

The Enemy Achieves Surprise: Are Intelligence Failures Avoidable?

Yengoude EA*

Norwegian University of Life Sciences, Norway

*Corresponding author: Yengoude EA, Norwegian University of Life Sciences, Norway; Tel: +962 6 535 5000; E-mail: erskine.apiiyah@gmail.com

Received date: November 16, 2017; Accepted date: November 24, 2017; Published date: December 07, 2017

Copyright: © 2017 Yengoude EA. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract

While Intelligence Agencies around the world have achieved great feats in intelligence gathering and preventing surprise attacks against nations concerned, the most visible part of their work to the world is the failures that have been recorded in history. Notable among the record in history are the failure of British and American invasion in Iraq to uncover Weapons of Mass Destruction (WMD), the surprise attack by the Japanese against the United States Naval base at Pearl Harbor, the 9/11 Surprise attack against the United States in 2001, the Cuban Missile Crises, etc. These cases of intelligence failure have received several scholarly debates as to why the intelligence community failed in its work to avert the enemy's surprise. The focus of this paper is on the Intelligence Failure of the United States 9/11 terrorist attack in 2001 and the Yom Kippur war of 1973 (also known as the Arab-Israeli War). This paper examines these two cases from a different perspective by analyzing whether the failures in these two cases were avoidable with references made to the conventional causes of the failures in literature. By situating analysis in Betts' theory of intelligence failure, we argue that there are vulnerabilities in the intelligence process which can be located in the context of the structure of organizations (bureaucracy). This analysis reveals that the structure of organizations (bureaucracy) makes them prone to error. Some of the unforeseen vulnerabilities are created out of organizational reforms, communication gaps in the intelligence process and more importantly the overriding self-interest of decision makers which clouds their judgment during decision-making. We conclude that these identified weaknesses are natural to the intelligence process and efforts to perfect the system may only improve the results marginally. Therefore, the intelligence community is not insulated from surprise attacks which make intelligence failure an inevitable phenomenon.

Introduction

According to Lowenthal [1] one of the reasons why nations have intelligence agencies is to avoid being surprised. He explains further stating that to avoid surprise, intelligence communities have to keep track of events and threats that have the potential of endangering a nation's existence. Introducing the term "Intelligence process", he describes it as a schematic model used by Intelligence agencies meant to inform national defense policies and strategy, foreign policy, military operations, international security, etc. Against this background, it is plausible to argue that the success of any defense strategy or military operation depends heavily on what the defender or attacker knows (intelligence) about the enemy in order to avoid being surprised. However looking back into history, events like the surprise terrorist attacks of 9/11 on the United States of America, the Yom Kippur war of 1973, the failure of British and American invasion in Iraq to uncover Weapons of Mass Destruction (WMD) and the surprise attack by the Japanese against the United States Naval base at Pearl Harbor in 1941 have all been cited significantly as a mark of "Intelligence Failure". This paper therefore seeks to discuss the 9/11 surprise attack and the Yom Kippur war of by citing some of the causes of failure by the intelligence community and further providing some analyses of the failure within Betts' theory of intelligence failure in order to establish whether the failures were avoidable.

Definition of Terms

Intelligence

The word "intelligence" is a commonly used term by governments, the media and even individuals at various levels of discussion. Many scholars have attempted a definition of the term but no single definition has been able to capture the entire meaning of the term across specialties. Lowenthal [1] defines Intelligence as the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers; the products of that process; the safeguarding of these processes and this information by counter intelligence activities; and the carrying out of operations as requested by lawful authorities. He further explains intelligence as "issues related to national security-that is, defense and foreign policy and certain aspects of homeland and internal security". A former deputy Director of the Central Intelligence Agency Vernon Walters [2] also described intelligence as "information, not always available in the public domain, relating to the strength, resources, capabilities and intentions of a foreign country that can affect our lives and the safety of our people." First of all, the definitions above clearly draw the line between intelligence and information. Intelligence can be described as processed information, according to the definitions. Also, intelligence is either referred to as a "product" or a "process". Lowenthal's definition describes intelligence as both a process and a product and finally Vernon's addition points it out that intelligence is not easily accessible to everyone or has restricted access.

Intelligence failure

It has also defined as “the inability of one or more parts of the intelligence process-collection, evaluation and analysis, production, dissemination-to produce timely, accurate intelligence on an issue or event of importance to national interest” [3]. Also, in the words of Schmitt [4], an intelligence failure is basically a misconception of a certain phenomenon which causes a government or its security forces to take steps that are unsuitable and detrimental to its own interests. Erik Dahl [5] sums the definitions of intelligence failure by stating that common among all the failure is the element of surprise which is achieved on decision makers and leaders. For the policy maker and other leaders of nations, in order to avoid surprise, they rely on intelligence agencies to give them early warning to avert it. Failure to do so has overarching consequences for the state and its people.

The intelligence cycle

The intelligence Process is the stages through which raw information is processed into intelligence and further made available to policy makers for decision-making. According to Lowenthal [1], the typical intelligence cycle goes through five (5) stages of development. These are Planning and direction, Collection, Processing and Exploitation, Analysis and Production and Dissemination. The planning stage involves the identification of the need for intelligence while the gathering of the raw information required is in the collection stage. Processing on the other hand involves using all resources available to transform raw data into useable information for evaluation and analysis in the next stage. The product (intelligence) after analysis is then given to the final consumer for decision making. It is therefore understandable from the definitions by Lowenthal and Schimdt that intelligence failure can be located within any of the stages in this cycle. This paper will therefore try to look at how failures occur through the intelligence process including other factors that cause this process to malfunction. This will then lead me to answer the central question in this chosen topic: are intelligence failures avoidable?

Analytical Framework

Betts’ theory of intelligence failure

In his contribution towards a theory of intelligence failure, Betts [6] holds decision makers responsible for failure, stating that “the most crucial mistakes have seldom been made by collectors of raw information, occasionally by professionals who produce finished analysis, but most often by the decision makers who consume the products of intelligence analysis.” He believes that it will be misleading to conceive the idea of avoiding disasters through the perfection of procedures and norms because such a venture will only produce marginal results. This leads his theory to categorize the weaknesses in the intelligence process as psychological and political thereby offering a platform for conceptualizing where failures occur and how to address them.

The problem of Intelligence failure according to Betts can be conceptualized in three ways namely Failure in Perspective, Pathologies of Communication, and Paradoxes of Perception. Some failures have received a lot of attention especially if we look at it relegating the ratio of success of intelligence to the background. Indeed, failures are more profound and noticeable while a repelled disaster is almost oblivious. This is what Betts describes as failure in perspective. Pathologies in communication is regarded as the most

common and refers to the communication gaps that bedevils the process of transmitting intelligence to the consumer in order to bring to the notice of the policy maker the relevance of the intelligence at hand. The third and most important is the paradoxes of perception which he describes as the biases and beliefs of the policy maker that impedes them to make objective and accurate decision-making. To Betts, the effort to cure the pathologies identified in the system through reforms to the production of intelligence does not necessarily affect the consumption of intelligence positively due to the presence of the psychological and political factors.

Betts thinks that it is imperative to further break down the problem of strategic intelligence failures to be able to identify the exact paradoxes and pathologies that are extensive in nature. He analyzed them under the headings Attack Warning, Operational Evaluation and Defense Planning. The bane with the attack warning area according to him is the inability to estimate the enemy’s intentions in a timely fashion and being able to convince the authorities with such predictions. Another challenge of policy makers which is discussed under operational evaluation is the inability of policy makers to judge correctly the credibility and reliability of intelligence because they may be inconsistent with current intelligent estimates. Political leaders under this situation have dismissed critical signs even when they represented a majority view of the intelligence community. With defense planning, it is important to note that political leaders use intelligence estimates to inform their policy direction and particularly to determine budget allocations for national policies. Betts [6] notes that, debates over how much to allocate for security conflicts with other national policies and programmes. In fact, during peace time, he recounts that “with competing domestic claims on resources political leaders have a natural interest in at least partially rejecting military estimates and embracing those of analysts who justify limiting allocations to defense programs”.

Betts further identifies one of the obstacles to the effective consumption of intelligence as “wishful thinking, cavalier disregard of professional analyst, and above all the premises and misconceptions of policy makers”. Most cases of failure have been recorded in the stages of interpretation and response in the intelligence cycle. The misapplication of intelligence by policy makers leading to intelligence failures has therefore in most cases been as a result of own biases of policy makers.

Last but not least, Betts draws our attention to the barriers of analytic accuracy which are the ambiguity of evidence, ambivalence of judgment and atrophy of reforms. He notes that ambiguity can be as a result of excessive or conflicting data which carries with it the danger of oversimplification of data by analysts. This further gives room for intuition and guesses during the analysis which can result in intelligence failure. “Where there are ambiguous and conflicting indicators (the context of most intelligence failures), the imperatives of honesty and accuracy leave a careful analyst no alternative but ambivalence”. In the midst of all these inconsistencies, policy makers are prone to the exercise of caution thereby lacking the ability to take decisive steps to solve problems in decisive moments. Atrophy of reforms was used to refer to organizational changes that occur to deal with similar future failures. However, he thinks that organizational structures and bureaucracy still poses as an obstacle to the intelligence function. Intelligence specialist who are more objective have less influence in decision-making while operational authorities who are less objective dominate specialists in organizations. Betts therefore concludes stating that organizational reforms could be made to avert

the problem, however these changes usually persist momentarily and their relevance and effectiveness erode over time.

Betts emphasizes that the prescribed solutions apparently create new vulnerabilities in other areas giving new avenues for intelligence failures. A coping mechanism to ambivalence and ambiguity is to assume the worst in order to treat every threat as serious and genuine (ibid). This according to him reduces sensitivity to actual threats and more importantly a counterproductive and expensive measure. Streamlining the intelligence community in order to co-ordinate analysis has also been mentioned as a solution after intelligence failures. However, Betts notes that the problems of bureaucracy and competition can still create new problems. Another possible solution mentioned is the inclusion of multiple advocacies and the application of devil's advocacy approach. Similarly, Betts argues that multiple advocacies which make use diverse perspectives in analysis can still breed ambiguities. The same can be said for the devil's advocacy which makes use of opposing perspectives. Indeed, a striking option presented by Betts may be said to be the cognitive rehabilitation and methodological consciousness. By this, he meant that policy makers should be made aware of their own psychologies and biases to reduce their vulnerability to cognitive pathologies. He however agrees that cognition is impractical and difficult to measure and stressed that preconceived ideas and biases are difficult to alter especially when policy makers devote less time for any serious reflection.

Against this background, it is obvious that Betts tries to provide solutions to intelligence failure that he admits are imperfect. His suggestions do not arrest the problem of intelligence failure. However, they offer the opportunity for some marginal improvement in the intelligence process. According to him "although marginal reforms may reduce the probability of error, the unresolvable paradoxes and barriers to analytic and decisional accuracy will make some incidence of failure inevitable". In this light, we proceed to do this analysis within the framework of Betts' theory by examining some case studies.

Case Studies

The Yom Kippur war

On 6th October 1973, Egyptian and Syrian military forces launched a surprise attack on Israel on the day of Yom Kippur knowing that the military of Israel will be observing the religious celebration of that day [7]. Prior to the attack, the Israeli Directorate of Military Intelligence (AMAN) assumed that Egypt was not going to attack until they solved their air superiority problem and secondly, Syria was not going to launch an attack without Egypt (ibid). On 25th September, General Zeira, the Director of AMAN dismissed intelligence from King Hussein of Jordan of an impending attack on Israel (ibid). Another warning on 30th September indicating that an Egyptian military exercise was going to end up in a real war was also regarded as baseless by the Military High Command [7]. In early October, Israel learnt that there was an ongoing evacuation of women and children in Egypt together with a heavy build-up of military forces. Zeira still did not interpret this as a build-up for war until 6th October when Ashraf Marwan, a spy in Egypt, informed Zeira that war was eminent at 0400 hrs [8]. Though he was now convinced with the latest intelligence, it was too late to build defenses to repel the attack. Surprise had already been achieved by the Egyptian and Syrian forces.

To analyze this strategic surprise, Honig [8] cites the orthodox school in his work which emphasizes that analysts are unable to

diagnose with accuracy if intelligence received is part of the enemy's deception plan or information from a spy could be a lie. He notes that the possible case of misleading information causes analysts to be pessimistic about the credibility of their sources of information as against their own judgments of the situation. Such was the case in the Israeli situation with events leading up to the strategic surprise. Zeira had received information from Ashraf Marwan in 1972 and 1973 about the impending war but in each case the intelligence contradicted the possibility of war which caused him to dismiss the credibility of the intelligence he received later. This is the challenge that Betts summarized under attack warning and operational evaluation in his analysis of strategic failures. The military high command could not establish the nexus between the attack warning and their own estimates together with the inability to estimate precisely enemy intentions with the intelligence available. The 1972 and 1973 false alarms made them more vulnerable to surprise since such false alarms are capable of blurring intelligence even though they may be accurate [9].

Against this backdrop, some scholars have argued that it is possible to check the credibility of HUMINT based on the motives of spies which can be assessed on the mode of recruitment of the spy and his or her relationship with the HUMINT agency. However, Honig argues that this is a complicated task to execute because it is impossible to penetrate the soul of a spy physically to determine his or her exact motives. Spies could have mixed motives and each motive may override the other in different circumstances. This brings into question the difficulty in judging the loyalty of a spy and the extent to which he would lie or hide information (ibid). This was exactly the nature of the dilemma that confronted AMAN. It was certainly difficult for AMAN to judge the motives of the Egyptian spy Ashraf Marwan since he had offered his services in 1969 in return for huge sums of money.

Other arguments have also held that the scale of the Egyptian exercise together with military assets deployed did not pass for a mere military exercise and therefore should have been an indication of an impending war. Honig [8] counters this argument and explains that the scale of deployment could have also passed for a mere bluff by the Egyptians to get Israel to accept their negotiation positions. Additionally, the scale of previous exercises had evolved incrementally which also could have been interpreted as Egypt's readiness for war from time to time but could not pinpoint exactly when Egypt will wage war against Israel.

The existence of the copious evidence did not take out the problem of ambiguity. In the face of such ambiguities most decision makers usually resort to their own judgments which they draw from their professional experience. However, Betts [10] thinks that relying on one's own experience makes decision-makers more prone to error than even ignorance especially when the enemy does not follow consistently the general pattern of past behaviour. This is exactly the same point emphasized in the barriers to analytic accuracy by Betts which played out in the posture of the Military high command in accepting that war was eminent. They relied more on their personal judgments instead of dwelling on the tactical situation that presented itself.

The problems with bureaucracy and the structure of organizations also featured in the Yom Kippur war. It is on record that among the intelligence officers who were to analyze Egyptian behaviour in order to estimate their intention, the one who had his analysis right was Lieutenant Benjamin Simon Tov of the IDF Southern Command [11]. It is critical here that looking at the chain of command, the influence of a Lieutenant was the least to be considered in the analysis. More weight

was given to the estimates of experienced senior officers of the higher ranks who according to Welinsky are less objective and more prone to biases due to their personal interests and obvious reliance on past experiences which may have not been relevant in this case.

Considering the above analysis, it is therefore telling that the absolute prevention of the Egyptian surprise attack on Israel could not have been guaranteed even if an attempt was made to identify all the weaknesses discussed above. Clearly, such an attempt to make reforms could still create new vulnerabilities making the system still prone to failure. The nature of the military structure was working against itself in the pursuit of finding the right intentions of the Egyptians. Indeed, the Yom Kippur war scenario was also a combination of the political and psychological factors discussed which could not have been identified in a single set of analyses right down from the build-up of the war till the time the time attack was launched. The element of surprise was therefore inevitable and the failure of the Israeli intelligence agency was also not avoidable on this basis.

The 9/11 terrorists attacks

On September 11, 2001, Islamic extremist associated with the Al-Qaeda terrorist group launched successive attacks against the United States of America by crashing two aircrafts into the towers of the World Trade Centre and another one into the Pentagon. After the attacks, the 9/11 Commission report indicated that the attack should not have come as a surprise to the United States since the terrorists had given copious warnings that an attack was looming. To cite a specific flaw in CIA operations, it is recounted that in January 2000, a meeting was held in Malaysia by some members of the Al-Qaeda terrorist organization which included Khalid al-Midhar, the terrorist responsible for the hijacking of the American airline (Flight 77) and later crushing it into the Pentagon [12]. It is important to note that America's most sophisticated intelligence agency, the CIA had very important details of the hijacker including his full name, photograph and passport number but however failed to put Al-Midhar on the watch list of the intelligence community until August 23, 2011. Several literatures have cited the 9/11 attacks a classical example of intelligence failure. James Wirtz [13] who is cited in Dahl [5] summarizes that: "even accounting for hindsight, it is difficult to understand how the government, the public and the scholarly community all failed to respond to the threat posed by Al-Qaeda, in a way that is eerily similar to the failures that preceded Pearl Harbour". The central question that therefore keeps coming is: why did it take the intelligence community so much time to act despite the threats of a possible attack that it received over the period? Against this background, an analysis was done on the intelligence failure based on Betts' theory in order to establish whether the failure of the intelligence community could have been avoided.

Scholars like Zegart [12] indicate the ability of the intelligence community to adapt to the new wave of threat after the collapse of the Soviet Union as one of the reasons why the intelligence community failed. However, further in her argument she supports the arguments of Robert Betts by assigning the failure to the nature of organizations (Bureaucracy). It is in the nature of organizations to follow routines and adhere to strict organizational culture but this structure of organizations makes it very difficult for them to deviate from the standard operational procedures even when a deviation could be beneficial to the current circumstances: a circumstance which has been labelled by Levitt and March [14] as the "competency trap". Therefore, the CIA and other intelligence agencies at the time of the 9/11 attacks

exhibited the true nature of its structure given the circumstances at the time. Zegart [12] maintains that the structure of organizations is supposed to make them reliable, however this same feature that gives organizations its reliability poses as a challenge to its ability to adapt to changes. Moreover, we cannot say with absolute surety that a change in focus of the CIA about the changing threats to the US could have been a full-proof to avoiding the surprise attack. In fact, Betts notes that bureaucratic reforms come along with new unforeseeable challenges that could still work against the intelligence function. Against this background, we argue that intelligence failure was borne out of the structure of organizations within the intelligence function which makes the intelligence community vulnerable to the element of surprise at all material times.

According to the 1996 House Intelligence Committee staff study, one of the causes of the 9/11 intelligence failure was the lack of "co-operativeness" within the intelligence community or the lack of integration between the individual agencies [12]. This led to the lack of information sharing between the intelligence communities and the law enforcement agencies. Robert Betts refers to this problem as pathology in communication which is a weakness in the intelligence process. By inference, the communication gaps that occurred at the time of the 9/11 attack was a weakness within the intelligence process which by extension was as a result of the legislative instruments regulating the process of collecting intelligence. Methods and sources for intelligence gathering were protected while the intelligence community was always reminded to adhere to the laws and policies of the United States including the famous Foreign Intelligence Surveillance Act (FISA) designed to protect the rights of American citizens [15]. According to the white paper prepared by the AFCEA International in 2007, these procedures and legislations were so restrictive that it made information exchanges outside the intelligence community and even within it impossible or illegal. This therefore one of the major reasons why the CIA will did not release the full names of the terrorist because it will bring into question their methods of acquiring information including listening into phone conversations which at the time was illegal.

Based on this, it is fair to argue that the intelligence community was in fact operating within the framework of the law and also functioning according to standard operational procedures even though such procedures and rules were inimical to the prevention of a surprise attack. The nature of the rules and processes (from both external and internal) was an impediment to the sharing and flow of information that was necessary for the prevention of the 9/11 surprise attack. The weaknesses that these structures (which are a natural part of bureaucracies) present in the intelligence process is what makes the avoidance of the surprise attack inevitable due to their inherent vulnerabilities.

The 9/11 commission report also indicated that "the system was blinking red" since the FBI and CIA had given some indications to the Bush administration that America was under threat of an attack. Even though intelligence came in bits and pieces, likely targets were known to the intelligence community and the Bush administration but government was slow to understand and slow to act in the heat of this conflicting information. This is where it is important to highlight on ambiguity of evidence which Betts believes could cause policy makers to misunderstand analysis provided thereby leading to poor judgment and decision-making. As indicated earlier in Betts analysis of an attack warning, he indicated that policy makers would also act with no sense of urgency or discount threats if they misunderstood it all did not conform to existing intelligence estimates. The 9/11 report further

indicated that as at September 4, 2001 the United States Government had not been able to make up its mind on whether Al-Qaeda was a big deal. In fact, the issue of terrorism was not an overriding national security concern to the 9/11 Bush administration (ibid). Measuring the posture of the Bush administration in relation to defense planning under Betts analysis of strategic failure, it is possible that the political leadership had other competing domestic issues on the table which caused them to place less priority on the terror threat. This according to Betts, is a natural reaction from leaders especially during peace time.

Conclusion

Intelligence failures occur because there are inherent weaknesses in the intelligence process which are basically psychological and political. The failures during the Yom Kippur war and 9/11 demonstrated the vulnerabilities that Betts talks about in his theory of intelligence failure. During the discussion, we touched on the structure of organizations (bureaucracy) which makes them prone to error; unforeseen vulnerabilities that are created out of organizational reforms and barriers to analytical accuracy stemming from communication gaps, overriding self-interests of decision makers which clouds good judgment were all found to have been some of the conventional causes of intelligence failure. However, a further analysis of these factors indicate that they are weaknesses that are only inherent in the intelligence process which can only be managed to reduce their impact but cannot be eradicated entirely. Against this background, we conclude with the following summary from Betts [10] which states that "Nations can be hit with calamities not because their leaders are not informed but because the national capabilities are deficient. Intelligence failures are not only inevitable but they are natural. They are only less forgivable because they are consequential".

References

1. Lowenthal MM (2015) *Intelligence: from Secrets to Policy*. Washington DC: CQ Press.
2. Walters VA (1978) *Silent Missions*. New York: Double Day and Company Incorporated.
3. Lowenthal M (2006) *Intelligence: From Secrets to Policy*. Washington D.C: Congressional Quarterly Press.
4. Schmitt GJ (2005) *Truth to power? Rethinking Intelligence analysis*.
5. Dahl E (2013) *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond*. Washington D.C: Georgetown University Press.
6. Betts R (2007) *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia University Press.
7. Bar-Joseph U (2005) *The Watchman Fell Asleep: The Surprise of Yom Kippur and Its Sources*. New York: Sunny Press.
8. Honig O (2008) *Surprise Attacks-Are They Inevitable? Moving Beyond the Orthodox-Revisionist Dichotomy*. *Journal Security Studies* 17: 72-106.
9. Jervis R (1986) *War and Misperception*. London: Cambridge University Press.
10. Betts R (2014) *Analysis, War and Decision Why Intelligence Failures are inevitable*. *Journal of the America Intelligence Professional* 54.
11. Avi S (1967) *Failures in National Intelligence estimates: The case of the Yom Kippur war*. *World Politics* 28: 348-380.
12. Zegart BA (2005) *September 11 and the Adaptation Failure of US intelligence Agencies*. *International Security* 29: 78-111.
13. Johnson KL, Wirtz JJ (2008) *Intelligence and National Security: The Secret World of Spies: An Anthology*. New York: Oxford University Press.
14. Levitt B, March JG (1988) *Organizational Learning*. *Annual Review of Sociology* 14: 319-340.
15. AFCEA International (2007) *The Need to Share: US Intelligence Community and Law Enforcement*.