The Changing World of Contemporary Terrorism and 'Intelligence Failures'

ARPAD PALFY

"Warning is a necessary but insufficient condition for avoiding surprise"
Richard K. Betts

The events of September 11th are likely to remain etched in our common memories indefinitely. It is therefore important that governments and societies recognize their responsibility to explore ways of preventing similar occurrences from happening in future. In doing so, analysis should remain as objective as possible and focus on *all* of the possible variables which may have led to such a horrific outcome. Hence, it is critical that the full range of possibilities, outside of those citing 'intelligence failure' as the main culprit, also be carefully examined.

Although all the details surrounding September 11th are not yet known, presently available information seems to indicate that intelligence officials did in fact receive and transmit some warnings of impending terrorist activity, but were vague or unclear as to the precise time and location of a possible attack.[i] While such a deficiency may have been circumvented by a greater capacity in terms of human intelligence,[ii] the lack of such specifics does not necessarily indicate an intelligence failure *per se*.

This paper argues that the precise role of intelligence, in terms of a craft as well as a state asset or resource, should not be viewed as a crystal ball capability or as a predictor of specific events, but rather as a state decision-making tool. Second, it demonstrates that the contemporary security environment related to terrorism and terrorist organizations is more fluid, as terrorist groups have become organizationally and functionally adaptive to their operational environments when compared to more traditional groups. Invariably, these realities may initially manifest themselves in a proportionally higher number of surprise attacks as both intelligence organizations and governments attempt to adapt to such circumstances. These two points will also emphasize why September 11th should not necessarily be seen as the intelligence failure it has been branded by some analysts.

Furthermore, the multiple terrorist incidents leading up to September 11th, such as the 1993 bombing of the World Trade Center, the Oklahoma City bombing in 1995, and the attack on the American Embassies in 1998, coupled with a significant increase in counter-terrorist budgetary allocations, totaling $19 billion in early 2001, seemed to indicate that the US Government was well aware of, and sensitive to, the possibilities of a serious attack occurring.[iii] Its lack of definitive response in terms of legislation and preparedness, despite such events, may perhaps indicate the presence of deficiencies outside of the intelligence sector.

The conclusions of this study are that the frequently misused term of 'intelligence failure' is often automatically associated with the mere occurrence of a surprise attack, rather than as a result of an examination determining whether or not the mechanisms of the intelligence process functioned as intended. Analyzing the relationships between intelligence, terrorism, and state decision-making processes is crucial if governments are to develop new procedures and policies, or reorganize old ones, in hopes of preventing future occurrences. Citing intelligence failures following a surprise attack, without exploring the full range of possible reasons *behind* the occurrence, may potentially lead to further complications, reoccurrences, or the inadvertent exchange of one set of problems for another.

Intelligence and the Concept of Failure

Varying definitions of intelligence in both academic and government circles abound. While most analysts and authors acknowledge the presence of a critical relationship between intelligence and the decision-making process, few of them include it as a defining characteristic of intelligence. For instance, Sherman Kent defines intelligence as a kind of knowledge, a type of organization producing and providing such knowledge, and as the activities undertaken by organizations in the pursuit of such knowledge.[iv] While adequately qualifying the term in delineating its responsibilities and activity, the three facets listed provide only partial clarity as to the ultimate function or role occupied by intelligence as a decision-making tool. Though considered implicit to some, the production of this knowledge does not occur simply for its own sake. The media and general public sometimes tend to artificially separate the term from its more definitive purpose as an aid to decision-makers. This tendency is what most often leads critics to erroneous assessments when examining the occurrences of intelligence failure.

The term ‘intelligence failure’ would best be defined as the malfunctioning of one or more aspects of the intelligence process or cycle. In other words, the activities corresponding to the procedural means of organizing, gaining, understanding, reviewing and forwarding the ‘knowledge’ produced by a given organization; more specifically the steps of planning and preparation, collection, evaluation and analysis, production, and dissemination. This definition would be better suited to analyses examining possible intelligence failures, because it allows for a clearer distinction between intelligence, as defined, and its eventual *purpose* as a decision-making asset.

Though not incorporated into his definition, Kent emphasizes the importance of the intelligence decision-making relationship as a critical aspect of its raison d'être. While highlighting that state decision-makers are responsible for ensuring proper guidance of intelligence organizations, he also emphasizes that intelligence remains ancillary to government objectives, policy formulation, and the carrying out of operations as it can and should only perform the service function it was designed for.[v]

The implications of this producer-consumer relationship are manifest in pre and post intelligence cycle occurrences. Although the intelligence cycle incorporates its own planning and preparations stage, guidance from the end-user prior to the cycle's commencement is required in order to ensure direct applicability of the final product. When the finished product is disseminated, and the intelligence cycle is completed, the onus of responsibility falls back onto the decision-maker as to the proper interpretation and use of the intelligence provided.

The types of possible failures leading to surprise attack are demonstrated by the manner in which the described purpose of intelligence interacts with the decision-making process or decision maker. In other words, how the end users or policy makers receive, interpret and employ the intelligence provided can shed considerable clarity on the *type* of failure being examined. Factors such as a possible lack of trust between the client and provider or, the refusal by the decision maker to accept or act upon intelligence provided which is seen as contradictory to an established set of preconceptions regarding a given issue, can all have an impact on the use and interpretation of the intelligence product.[vi]

While all of these pre- and post-dissemination factors, if unforeseeably allowing for the occurrence of a surprise attack, may incite accusations of intelligence failure, the fact that they occurred prior to or following the completion of the intelligence cycle would indicate otherwise. Therefore, intelligence processes and organizations may be mistakenly held accountable for outcomes of situations, actions, non-events or in-actions, following their fulfillment of responsibilities to the user(s).

In the event that intelligence failures do occur, the reorganization of the intelligence system, or of a particular agency, has often been highlighted as a means of preventing future occurrences of a similar nature. Historically, the American intelligence community has undergone several such changes throughout its existence, in an attempt to reduce the likelihood of future surprises or failures. These endeavors at organizational restructuring, however, have seldom provided for the absence of intelligence failures following their implementation; hence, the assumption that intelligence reorganization *alone* will reduce the likelihood of future intelligence failures is unfounded.[vii]

Because "warning is a necessary but insufficient condition for avoiding surprise",[viii] a follow-up to an intelligence warning is absolutely necessary if surprise is to be avoided. To clarify, the surprise attack by North Korea in 1950 can be interpreted as a policy or decision-making failure, rather than an intelligence one. Although the pre-intelligence cycle guidance from decision-makers was accurate in directing intelligence to monitor Communist movements in Europe and Asia, the post-intelligence cycle acceptance and application of intelligence warnings proved disappointing. The perception at the time, based on the occurrences and provocations the preceding year, were that North Korean forces would continue their limited border incursions without venturing any further south.[ix] President Truman's memoirs indicate that while Central Intelligence reports told him that North Korea might invade at any time, and had the capability of doing so, he lacked the information providing him with clues "…as to whether an attack was certain or when it was likely to come".[x] In his defense, however, he adds that such reports were not only limited to Korea, but were relevant to numerous areas around the world where the Russians were also deemed to possess an equally dangerous offensive capacity.[xi] In this case, surprise occurred irrespective of warning and suggested preparations, thus making it a policy rather than intelligence failure.

Conversely, the 1968 Communist uprising in Vietnam, or Tet Offensive, was an exemplary case of intelligence failure. While intelligence analysts did receive increasingly frequent reports indicating a significant enemy build-up and the likelihood of offensive operations, they failed to adequately prepare the decision-makers. The reason behind this failure was an analytical pitfall known as mirror-imaging, which consists of analyzing an opponent's position via one's own perceptions. In other words, a large-scale attack against targets in South-Vietnam seemed nonsensical from an American military commanders' perspective, and thus was dismissed as equally unlikely for the enemy. The analytical foresight required to conceptualize the potential of a political victory, regardless of the military outcome, was non-existent.[xii] Hence, surprise occurred because decision-makers were improperly warned and thus unprepared.

The highlighting of these issues, however, is not intended to suggest that intelligence failures, as the proper use of the term would imply, do not occur; nor does it seek to insinuate that the reformations of intelligence organizations to coincide with present and future security environments not be undertaken when deemed appropriate. Rather, it intends to demonstrate that the mere occurrences of surprise attacks should not automatically or necessarily be associated with the malfunctioning of the intelligence process, as the Korean War case suggests, and that *all* possibilities and relationships be explored if the purpose is to prevent future surprises.

Once these variables are identified, it is vital that they be properly categorized into their respective intelligence or decision-making process camps. This segregation according to purpose and responsibilities should, in turn, theoretically provide a clearer appreciation of the possibly preventable circumstances surrounding the occurrence of a surprise, as well as alleviate future misusages of the term ‘intelligence failure’.

Contemporary Terrorism

Linking the above to terrorism, it is important to highlight that while terrorism’s impact has been considerably amplified by television and other forms of media, the use of terrorism as a tactic is not new.

The current debates over the changing aspects of contemporary terrorism predominantly revolve around its level of perceived lethality in terms of producing large amounts of casualties and its potential selection of weapon systems, such as Weapons of Mass Destruction (WMD). In actuality, contemporary terrorism can be better appreciated in terms of the alterations in organizational structures and concepts, when compared to groups in previous decades, rather than in terms of general strategies. In other words, while the overall strategy of terrorism remains unchanged in its desire to influence an audience beyond the immediate victim, its organizational methods have changed according to the requirements it perceived as necessary to ensuring its own survival, and to circumventing the increasingly complex barriers erected by law enforcement and intelligence organizations. As a terrorist group’s greatest strength lies in its ability to conspire, a proportional relationship exists between this ability and its likelihood of conducting a successful mission.[xiii]

Similar to terrorist groups, intelligence organizations have also undergone considerable changes over the years in order to overcome the terrorist threat. The successes of these developments are epitomized by the subsequent changes witnessed in the terrorist groups themselves. To illustrate, terrorists and governments, including intelligence organizations, are embroiled in a perpetual struggle aimed at defeating the other's operational capacity. As their relationships oscillate in opposite directions, a zero-sum outcome emerges based on the occurrence of a successful outcome for one of the two sides. In other words, a success for one equates to a loss or defeat for the other, and vice versa.[xiv]

The oscillation is caused by the developments taking place on each of the opposing sides as they simultaneously seek to prevent the other from conducting a successful operation. As a result, the mathematical probability of a successful outcome generally tends to favor one opponent over the other, even if only slightly, until new developments emerge re-altering the balance between the two. For example, if hijacking and hostage taking are new tactics developed by a terrorist organization, the probabilities of a successful outcome will be greatest with the first use of this tactic for the terrorist and progressively degenerate in the authorities' favor as they develop adequate counter-measures to deal with them. Once the situation is reversed and the balance is shifted to the defending side, new developments by a terrorist organization are sought in order to defeat these counter-measures and regain the upper hand by instigating a new type of incident unfamiliar to the authorities. Although hijacking is used as an example here, the same may apply to organizational developments, weapon system selection, or any other type of development potentially altering the balance between the competing opponents.

Admittedly, as with all models, this one may seemingly oversimplify reality in its attempt to explain it. However, as it is difficult to quantify and appropriately demonstrate the progressive and developmental relationship between intelligence and terrorism, this model remains a practicable means of examining the basic underlying concepts of this relationship.

The implications of this regenerative cyclical model are three-fold. First, it implies that intelligence organizations, as well policy and decision-makers, will be required to develop a clear understanding of this oscillating relationship when considering innovative ways of dealing with the terrorist threat. Incorporated into this understanding, would also be the recognition by both decision-makers and intelligence organizations of the limited life-span of their policies based on the anticipated counter-developments of the opposing side, as well as a simultaneous appreciativeness of the potential rapidity of adaptation by an opponent to such changes.

Second, this cycle also implies that intelligence failures will undoubtedly occur at some point, particularly when the disparity between the competing entities is the greatest, and balanced in the opponent's favor. If appropriately recognized, this realization can also act as a type of general warning to policy makers of, if nothing else, a period where the mathematical probability of intelligence failures is greater than usual. Although a statement of this nature, to any decision-maker, might be unacceptable, such warnings or identifications of weakness may have significant potential in generating preventative policies aimed at reducing the identified gap.

Third, when intelligence failures do occur, the approximate identification of the position held by the surprised party in relation to its opponent's relative position can, assist in the development of appropriate reorganization policies and/or, aid in the identification of the specific areas *within* the intelligence or decision making processes requiring better adaptation to the unfamiliar threat.

Although both policy and intelligence failures pose an equal future liability in terms of the contemporary terrorist developments highlighted, the recognition of the listed implications is vital if democratic governments are to develop the flexibility required to overcome the advantages presently enjoyed by contemporary terrorism.

While recognizing the prevalence of terrorism's contemporary manifestations, particularly in terms of organizational principles and complexity, it is equally important to note that some methods employed *within* the tactic of terrorism as a whole are and have been reused several times due to their perceived level of operational efficacy in generating favorable outcomes to the perpetrating organization; bombings and assassinations are examples of such enduring tactics. The 2001 events in New York epitomize how an already developed and previously-used method, such as hijacking, can be adapted to new operational scenarios and provide successful results for the perpetrators. Without necessarily binding this study to any particular incident, the type of ingenuity and operational creativity demonstrated by the September 11th attacks are the same principles which have ensured the survival of terrorism as a functional tactic in the minds of those employing it.

The Al-Qaeda organization in particular demonstrates this contemporary manifestation in that it incorporates structural complexity with remarkable flexibility by using loose networks of existing groups and individuals, sometimes developing mission specific organizational or individual affiliations, single-mission or 'one-time-use' terrorists or terrorist cells (including those prepared to commit suicide), and may also make use of flexible and/or ad hoc terrorist cells or cell structures which are activated only a short time before a planned incident.[xv] Another example of this type of development would be Louis Beam's 'leaderless resistance', which comprises no organizational structure to speak of but, rather, a physically disconnected group of like-minded individuals communicating over the internet, or via other means, who are encouraged to undertake any operation against the American government they deem appropriate to their movement. These activities or principles serve the same purpose: ensuring group survivability while defeating the intelligence and law enforcement hurdles impeding potential successes.[xvi]

However, there do remain certain aspects of a terrorist mission which are likely to linger unchanged as the tactic of terrorism itself contains some inherent operational limitations. For instance, while terrorist groups tend to have long-term strategic objectives, they will likely continue to undertake relatively short duration operations as they are incapable of maintaining the initiative once tactical surprise has been achieved. Therefore, extended operations, those lasting more than several hours, will remain somewhat rare as they are less likely to achieve successful results, given that synergy and simplicity are crucial qualities on most terrorist operations.[xvii]

Dealing with the Past

While most facts surrounding September 11th are not yet known, available information seems to show that intelligence officials did receive and transmit some warnings of impending terrorist activity, but were vague or unclear as to the precise date, time and location of the possible attacks.[xviii]

The multiple events leading up to September 11th, such as the first attack on the World Trade Center in 1993; the Oklahoma City Bombing in 1995; the attack on the American Embassies in Africa in 1998; the bombing of the USS Cole in 2000; the foiled attempts aiming to collapse the Lincoln and Holland tunnels in 1993; the downing of 11 American airliners in Asia in 1995; and the attack on the Los Angeles airport during the Millennium celebrations, were all paralleled by the creation of the CIA's Counter-terrorism center (CTC) in the 1980's, the creation of a special section within this center dedicated solely to Bin Laden in 1996, and a significant increase in counter-terrorism budgetary allocations totaling $19 billion by early 2001.[xix] These factors would seem to suggest a pre-incident level of awareness, and sensitivity to, the possibilities of a serious terrorist attack.

Similarly, a lack of definitive action in terms of legislation and preparedness, even in-light of such events, may be more indicative of deficiencies within the policy and decision making processes rather than of ones in intelligence procedure. Irrespective of the fact that some warnings were available, examples of possible actions could have included increasing airport and aircraft security, or developing and overseeing standards related to employment and training of airport screening and security personnel. Others have also highlighted restrictions involved in domestic surveillance operations, and considerations relating to civil liberties, as possible constraints. Secondary considerations may have included air-defense capabilities exceeding the four unarmed fighter planes available to protect the northeastern US at the time. In short, all of the security-related policy developed after the event could have just as easily been researched, developed and implemented prior to it.[xx]

The crux of the argument therefore remains that governments and societies targeted by such threats have a clear responsibility to look past the media and public labels of ‘intelligence failure’ and examine all aspects of the situation, both individually and in relation to each other, in order to prevent this from happening again. In examining and raising some of the issues surrounding recent allegations of ‘intelligence failure’, this paper has sought to accomplish that.

Dealing with the Future

If intelligence organizations hypothetically performed as they were expected, given the nature of contemporary terrorism, will future warnings remain as vague as those preceding September 11th? How can vague warnings be translated into better policy? In short, is there hope?

Increasing the access of intelligence organizations to decision makers may streamline the intelligence decision-making process. Such organizational elasticity, however, should not necessarily reach as far down as the collection process, but may consider access to senior analysts a workable possibility.

It would also be possible to educate decision-makers in the capabilities and functions of intelligence, the nature of the terrorist threat, and the relationship which exists between the two. Such an undertaking might allow intelligence organizations to take an active part in the decision making process by providing ideas for new non-partisan policies geared toward overcoming the competitive intelligence-terrorist relationship.

Similarly, decision-makers should be incited to follow-up with intelligence organizations after terrorist incidents, and review their original decisions and guidance to the organization based on the new developments. Increasing bureaucratic and organizational flexibility would allow governments and intelligence organizations to increase their adaptive capacities to a faster-paced security environment. In this same vein, avoiding cognitive distortions potentially leading to biased interpretations becomes a prime undertaking. Decision-makers should be encouraged to make decisions which they are comfortable amending should the need arise, as the changing threat may alter a policy's applicability and effectiveness. In short, the implications of the oscillating relationship between intelligence and terrorist organizations should be implemented *into* the decision-making process.

Equally important, decision-makers and intelligence organizations must also be aware of the pit-falls of success, such as generating self-negating prophecies. Successful intelligence warnings and subsequent government actions may result in attacks being canceled or altered, and thus may seem to indicate a false sense inactivity. Successes may therefore result in increased complacency, which, in-turn, may increase the likelihood of failure.

Although all suggestions for changes to the system should be examined, Richard Betts points out that the complexity of intelligence organizations, and their relationship with the state, is so great that any suggested change carries an innate risk of producing unforeseen problems or replacing old problems with new ones.[xxi]

In closing, the relationships between intelligence, decision-making and contemporary terrorism are so intricate and far-reaching, that categorizing a surprise event solely as an 'intelligence failure' without making allowances for adjoining factors may potentially prove detrimental in the long run.

[i] Bill Gertz, *Breakdown: How America's Intelligence Failures Led to September 11*(Washington D.C.: Regnery Publishing 2002) pp. 15-17, 21-27 and Richard K. Betts, 'Fixing Intelligence', *Foreign Affairs* 81/1 (Winter 2002), p.56.

[ii] Ibid. pp.166-167 and Betts (note1) p.46.

[iii] Gertz (note 1) p.14.

[iv] Sherman Kent, *Strategic Intelligence for American World Policy*. and Michael Herman, *Intelligence: Power in Peace and War* p.3.

[v] Kent (note 4) pp.180-182.

[vi] Kent (note 4) p.190 and Betts, 'Analysis, War, and Decision: Why Intelligence Failures Are Inevitable'. *World Politics* 31/1 (Winter 1978) p.61.

[vii] Betts (note 1) p. 53.

[viii] Betts, *Surprise Attack: Lessons for Defense Planning* (Washington D.C.: Brookings Institute Press, 1982) p.87.

[ix] Ibid. p.106.

[x] Harry S. Truman, *Memoirs, vol. 2: Years of Trial and Hope*, p.331.

[xi] Ibid.

[xii] Mark M. Lowenthal, "The Burdensome Concept of Failure", in Alfred C. Maurer, Marion D. Tunstall, and James M. Keagle, eds. *Intelligence: Policy and Process*. p.16.

[xiii] Betts (note 1) p. 46.

[xiv] The definition of a terrorist 'success' remains an important debate in academic circles and is therefore not addressed in depth here. However, it is important to consider the implications of a political success versus an operational one. As the Tet Offensive demonstrated, the former is possible even without the presence of the latter.

[xv] Simon Reeve, *The New Jackals: Ramzi Yousef, Osama Bin Laden and the Future of Terrorism*,

pp.179-195. and Yonah Alexander and Michael S. Swetnam, *Usama Bin Laden's Al- Quaida: Profile of a Terrorist Network*. (New York : Transnational Purblishers, 2001).

[xvi] Jeffrey Kaplan, 'The American Radical Right's Leaderless Resistance', *Terrorism and Political Violence* 9/3 (Autumn 1997) pp. 80-95.

[xvii] David C. Rapoport, 'Terrorism and Weapons of the Apocalypse', *National Security Studies Quarterly* 3/3 (Summer 1999) p.51.

[xviii] Betts (note 1) pp.49, 56 and Gertz (note 1) pp. 15-17, 21-27.

[xix] Gertz (note 1) p.14.

[xx] Betts (note 1) p.45.

[xxi] Betts (note 1) pp.43-53.