000). Counterintelligence: The broken triad. *International Journal of Intelligence and Counterintelligence*, 13, 265-300.