2013-05-20

Indications and warning in an age of uncertainty

Wirtz, James J.

Routledge, Taylor & Francis Group

International Journal of Intelligence and CounterIntelligence Volume 26, Issue 3, 2013
http://hdl.handle.net/10945/47539

International Journal of Intelligence and CounterIntelligence, 26: 550–562, 2013

ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2013.780558

Routledge
Taylor & Francis Group

JAMES J. WIRTZ

Indications and Warning in an Age of Uncertainty

Indications and warning intelligence is an important and time-tested methodology employed by intelligence analysts to warn military officers and policymakers about changes in an opponent's operational ''posture'' which indicate that the likelihood of dangerous or aggressive activity is increasing. In recent times, it has fallen out of fashion because policymakers and the public alike have come to expect that the Intelligence Community will be able to provide ''specific event predictions'' of an opponent's future actions. In other words, people tend to believe that intelligence analysts should be able to state who is about to undertake some unwanted activity, as well as where, how, when and why the action will unfold.

Another expectation is that these specific event predictions will be offered early enough so that policymakers and operators can take effective action to prevent the occurrence of some nefarious act or attack. Specific event prediction is indeed the ''holy grail'' of intelligence analysis, and analysts sometimes do manage to warn of specific events before they unfold. In 1942 naval intelligence analysts predicted the Japanese attack on Midway.

Dr. James J. Wirtz is Dean of the School of International Graduate Studies and former Chairman of the Department of National Security Affairs at the Naval Postgraduate School, Monterey, California. A former Chairman of the Intelligence Studies Section of the International Studies Association, he was President of the International Security and Arms Control Section of the American Political Science Association. A graduate of the University of Delaware, with a Ph.D. from Columbia University, New York City, Dr. Wirtz is the author and co-editor of several books on intelligence and arms control.

The Intelligence Community detected Soviet efforts to place medium range missiles in Cuba before these actions became a *fait accompli*.[1] But for theoretical, bureaucratic, and cognitive reasons, specific event prediction is extraordinarily difficult to achieve in practice. Success tends to be the exception, not the norm.

Indications and warning intelligence offers a powerful and important alternative to a focus on specific event prediction that might in fact be better suited to contemporary threats posed by non-state actors or rogue regimes. To be effective, however, both analysts and policymakers must understand the philosophy and methodology that animates indications and warning intelligence. They not only have to comprehend its strengths and limitations, but they must also understand the part they have to play to best utilize indications and warning intelligence to deter or defend against an opponent's pending initiatives.

INDICATIONS AND WARNING INTELLIGENCE DEFINED

Indications and warning intelligence is an effort to identify and monitor changes in an opponent's operational posture by assessing whether or not the opponent's military units or other types of operational capabilities are in a "day alert" or "generated alert" status. Day alert represents a normal, or peacetime, status in which assets are maintained in a routine posture and are not highly capable of being used to conduct offensive operations or even any significant operation at all. By definition, most military or police units are usually in a day alert status—their activities are centered on undertaking routine maintenance, training, or other activities required to preserve the potential for real operations. Each organization also possesses a unique day alert posture because bureaucratic procedures, equipment maintenance demands, funding cycles and personnel practices combine to create routines and patterns of activity that are not easily broken. At any given moment in time, for instance, about two-thirds of the ships in the U.S. Navy are in port undergoing routine maintenance or major overhauls that are planned years in advance, which would suggest that the day alert status of the U.S. Navy corresponds roughly to a situation in which thirty percent of available assets at any given time are deployed at sea and are capable of undertaking military operations.

In contrast, a generated alert status represents a break with this normal peacetime pattern of activity. It constitutes a halt in routine and instead focuses on making the largest possible force available to undertake operations. Maintenance and other housekeeping measures are curtailed and deferred as units take up attack positions or are otherwise postured to undertake actual operations. The process of force generation generally follows a bell curve—as a majority of a force is brought up to operational

readiness, its capability tends to peak for a limited period of time and then begins to diminish as deferred maintenance and other housekeeping requirements tend to reduce operational capabilities. The decision to generate forces thus implies real costs that will have to be paid in the form of reduced operational capabilities in a future day alert posture since units are then forced to complete deferred maintenance and other routine matters that were ignored during the generated alert. The fact that the act of generating forces is not without long-term operational costs and risks is extraordinarily important because it ties the operational decision to generate forces with the fundamental strategic and political calculations of the government or non-state actor that places its units on a state of maximum readiness.

The movement of forces from a day alert to a generated alert status often creates a string of observable actions that can be detected by the collection efforts of oppositional intelligence agencies. For military formations, leaves are cancelled and reservists are mobilized, units depart bivouac and move to staging areas, command and control networks are activated, and even rumors about impending military action begin to circulate among civilian populations and government agencies. In terms of non-state actors such as criminal organizations or terrorist cells, deviations can be observed in what constitutes normal activity as efforts begin to focus on launching initiatives, not simply maintaining clandestine cells. Chatter on Internet-enabled terrorist networks might increase as coded messages are relayed to fellow travelers leaving them to prepare to face enhanced law enforcement activities and making a break with ''peacetime'' command and control procedures. Talk which can be picked up by informers might begin to circulate within criminal or terrorist circles about the increased likelihood that a major operation is about to unfold. Paradoxically, the very absence of signals of normal activity can also suggest a sharp increase in operational security that could indicate that military forces or terrorist and criminal organizations are attempting to hide last minute preparations to stage a significant operation. The absence of chatter on Internet networks or indications that routine activities have been inexplicably curtailed can serve as important signals that the opponent might be changing its readiness posture. Both the presence of unique signals or the absence of routine signals—the presence or absence of data—can serve as important indicators that an opponent is moving from a day alert to a generated alert status.

Indications and warning intelligence is thus focused on detecting changes in the operational posture of the opponent in order to provide an alert that the likelihood of dangerous or otherwise unwanted activity is increasing. It is a continuous effort to reassess the likelihood of enemy action over the short-to-medium term (days or several weeks). While not

necessarily intended to estimate exactly what is about to unfold, it is instead intended to warn policymakers, military and intelligence officers, and law enforcement officials that the threat they face is increasing. In this sense, it is not a single event prediction, but a risk assessment that can be used to alert military forces to move to a heightened state of defensive alert or to inform law enforcement officials that the time has arrived to implement heightened security procedures. This type of information is crucial because military organizations and law enforcement cannot indefinitely operate on maximum defensive alert. Thus, indications and warning intelligence must be tied to appropriate action on the part of the recipient in order to increase defenses or security activities to meet an attack or, better yet, to have a deterrent effect on the party contemplating some nefarious activity. If the success of an attack depends on a complacent opponent, indications and warning intelligence that is followed by a change in defensive posture can deter or derail an attack or some other undesirable action.

THE TRADITIONAL VIEW

During the Cold War, the U.S. Intelligence Community devoted vast resources to monitor the status of Soviet conventional and nuclear forces in an effort to provide warning of nuclear attack against the United States and its allies or a Warsaw Pact offensive against the North Atlantic Treaty Organization (NATO). For individual analysts to be given responsibility for the day-to-day monitoring of individual Soviet military formations or key parts of its strategic nuclear force was not uncommon. Checklists were drawn up to help analysts monitor routine ''life-cycle events'' (e.g., maintenance and training activities) so that anomalies in normal patterns of activity could be identified for additional analysis. By subjecting previous findings to continuous scrutiny, minor alterations in behavior could be analyzed in the search for evidence of a gradual change in readiness that might constitute a pattern of denial and deception intended to lull an observer into a false sense of security that was intended to bolster a clandestine movement toward generated alert. If changes were detected, warnings could be delivered through dedicated communication channels directly to officials and officers who possessed a series of pre-planned responses to meet specific warnings or changes in the opponent's day alert posture.

This traditional use of indications and warning intelligence was facilitated by several factors that emerged during the sustained confrontation between the Soviet Union and the United States during the Cold War. The likely, and most threatening, dangers posed by the USSR were understood and generally accepted across the Intelligence Community. The Warsaw Pact posed a threat of a massive conventional nuclear attack across the

inter-German border along recognized invasion corridors that permitted the movement of large armored formations (e.g., the Fulda Gap). The Soviet Union also posed a threat of nuclear attack by sea-based and land-based ballistic missiles and long-range bombers following a period of force generation that was intended to strike a devastating blow against U.S. strategic nuclear forces, limiting the damage they could inflict against the USSR in a retaliatory strike.

Deviations to these general threats were also identified and understood. In Europe, analysts recognized that the Soviets might launch a ''standing start'' attack under the guise of a large exercise without placing the entire Warsaw Pact on generated alert, seeking to capitalize on the element of surprise in a mad dash to the English Channel. In the strategic nuclear realm, the Soviets also retained the capability of launching a ''bolt-from-the blue'' attack by utilizing capabilities available on day alert in an effort to destroy a significant portion of the U.S. nuclear force caught on its bases in a day alert posture. But even these ''day alert'' deviations in Soviet strategy were subjected to indications and warning analysis. Analysts not only monitored signs that the Soviets were generating their forces to launch an all-out attack, they also searched for evidence that the Soviets were preparing to launch standing start or bolt-from-the-blue attacks from a day alert posture. Indications and warning methodologies were institutionalized by developing standard procedures within the Intelligence Community and pre-planned responses to warnings issued across dedicated communication channels. A conscious effort was made to get within the opponent's ''decision and operation cycle,'' so that a response to warning could actually outpace the other side's preparations for attack.

The fact that large forces faced each other across the Cold War divide actually facilitated indications and warning intelligence because even small changes in their alert status tended to generate signals that were not easily concealed or ignored. Sustained interaction and collection and analysis activities over decades also led to a deep understanding of what actually constituted a normal ''day alert'' posture. Conventional and strategic arms control negotiations facilitated understanding of the opponent's doctrines and standard operating procedures by increasing transparency. The fact that both sides also relied on similar military technology produced an abundance of technical and operational expertise that enhanced the analytical process—U.S. Army officers with experience in armored operations, for instance, provided a ready supply of technical and operational knowledge when seeking to understand Soviet armored operations and doctrine. Because both countries relied on large bureaucracies to produce their military capabilities, organizational behavior provided an additional commonality in practices and procedures that were easily recognizable across the ideological divide of the Cold War.

That ''bureaucratic politics'' was a major area of practical and theoretical interest within the U.S. academic and policymaking communities during the 1960s and 1970s was no coincidence because it did much to explain operational, procurement, and doctrinal forces that shaped the activities and initiatives of military organizations.[2] Organizational behavior was the dominant explanation used to account for ''irrational consistency'' on the part of Soviet military organizations in the face of a changing political, strategic and technological environment.[3] The shared history of strategic interaction that emerged during the Cold War also facilitated indications and warning intelligence because it created reference points that could be used as a benchmark for Soviet responses to various kinds of incidents, creating a basis for diplomatic and military-to-military contacts that increased transparency into Moscow's motives and alert decisions. The fact that the analytic assumptions behind the assessment of Soviet procurement decisions, day alert postures, and doctrine were subjected to sustained academic, intelligence, and policy debate guaranteed that the basis of indications and warning methodologies were subjected to continuous revision and refinement.

THE CONTEMPORARY SETTING

Since the end of the Cold War, indications and warning intelligence has no longer been a leading element of the tradecraft employed by the U.S. Intelligence Community, although it is still highlighted as an important analytical technique by leading intelligence scholars and practitioners.[4] This probably relates to the fact that indications and warning intelligence is apparently linked to its Cold War applications, and seems unsuited in the minds of many to address current threats posed by non-state actors or rogue regimes whose behavior appears highly unpredictable and difficult to track using existing collection techniques.

Two objections are often mentioned in negative assessments of the ability of indications and warning methodologies to address contemporary threats. First, contemporary threats, especially those posed by non-state actors, are sometimes said to fail to generate signals of sufficient strength, novelty, or significance to be subjected to analysis using traditional indications and warning techniques. Admittedly, the signals generated by a clandestine terrorist cell that is about to launch an attack are different than the signals created by several armored corps as they move out of their bases towards forward attack positions. Nevertheless, terrorist organizations or criminal syndicates also generate discernible signals when they too shift from day alert to generated alert in the days and weeks proceeding an actual operation. The Intelligence Community can discern these signals. As the *9/11 Commission Report* stated, the ''system'' was ''blinking red'' in the

summer of 2001, highlighting the fact that intelligence officials and policymakers had detected a significant change in al-Qaeda's operations that suggested that an action, directed against the airline industry, was increasingly likely.[5] Even before the 11 September 2001 (9/11) terror attacks against the Pentagon and the World Trade Center, the Intelligence Community was capable of monitoring changes in the status of terrorist organizations and other non-state actors.

Second, the belief is that the threats posed by non-state actors are so novel and unpredictable that identifying likely avenues, methods, and targets of attack is impossible. In other words, unlike the Cold War, where invasion corridors were known and the nature of the danger seemed obvious, the threats posed by non-state actors now appear too diabolical and innovative to be anticipated in advance. But the idea that intelligence analysts and policymakers lack the requisite imagination to anticipate probable threats is also a bit of a red herring. The motives and modus operandi of clandestine networks are usually well known, and are sometimes even announced by non-state actors who wish to bolster political support for their objectives. Also true is that non-state actors' behavior is not constrained by the standard operating procedures or regulations of state actors that rely on bureaucracy to generate military power. Nevertheless, the exigencies of operating clandestinely and the sheer difficulty of undertaking significant action with limited resources channels their behavior and initiatives along relatively predictable paths.[6] Al-Qaeda's preference for the use of explosives and its interest in targeting transportation networks remained a feature of the organization both before and after the 9/11 attacks.

Rationality Bias

By contrast, several less well-recognized issues have emerged that tend to complicate the contemporary use of indications and warning techniques. The perceptions of analysts and policymakers alike are often shaped by a rationality bias when it comes to assessing the likelihood of some potential threats. Often the actions of non-state actors or rogue regimes appear "hare-brained" or bizarre *ex ante* because they seem to lack either strategic or political purpose, or appear extremely unlikely to yield significant effects, especially against mobilized national defenses or the law enforcement establishment.[7] Analysts thus have difficulty in making a convincing case to themselves or to policymakers that significant and costly responses must be made to what appears to be far-fetched or ill-conceived plans that seem to offer little prospect for success.

This perception, in turn, exacerbates a fundamental dilemma inherent in the political decision to respond to warning. Specifically, contemporary

threats often appear vague, probabilistic, and highly unrealistic, while the costs of response are known, high, and certain.[8] Policymakers are thus forced to bear real political and financial costs to head off possible threats that appear from their perspective *ex ante* as ludicrous or strategically unsound for the party launching the initiative. This dilemma is compounded by the fact that policymakers often prefer ''all or nothing'' responses to warnings—they want options that are guaranteed to head off the threat detected by analysts. However, for analysts to supply this guarantee is virtually impossible because indications and warning methodologies do not yield a specific event prediction, which prevents them from determining if a potential response will deter or defeat an attack before it occurs.

As a result of the tradeoffs involved, policymakers sometimes adopt a ''wait and see'' attitude in responding to warnings of an apparent change in the alert status of the operational units of non-state actors. A wait and see attitude, however, undermines the effort to get inside the opponent's decision and operational cycle—a defensive response has to be undertaken before an opponent is fully prepared to launch some initiative if indications and warning techniques are to yield their greatest benefit.

Another issue that complicates the contemporary use of indications and warning methodologies is the fact that non-state actors and (sophisticated) rogue regimes are likely to direct their attacks or initiatives against the military or security weaknesses of their opponents. This would suggest that contemporary indications and warning methodologies must incorporate a net assessment on the part of analysts and policymakers when it comes to responding to changes in the alert levels of opponents' units. In other words, analysts and policymakers must have some awareness about the ability of non-traditional targets and civilian infrastructure to respond effectively to warning, and not simply assume that changes in opponents' alert levels will meet with an appropriate response. For instance, as some of the al-Qaeda terrorists boarded aircraft on the morning of 11 September 2001, they did draw attention on the part of airline personnel, but the security procedures triggered were inappropriate to the threat they faced.[9] Perhaps when warnings are issued to policymakers they should be accompanied by some form of assessment as to why the increased threat is particularly alarming, in the sense that it may be directed at targets that are ill-prepared to deter or defeat an attack.

Benefits From Warnings

Several observations can be offered about the threats posed by emerging non-traditional forces (i.e., terrorist cells, criminal networks, rogue regimes) in relation to the benefits offered by indications and warning

analysis. Compared to the signals generated by the large rival military bureaucracies that were subjected to scrutiny during the Cold War, the signals generated by non-state actors are limited in number and relatively faint. At the same time, the resources available to non-state forces are also limited compared to state elements, and their operations are constrained by the availability of only minimal resources and the exigencies of clandestine operations. Moreover, their operations must be undertaken on the finest of margins because any effort to devote additional material resources or personnel simply increases the probability of detection by opposing intelligence agencies. Clearly, too, ideology, culture, and expertise—to say nothing of their political agenda—make discerning their modus operandi and operational objectives relatively easy. The fact that aggressors must attack an opponent's weaknesses and not its strengths in order to generate a significant political impact can also be used as a guide to understand likely threat vectors. When subjected to sustained collection and analysis, monitoring the day-to-day activities of non-state actors is theoretically possible in seeking to understand what in fact constitutes their ''day alert'' status, and to detect subtle changes in the signals they generate to warn that they are in fact moving to a ''generated alert'' posture. In other words, detecting the threat posed by non-state actors when compared to state actors is somewhat more difficult. But given the more limited nature of the threat constituted by non-state forces, the suggestion is that more limited responses might be sufficient to deter or defeat the threats they pose.

TOWARDS A MODERN INDICATIONS AND WARNING CAPABILITY

Indications and warning methodologies are based on key concepts and assumptions that must be understood and accepted by analysts and policymakers. Foremost among these assumptions is that indications and warning intelligence does not necessarily yield specific event predictions, only indications that the threat posed by some opponent is increasing. If commanders or policymakers insist on receiving specific details about what is about to transpire, or responses guaranteed to head off an attack, or compelling explanations for why an opponent is about to undertake an extremely counterproductive initiative, then warnings are likely to yield few positive results. If analysts wait until the situation unfolds to the point where answers can be offered to these questions, it will likely be too late to respond effectively. Analysts and policymakers must overcome the dilemma inherent in indications and warning methodologies—they must devise a way to overcome policymakers' preference for an ''all or nothing'' response when it comes to selecting a response to warning.

Indications and warning intelligence is also based on the detection of anomalies, which requires sustained analysis so that patterns of activity

that reflect ''normalcy'' can be identified. In the absence of a clear conception of expected behavior and well-defined checklists of warning indicators, however, indications and warning methodology can still provide a valuable service because it can serve as a way to direct scarce collection and analytical resources towards individuals, groups, facilities, organizations, or military units that appear to be engaging in unusual activity or that are failing to exhibit the signals expected by normal patterns of activity. Investigators who arrive at some facility might in fact find perfectly innocent and compelling explanations for the emergence of some anomaly, but anomalies require additional analysis because they offer a good way to penetrate denial and deception techniques employed by state and non-state actors. Detecting anomalies among individuals or groups might appear impossible to achieve, but the al-Qaeda operatives involved in the 9/11 terror attacks left signals that were in fact detected by their flight instructors, which were subsequently discussed within the Federal Bureau of Investigation (FBI). The fact that the law enforcement or intelligence communities did not investigate why groups of foreign students from the Middle East were interested in learning how to fly, but not necessarily land, aircraft suggests that both analysts and policymakers alike failed to recognize what actually constitutes raw intelligence and warning data.[10]

Available Threat Responses

Once anomalies are detected, policymakers must understand the range of appropriate responses available to respond to heightened threats. At a minimum, they need to understand that a change in defense and security postures can derail an opponent's plans. A change in defense posture can deter an opponent from taking undesirable action because it can deny the opponent the element of surprise needed to achieve a *fait accompli*, which changes the strategic setting in a way that makes existing deterrent threats less relevant. A change in security postures can also delay some nefarious scheme concocted by a non-state force because it negates the assumptions behind some finely crafted plan that is intended to exploit weaknesses in day alert security procedures intended to safeguard critical infrastructure or vulnerable aspects of civil society. Delay also provides law enforcement with the additional time needed to investigate leads and to explore anomalies detected in the behavior or status of non-state actors, providing an opportunity to disrupt activities by identifying and detaining the individuals who are key to impending operations. Because non-state aggressors are forced to undertake operations on the finest of margins, a change in defensive and security operations should force them to reassess planned operations in order to guarantee their effectiveness even against new defense postures or security procedures. In this sense, time is on the

side of the defense forces because a ''mission kill'' provides the opportunity for law enforcement or intelligence agencies to target key parts of the opponent's infrastructure, which can ultimately eliminate the threat.

Because small changes in defensive and law enforcement postures can deter a potential attack or produce a mission kill against initiatives launched by non-state actors, indications and warning intelligence can overcome policymakers' preferences for an ''all or nothing'' response to warning. Intelligence analysts need no longer present policymakers with specific event predictions that identify exactly what is about to unfold or offer a compelling explanation for why an opponent is about to undertake some actions that appear *ex ante* as strategically ill-advised or self-destructive. Instead of requiring policymakers to adopt costly and extreme responses to potential threats, analysts have to request only relatively modest changes in defense and security postures to deny the opponent the element of surprise, or to derail an opponent's plans that are crafted to meet specific strategic settings. By reducing the anticipated costs of a response to potential threats, intelligence analysts can increase the probability that policymakers will undertake changes in defense and security postures needed to deter or derail threats. For example, a modest change in airline security procedures before the 9/11 terror attacks might have forced the al-Qaeda operatives to reevaluate their plans to ensure that they would not run afoul of airline security. The Japanese fleet moving towards Pearl Harbor in December 1941 had instructions to abandon its operations if it lost the element of surprise. Ultimately, indications and warning techniques offer the possibility of deterring attack by increasing defensive readiness, a metric that might constitute a new ''holy grail'' for intelligence professionals.

OVERCOMING STUMBLING BLOCKS

Indications and warning methodologies comprise a significant tool that offers important ways to organize strategic responses to today's threats. Together they offer important insights into collection techniques, suggesting the importance of long-term research in developing a broad awareness of emerging threats. They also offer a way to direct more focused collection efforts to investigate anomalies in the known patterns of behavior of both state and non-state actors. For analysts, indications and warning methodologies also offer a way to defeat an opponent's efforts at denial and deception by highlighting the collection and analytical techniques needed to investigate and explore anomalies that emerge. Indications and warning methodologies also offer a way to overcome response dilemmas and the general reluctance of policymakers to incur substantial and known costs in response to possible threats that appear

ex ante as unrealistic or ill advised. In effect, indications and warning methodologies offer a strategic way to organize national intelligence and response efforts across the entire intelligence, defense and security enterprise.

Although indications and warning methodologies offer a constructive response to today's security challenges, they have clearly have fallen out of fashion among intelligence professionals. In part, indications and warning is often viewed as better suited to a different setting—the prominence of the technique during the Cold War might make it appear as unresponsive to present circumstances. As a result, intelligence managers and policymakers have failed to consider how indications and warning techniques can be applied to meet today's challenges. Another stumbling block is the fact that indications and warning methodologies have to be implemented across the entire intelligence cycle—collection, analysis, and response—in order to be effective. Because few mechanisms are available to organize and inform both intelligence professionals and government officials about their roles in the indications and warning process, indications and warning is unlikely to experience a resurgence as a key instrument of intelligence and strategic policy.

The failure to consider and apply indications and warning methodologies in the effort to exploit the opportunities for collection and analysis created by the information revolution is especially unfortunate. Nevertheless, indications and warning remains as an important and effective tool in the national effort to avoid surprise, and to deter opponents who seek to exploit defense and security weaknesses to achieve their objectives.

REFERENCES

[1] In the words of Sherman Kent, photographic evidence of efforts to deploy Soviet medium-range ballistic missiles in Cuba was a ''moment of splendid,'' Kent quoted in Loch K. Johnson, *National Security Intelligence* (Cambridge: Polity, 2012), p. 50.

[2] Some scholars even suggested that the use of similar military technology and the reliance on large bureaucracies was leading to a process of ''convergence'' between the United States and the Soviet Union. In other words, the need to exploit similar technologies via large bureaucracies was leading to the adoption of similar standard operating procedures, technical solutions and military doctrines when it came to the military competition between the Superpowers. See Zbigniew Brzezinski and Samuel P. Huntington, *Political Power: USA/USSR* (Westport, CT: Greenwood Press, 1982).

[3] The best known of these studies was Graham Allison, *Essence of Decision* (Boston: Litle Brown, 1971).

[4] Richards J. Heuer, Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis* (Washington, D.C.: CQ Press, 2011).

[5] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: Norton, 2004), p. 254.

[6] For a description of how the exigencies of a covert or clandestine existence shape the operations of non-state actors see J. Bowyer Bell, ''Conditons Making for Success and Failure of Denial and Deception: Nonstate and Illicit Actors,'' in Roy Godson and James J. Wirtz, eds., *Strategic Denial and Deception: The Twenty-First Century Challenge* (New Brunswick, NJ: Transaction, 2002), pp. 129–162.

[7] James J. Wirtz, ''Theory of Surprise,'' in Richard K. Betts and Thomas G. Mahnken, *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel* (London: Frank Cass, 2003), pp. 101–116.

[8] According to Jack Davis, policymakers are acutely sensitive to the ''wrenching shift in defensive resources that would be required if . . . warnings were taken seriously,'' see Jack Davis, ''Strategic Warning: Intelligence Support in a World of Uncertainty and Surprise,'' in Loch K. Johnson, ed., *Handbook of Intelligence Studies* (New York: Routledge, 2007), p. 186.

[9] *The 9/11 Commission Report*, p. 1.

[10] *Ibid.*, pp. 272–276.