UNISCI Discussion Papers

METHODOLOGICAL APPROACHES TO THE CONCEPT OF INTELLIGENCE FAILURE

AUTHOR[1]:	GUSTAVO DÍAZ UNISCI
DATE:	January 2005

In a field where a great deal of emphasis is placed on reducing uncertainty[2], it would be somewhat disheartening to accept that failures may be inevitable, yet the possibility of failure is an inherent aspect of intelligence[3]. Failure in intelligence has always attracted more attention than success and that is why there have been numerous studies on intelligence failure during the last few decades. The intelligence failure has been a topic of concern for academics and also intelligence analysts, yet almost all contemporary studies in this field have been made by American scholars.

These studies were initiated with the Pearl Harbour attack, examined by Roberta Wohlsletter[4]. In the 1980s, a lot of literature grew around the subject of strategic surprise, as scholars such as *Richard Betts*[5] and *Michael Handel*[6] developed theories to explain not only the failure of Pearl Harbour but also other "disasters" such as the Yom Kippur war in 1973[7].

The different literature during the years has focused on a particular aspect of intelligence failure, the failure to detect or prevent a surprise attack. In words of Walter Laqueur "One of the major functions of an Intelligence service, is to shield those it serves against surprise"[8].

---

[1] Las opiniones expresadas en estos artículos son propias de sus autores. Estos artículos no reflejan necesariamente la opinión de UNISCI. The views expressed in these articles are those of the authors. These articles do not necessarily reflect the views of UNISCI.

[2] Lowenthal, Mark (1992): *U.S. Intelligence: Evolution and Anatomy*. Westport, CT: Praeger, p.19.

[3] Betts, Richard: "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable". *World Politics,* Vol. 31, No. 1 (1978), p. 62.

[4] Wohlsletter, Roberta (1962): *Pearl Harbour Warning and Decision* . Stanford, Stanford University Press.

[5] Betts, Richard: "Analysis war and decision: Why intelligence failures are inevitable". *World Politics*, Vol. 31, No. 1 (October 1978).

[6] Handel, Michael: "Intelligence and the problem of strategic surprise", *Journal of Strategic Studies,* No. 7 / 3 (September 1984)

[7] Kahn, David: "The Intelligence Failure at Pearl Harbour", *Foreign Affairs,* Vol. 70, No. 5 (Winter 1991/1992); Handel, Michael: "The Yom Kippur War and the Inevitability of Surprise", *International Studies Quarterly* (September 1977).

[8] Laqueur, Walter (1985): *World of Secrets The uses and limits of Intelligence,* London, Twentieth Century Fund, Weidenfeld and Nicolson, p. 255.

Writers on strategic surprise have examined the failure of intelligence services to prevent a wide variety of unexpected events that pose a threat to national security; post 9/11[9] the study of intelligence failure has become of particular national concern in the US.

Scholars have generally concluded that failure is inevitable, but diverging points of view have existed with regards to the origin of failures.

This paper will begin by examining the relevant literature on intelligence failure. It will show that in these writings one can find different approaches to the analysis of this topic.

Today one can find enough (open source) material available about this subject to make a serious study grounded in intelligence theory. Firstly however, we should define what is meant by intelligence failure by understanding the very meaning of intelligence itself. By doing so one can then conclude what the essence of intelligence failure really is.

There are no common definitions of intelligence[10] and the various definitions are dependent on the interpretation of the term. For this essay the intelligence definition of Sherman Kent will be utilised .It must be recognised though that this is neither the only definition and perhaps may not be the most complete of all. For Kent, Intelligence is "*Knowledge upon which we based our high level national policy toward the other states of the world"*[11]. In other words, it is the knowledge upon which decision makers formulate judgements concerning national security, such a short definition alludes to the view that the point at which we begin is that of the conflict between nations. Conflict of interest leads to secret information; to hide vital information from the enemy. Intelligence failures then are inevitable from the outset due to it being a zero sum game -The failure of intelligence on one side will always be the counterintelligence success of another one. From here we can now determine that the job of intelligence is not to predict the future, but to help policy makers think about the future. William Colby provides the most useful definition here *"The true definition of intelligence is to help make decisions to bring about a better future and avoid the dangers than an intelligence projection might present to change rather than merely to know the future"*[12].

So, what do we understand by an intelligence failure? Mark Lowenthal provides a good start, "*an intelligence failure is the inability of one or more parts of the intelligence process (Collection, evaluation, analysis, production, dissemination) to produce timely, accurate intelligence on an issue or event of importance to national interest*[13]*"*, but Lowenthal's definition neglects the link between intelligence and policy.

On the other hand Abram N. Shulsky focuses on those who receive intelligence. For Shulsky an intelligence failure is essentially *"a misunderstanding of the situation that leads a government to take actions that are inappropriate and counter productive to own interests"*[14].

---

[9] Goodman, Melvin: "9/11.The failure of strategic Intelligence", *Intelligence and National Security*, Vol.8, No. 4 (Winter 2003), p. 59-71.

[10] There have been a wide debate about what intelligence is but there is not space in this work for this interesting question.

[11] Kent, Sherman (1949 reprint 1965) *Strategic Intelligence for American World Policy*. Princeton, Princeton University Press*, Preface.*

[12] Colby, William: "Deception and Surprise: Problems of analysis analysts*". Intelligence and National Security* (1981), p. 84.

[13] Lowenthal, Mark: "The Burdensome Concept of Failure", in Maurer, Alfred C., Tunstall, Marion D. and Keagle, James M. (eds.) (1985): *Intelligence: Policy and Process*. Boulder, Westview Press, p. 51.

[14] Shulsky, Abram (1991): *Silent Warfare.* Washington D.C., Brassey's, p. 63

One can therefore conclude that the best definition is a combination of both intelligence failures: the failure of the intelligence process and the failure of decision makers to respond to accurate intelligence.

With the boundaries of what we understand by intelligence already reduced , what is the mission of the intelligence?, and most importantly, what is intelligence failure? One can now use different theories to attempt to explain the failures of intelligence. After a thorough analysis, different theories of intelligence failure will be split down to two different approaches.

1. The traditional point of view

It is the predominant one in the literature of the intelligence failure. It tends to analyse intelligence failures with the specific aim of identifying those responsible for it. Essentially the question being asked is, "Who is at fault?" Is it the Intelligence community, decision makers or decisions taken by the enemy?

The main writer of intelligence failure as policy maker's fault is Richard Betts, who has made a major contribution to this point of view. He argues that "*intelligence failures are not only inevitable, they are natural"*[15]. For this writer, the work of analysis is ambiguous and policy makers are most often responsible for failure for not taking the advice given by intelligence[16]. It is a fact that policy makers will often ignore or misunderstand and intelligence product .In his later book[17] Betts emphasised the responsibility of decision makers even more strongly. Betts argues that a great deal of emphasis is placed upon warning at the expense of required response. For this author it is a fundamental issue to develop a theory of the subject, rather than focusing on case studies alone. In this way he conceptualised the intelligence failure in three overlapping ways. Firstly, mistakes can happen in any activity, but, in the nuclear age, just one error may lead to apocalyptic consequences. For Betts: the perfect production of intelligence does not necessarily lead to perfect intelligence consumption. He calls this the "*paradoxes of perception*". So the main responsibility of intelligence failure is therefore placed on the policy makers. Similarly intelligence services must transmit the information to the policy makers and make them feel that the issue is important[18]. This is called "*Pathologies of communication*". Betts argues that the basic barriers to analytic accuracy are "ambiguity of evidence, ambivalence of judgement and atrophy of reforms"[19]. Drawing upon this argument the main problems here are *the subjectivity of the human cognitive process* and the ambivalence of the interpretation of the information. Betts proposes some solutions to minimize the intelligence failure and the risks of related issues, like the risk of false alarms, which can lead to the cry wolf syndrome. Multiple advocacies ensure that all views held by individuals within the analytic system will be granted serious attention but it can also lead to ambiguity and confusion. Devil's advocacy is the problem of constantly assuming

[15] Betts, "Analysis war and decisions", p. 88

[16] There are two main lines in the United States about the relation of the intelligence community with the politician: Sherman Kent's line and Kendall's perspective about the degree of linkage of intelligence with politics. For a deep analysis see: Studies in Intelligence: "The Kent-Kendall debate of 1949*".World Politics,* Vol. 36, No. 5 (1992).

[17] Betts, Richard (1982): *Surprise attack: Lessons for defence Planning.* Washington D.C., The Brookings Institution.

[18] Betts, Richard and Mahnken, Thomas (2001): *Paradoxes of Strategic Intelligence.* Frank Cass, p. 63.

[19] Betts: "Analysis war and decision", p. 67.

the worst, which may lead to a permanent state of alert that could be difficult to maintain in a democratic state and may end up aggravating the cry wolf problem. For Betts, the best solution is to make plans to deal with surprise and try to reduce its consequences. One of the main critiques of this point of view is that include the decision makers inside the intelligence failure and perhaps intelligence failure is one thing and decision makers failure is another.

The second representative of the traditional school of intelligence failure is Michael Handel.[20] He argues that despite the presence of sufficient indicators, intelligence professionals and decision makers often fail to arrive at the correct conclusion. He points out that there is a slight chance, despite the availability of adequate information, that new technologies and full human effort can not prevent a surprise attack, because the main problem of intelligence failure lies in cognitive issues of human activity. Handel too describes intelligence failures as inevitable. He draws a list of problems suggesting that intelligence failures could occur as a result of a wide variety of factors; but he felt that the principal cause of intelligence failure was based in the psychological limitations of human nature[21], and most intelligence failures occur because intelligence analysts and decision makers refuse to adapt their concepts to the new information. Handel states "Since intelligence failures are inevitable we must learn to live with ambiguity, the best way of avoiding surprise is being able to cope with it, once it has taken place"[22] Handel agreed with Betts that the highest level of responsibility lies with the decision makers who refuse to accept the analysis provided by intelligence. Handel and Betts both conclude that the technological progress does not dramatically aid in forewarning of surprise attacks. For these authors the technological revolution is not the main problem of intelligence failure, both are focused on the limitations of human cognition.

Similarly Loch Johnson has written that the unwillingness of policy makers to accept the intelligence community's judgements , is a central problem in intelligence "They are out there permanently and their mission is to convince the decision makers the reality of the threats for the national security of a country"[23].

Other intelligence scholars have been of the view that the most obvious reason for intelligence failure is the lack of knowledge. Ignorance[24] is sometimes the main reason of intelligence failure, this is just the main function of intelligence service, to reduce the uncertainly and the ignorance about a theme. While the dominant view among scholars is that policy makers deserve more responsibility for failure than they usually receive, others argue that the fault usually begins with the intelligence community. This interpretation of intelligence failure has often been made by policy makers. Not all such critiques are made by policy makers, though similar critiques have been made by those within the Intelligence community, such as Patrick J. McGarvey[25]. There is much writing on the failure of analysis in the intelligence community. The critique of the responsibility inside the intelligence community usually leads to the analysis rather than the collectors or covert action. These

[20] Handel, Michael "Intelligence and the problem of the strategic surprise", *Journal of Strategic Studies* No.7 /3 (Sep 1984), pp. 230; Handel, Michael (1985): *Military Deception in Peace and War*. Jerusalem, Magnes Press.
[21] Betts and Mahnken, *Paradoxes of Strategic Intelligence,* p.166.
[22] Handel, "Intelligence and the problem of the strategic surprise", p. 45.
[23] Johnson Loch "Analysis for a new age", *Intelligence and national security* Vol. 11, No. 4 (October 1996), pp. 663.
[24] Laqueur, *World of Secrets,* p. 281.
[25] McGarvey, Patrick: "DIA Intelligence to please", in Halperin, Morton H. and Kanter, Arnold (eds.) (1973): *Readings in American Foreign Policy*. Boston, MA. Little Brown.

writings argued that the interpenetration of information may be at fault, rather than the methods used to collect the information.

One of the main representatives of this theory of the intelligence failures likens it to a disorder of the analytical process and that the main responsibilities are in the intelligence community. Abram N. Shulsky argues that despite analytical process is an intellectual activity, it takes place in an institutional setting and it is produced through standard procedures, so that the final result is more the product of a system than that of a single individual[26]. As such it is vulnerable to certain bureaucratic pathologies. In many cases intelligence has been subordinated to policy. Similarly, intelligence judgements may often be made to produce results that superiors wish to hear rather than what the evidence indicates. Other problems are those presented for the security regulations, in restricting the circulation of sensible information. This point of view is of great importance because it regards intelligence failure as a bureaucracy malfunction. This has also been the view of many other intelligence scholars[27]. Abram Shulsky[28]presents some solutions to the problem of intelligence failure with institutional solutions that require the restructuring of the institutional framework in which intelligence analysis is carried out, and intellectual solutions based in attacking the heart of the problem of intelligence failure, the thought process of individual analysis. But the main solution for this author is the emphasis on knowledge of foreign societies. This idea is essential to understanding the co-operation and conflicts between different nations.

Some writers focus on deception and theorise that failure is the fault of the enemy and the actions of the attackers. The most prominent example is Barton Whaley[29] who examined the Nazi invasion of the Soviet Union in 1941. Whaley argues that the critical factor in surprise attack is what he calls stratagem: "A co-ordinated campaign of deception to mislead the victim's analysis"[30].

There are some very strong critics of this traditional approach. Like Abraham Ben-Zvi,[31] who argues that surprise attack has not come very far since Wohlsteller, he is not in agreement with the idea of cognitive limitations. Ariel Levite[32] also disagrees with the dominant view that intelligence failures are natural and inevitable, arguing that where there is sufficient intelligence available one can take appropriate defensive actions.

2. The optimistic school

The other approach is more optimistic. It holds that intelligence can be improved through the use of technology; in particular the tools of the information revolution, and that intelligence failure could be reduced by the use of the new techniques.

[26] Shulsky, *Silent Warfare,* p. 63
[27] Brady, Chistopher "Intelligence Failures: Plus Ca Change", *Intelligence and National Security,* Vol. 8, No. 4 (October 1993), p. 90.
[28] Shulsky, *Silent Warfare,* p.63
[29] Barton, Whaley (1973): *Code Word Barbarrosa* . Cambridge MA: The MIT Press.
[30] Ibid., p.171.
[31] Ben Zvi, Abraham: "A conceptual framework for the analysis of surprise attack*". World Politics,* XXVIII (April 1970).
[32] Levite, Ariel (1987): *Intelligence and Strategic surprise*. New York, Columbia University Press.

Some thinkers seem to have initially held this point of view but have progressively moved towards the traditional approach; one example is Klaus Knorr[33].

On the other hand, and returning to the point of view of this school, Joseph Nye and William Owens[34] explain that technology will give U.S. forces a wide asymmetry between what Americans and their opponents know.

There are relatively few academics among this school of military predominance, but one can mention Bruce Berkowitz, Walter Laqueur , Michael Herman ,David Kahn[35]…

For Michael Herman,[36] intelligence can not always be right, because "since estimating is what you do when you do not know it is inherent in a great many situations that after reading the estimate you still do not know." He concludes "states can never fully understand each other"[37] so intelligence failures not only can occur but they have to occur.

Michel Herman carries an interesting point, that assuming equal competences, intelligence might be expected to win in some context and counterintelligence in the other, so intelligence failure is the success of the enemy's counterintelligence.

As we can observe, for Herman the main problems of the analytical process point up to the cognitive rigidity and the human tendency to interpret all evidence in the light of preconceptions and to resist alternative explanations. This is the basis for the difficulty of the use of open sources (OSINT) in intelligence analysis or for the necessity of works about the reform of intelligence community (Like Terverton's work)[38]. The solutions that this author points to conclude that with the benefits of the technological revolution intelligence failures could be reduced dramatically but never made inevitable.

David Steele[39] is another representative of this school. He argues that to deal with the new threats in the 21st century the intelligence community must realize that intelligence is much more than just secret information; it is an advocate for OSINT. For Steele and authors like him, collection is the main problem of the intelligence community facing intelligence failure rather than analysis. These kinds of theories face the question of the change in the nature of threats in a very realistic way for the 21st century, with threats like terrorism. They compound one of the major critics of the literatures in intelligence failure, focusing principally on

[33] Knorr, Klaus: "Failures in national intelligence estimates" *World Politics,* XVI (April 1964).
[34] Nye, Joseph and Owens, William: "America's information edge", *Foreign Affairs.* Vol. 75, No. 2 (March-April 1996), pp.23-24. http://ics.leeds.ac.uk/papers/vf01.cfm?folder=49&outfit=pmt.
[35] Berkowitz, Bruce and Goodman, Allan (1989): *Strategic Intelligence for American National Security.* Princeton, Princeton University Press. Chapter 2 "The Cycle of Intelligence" starts with a "definition" of intelligence failure. Berkowitz, Bruce: "Information Age Intelligence", *Foreign Policy* 103 (Summer 1996), pp. 37. Note that although Berkowitz frequently advocates technological solutions, he also acknowledges that the intelligence community must address organisational and other problems. In the same way see Laqueur, *World of Secrets,* p. 308.
[36] Herman, *Intelligence Power in Peace and War,* p. 221.
[37] Ibid., p. 226.
[38] Treverton, Gregory (2001): *Reshaping National Intelligence for an Age of Information.* Cambridge, Cambridge University Press. An important book about U.S. Intelligence Reform in the 21st Century.
[39] Steele, Robert David: "The Importance of Open Source Intelligence to the Military", *International Journal of Intelligence and Counterintelligence* Vol. 8, No. 4 (Winter 1995), pp. 457-470. Other good resources from this author are: Steele, Robert David: "Crafting Intelligence in the Aftermath of Disaster", *International Journal of Intelligence and Counterintelligence* Vol. 15, No. 2 (Summer 2002), pp. 161-178; Steele, Robert David: "National Intelligence and Open Source: From School House to White House", *American Intelligence Journal,* 14, Nos. 2 and 3 (Spring/Summer 1993), pp.29-32.

analysis failure. Today collection will be fundamental to face correctly asymmetric threats like terrorism.

3. The alternative approach

There are other thinkers that argue that none of the studies of intelligence failure are sufficient to explain the disaster, indeed no single actor can reasonably be guilty of intelligence failure. This suggests that there is an alternative approach that may be useful in seeking to understand why such failures occur. If we think carefully about the failure in any human activity we would conclude that intelligence, like human activity, is imperfect and failures are normal in any human activity, so failure is a part of intelligence. This argument is the principal one claiming that intelligence is not a science because intelligence does not always give the same results with the same environment; there are always factors, which you cannot control. The principal exponent of this kind of argument is an alternative theory: which is called Intelligence Failure as a normal accident**.** Based on the studies of Charles Perrow[40] it has been called "Normal accident theory". This author argues that accidents in complex systems are inevitable, because it is impossible to anticipate all possible failures. In large organizations mistakes happen.

The problem of this theory is that we are talking about security measures and in this regard there are lives in the way, and the failures or mistakes lead to human death. This theory argues that accidents are ordinary events, caused by the accumulation of small mistakes. Normal accident theory suggest that while intelligence failures may be caused by the classic problems of intelligence, the inevitability of failure may be the result of the complex nature of intelligence. The fundamental importance of secrecy within the intelligence community may tend to exacerbate this complexity, reinforcing the point that Perrow makes about complex systems. So nobody within the system is able to see the entire picture.

4. Intelligence failures and the intelligence process

As we have concluded, it will be very important in the fight against the new threats of the 21st century in general and with the new face of terrorism in particular, focusing in the whole intelligence cycle .Because we are not really sure how real is this new kind of threat and it has a new kind of characteristics which they make very difficult to fight it with the traditional methods. In the next section I shall try to present the difficulties and limits of the rest of the intelligence elements for the concept off intelligence failure. I will try to present, as we have pointed bellow, the limitations on the rest of the intelligence cycle, collection counterintelligence and covert action (we already have analyze the analysis part) and how important will be put the focus of the study of intelligence failures in the rest of the process of intelligence to facing the "new threats" of the 21st Ct properly.

4.1. Collection

According to my own point of view the new nature of the threats in the 21st Century make the collection process the fundamental part in the study of intelligence failure. These new threats

[40] Perrow, Charles (1984): *Normal Accident: Living with High-Risk Technology.* New York, Basic Books.

are much more disperses and present really smalls signals, so collection will be fundamental to prevent intelligence failure.

As with intelligence as a whole, the collection process will always be flawed[41]. The collection of raw data presents us with limitations at every stage[42]. One could write a long list of the many specific methods of collection, but the focus of this section will be on the three generalized but main sources of intelligence collection: Human, Technical and Open Source.

4.1.1. Open Source Intelligence (OSINT)

The vast majority of intelligence data, approximately 70%-80% is collected from open sources, yet this most facile method of intelligence collection is limited in what it can contribute towards our understanding of a given situation[43]. OSINT proves to be both unreliable or difficult and impossible to attain in closed societies[44]. Furthermore, in more open societies OSINT may provide us with a better understanding of a state but when dealing with non-state actors such as terrorists, there are no sources to draw upon except for the odd audio, video or internet release. [45]With the development of the internet there has also been a great deal of information overload which again would force intelligence professionals to prioritize the open sources that they focus on, depending on how reliable or useful these sources prove to be. The vast volume of foreign language open sources has in many cases also led to a shortage of required translations[46]. Intelligence organizations simply do not have the human or economic means to cover all open sources all of the time, and are required at every stage to prioritize. This would again bring us back to the dilemma of deciding to give preference to certain open sources over others. Such prioritization is not only an imperfect process but would undoubtedly lead to valuable intelligence that will be overlooked, thereby increasing the likelihood of an intelligence failure.

4.1.2. Technical Intelligence (TECHINT)

Another field of intelligence collection that has been subject to information overload has been technical intelligence. With the development of many new means of communication and their subsequent expansion, intelligence agencies involved in signals intelligence (SIGINT) have been forced to use keyword techniques when deciding which communications to intercept[47]. Such a system would inevitably be subject to failure as there are an infinite number of methods to avoid such intercepts. Moreover, the volumes of intercepts are so great in number that a large amount of intercepts would remain un-deciphered and un-translated for long periods of time[48]. Intercepted Intelligence that may be of immediate use would therefore be rendered useless, thereby substantially increasing the likelihood of intelligence failures. At a time when states are faced with the strong and growing threat of asymmetrical warfare, they no longer have the luxury of acquiring intelligence by focusing on a limited number of communications methods, such as that of a nation-state's military.

---

[41] Pringle, Robert "The Limits of OSINT: Diagnosing the Soviet Media, 1985-1989", *International Journal of Intelligence and Counter Intelligence,* No. 16 (2003), p.284.
[42] Betts, 'Why Intelligence Failures are Inevitable', p.61
[43] Hulnick, Arthur: "The Downside of Open Source Intelligence", *International Journal of Intelligence and Counterintelligence,* No. 15 (2002), p. 566.
[44] Pringle, p. 84
[45] Hulnick, "The Downside of Open Source Intelligence", p. 566.
[46] Ibid., p.571.
[47] Shulsky, *Silent Warfare*, p. 31.
[48] Ibid., p. 30.

4.1.3. Human Intelligence (HUMINT)

Most of the problems with human intelligence arise at the analysis stage[49], but the gathering of this form of intelligence also presents us with limitations. Intelligence officers in the field may not always have the ability to make contacts with optimal agents, that is to say agents that will be able to provide them with the most accurate and reliable information possible. The main cause of this would be the unavailability of intelligence recruits with skills in difficult and isolated languages[50]. These limitations have forced the Intelligence organizations of English speaking countries to deal almost entirely with agents that have English language skills[51]. Teaching intelligence officers these language skills would be a time consuming process, at a moment when their immediate use would be needed. Intelligence organizations simply cannot identify and recruit the best possible agents and will therefore be limited in the kind of information to which they will have access.

5. Counterintelligence – Protecting secrets

The protection of acquired knowledge is a vital function of any intelligence organization. No amount of extensive security and stringent assessment checks will guarantee that an employee will observe the rules. It would also be logical to assume that if a person has access to any piece of information then it can in all likelihood be compromised. In holding the responsibility of protecting their knowledge, intelligence organizations are faced with two dilemmas in their selection of employees. Firstly, the instruments of psychological and behavioural measurement hold accuracy rates that are below 100 per cent, allowing individuals who may pose a security threat to be cleared for employment[52]. Secondly, attempting to create a profiling system that identifies future betrayers would be an imperfect process leading to the allocation of resources towards the wrongfully suspected rather than those well trained in evading detection[53]. Given the complexity and importance of this problem it seems somewhat surprising that so little scientifically grounded paradigms exist for the detection and prevention of such espionage methods.

Drawing upon psychological models would be the most rational method of detecting betrayers, as it offers us the chance to identify psychological abnormalities[54]. Whilst physical actions may identify a betrayer and prevent the continuing compromise of knowledge, it is the prevention of such an intelligence failure that should be our primary concern and for this we must turn to psychology.

The psychological paradigm essentially makes the assumption that those who are actively compromising information or liable to betray secrets, are likely to differ in a measurable, reliable, and different way from those people who are not likely[55]. Likewise, there exists the assumption that an underlying characteristic, not yet identified, is related to the likelihood of an actor to engage in betrayal. If this characteristic can be identified and measured reliably,

[49] Lefebvre, p. 232
[50] Hulnick, 'Fixing the Spy Machine', p. 40.
[51] Ibid., p. 154.
[52] Sarbin, R., Ralph, Theodore Carney and Carson, Eoyang (1994): *Citizen Espionage: Studies in Trust and Betrayal*. Westport, CT: Praeger, p.70.
[53] Sarbin, p.70.
[54] Ibid., p. 71.
[55] Ibid.

those who score below a scientifically established threshold denied the access to the most critical and sensitive positions of an intelligence organization[56]. Until such a system is brought to fruition, intelligence failures in this field will be a likely occurrence. The most common occurrences of betrayal have been linked to money, ideology, coercion and ego, all of which are extremely problematic to measure scientifically[57]. Other psychological factors in bringing out betrayal can be disaffection, vindictiveness and whimsy, all of which are again impossible to accurately measure with today's scientific and psychological capabilities. The complex nature of such traits also reduces the likelihood of scientific means ever being developed to fully screen out personnel that may in future betray secrets.

6. Covert action – Third parties

Covert action may inevitably fail for many of the same reasons that other sections of intelligence may fail. Its requirement for a clear set of objectives, an accurate understanding of the conditions in which it will take place and how the objectives will have been achieved, are all subject to fallible human interpretation[58]. Yet what separates this arm of intelligence from all others is its use of third parties. The use of such groups outside the direct control of intelligence organizations is essential in maintaining deniability[59]. They are commonly used in covert operations that aim to exert political and economic influence on foreign territories. Such exertion of influence can be done through foreign structural and agential means, examples being: paramilitary groups, political organizations and those generally aiding the foreign intelligence organization in achieving its objectives[60]. The use of such third parties produces a host of problems that would inevitably lead to intelligence failures. Regarding secrecy, third parties are not obliged to respect the rules that the personnel of an intelligence organization will have to abide by, nor will they have to go through vigorous and extensive screening process to ensure certain degree of reliability and trustworthiness[61]. This dependence on third parties can also be identified in the use of psychological warfare, as such actions put the onus on a third party target to believe what it is being told[62]. Such psychological operations would only be guaranteed to work if the target were to use an epistemologically constructivist approach with no other access to previous and present sources of knowledge. This of course is almost entirely unfeasible and would therefore expose psychological warfare to the likelihood of failure.

Conclusion

Failures are an inherent part of intelligence due to the reality of human and economic limitations. Economic limitations entail the allocation of scarce financial resources towards security threats. As each intelligence organisation have access to a limited amount of capital,

[56] Ibid., p. 72.
[57] Richelson, p. 272-293.
[58] Shulsky, *Silent Warfare,* p. 84.
[59] Wettering, Frederick L.: "(C)overt Action: The Disappearing 'C'", *International Journal of Intelligence and Counterintelligence*, No. 16 (2003), p.562.
[60] Wettering, p. 562.
[61] Gunter, Michael: "The Iraqi Opposition and the Failure of U.S. Intelligence", *International Journal of Intelligence and Counterintelligence,* Vol. 12, No. 2 (2002), pp.144.
[62] Shulsky , *Silent Warfare,* p. 93

the process of prioritisation will have to be fundamental. As the process of prioritisation is beset by cognitive human limitations it leads to results that are less than perfect. This shortcoming in prioritisation leads us to accept that if threats cannot be perfectly identified and prioritised then failures will be inevitable. Furthermore, ontological and epistemological hurdles exist in all elements of intelligence, but even more at the analytical level. Even if one makes the assumption that threats that are perfectly identified and prioritised, we are then faced with the limitations of intelligence collection. The vast volume of raw data facing collectors of intelligence means that collecting all relevant sources of information will be an impossible task. Useful or essential raw data that may prevent an intelligence failure will inevitably be missed. Once knowledge is acquired intelligence organisations are also forced to accept that no scientific methods exist to effectively screen out all those that are engaged in or seeking to betray secrets. Whilst certain instruments and methods such as the polygraph and background checks may be used, they are by no means fully accurate in identifying undesirable personnel[63]. The infinitely complex psychological issues involved with such identification leads us to conclude that betrayal of secrets may indefinitely continue being a problem for all intelligence organisations. Finally, the necessary reliance of most covert operations on third parties, leads us to accept that intelligence organisations will have to deal with agents and structures beyond their control, thereby making it highly likely that undesirable outcomes may be the result of such operations.

One hundred percent accuracy is the only margin of safety in preventing intelligence failures and one that is innately out of reach for any national security apparatus, intelligence being no exception. Given the case, we may have to consider failure as the undesirable normative state of intelligence, with all actions taken within its field made to reduce its likelihood.

According to my point of view, the different approaches do not focus on the whole process of intelligence and they put all the stress of intelligence failures on the analysis of the information or in the responsibility of the decision makers, or the importance of the developing of technology and its impact on intelligence failure concept's. The intelligence process works as a unit, and any dysfunction in any part of the cycle makes that the whole process does not work properly .That limitation of the review of intelligence failure in the whole process could be for the limitation of present a proper definition of intelligence.

We have tried to present hereby the major approaches of failures of intelligence systems. And we do not only present an alternative point of view but we have tried to fill the gap, focusing on intelligence failure in the rest of the intelligence process. There are few references regarding intelligence failure and new threats, like the global terrorism attacks and the fundamental role they play today. J. Bowyer Bell[64] argues that although non-state actors such as terrorist groups use hiding and secrecy routinely, they rarely have the skills and sources to conduct more than tactical deception. They are not a conventional adversary and a new approach is necessary to deal with this modern kind of threat.

We understand that the main difference between the two approaches is that the optimist school argues that the use of modern technology can improve its chances against terrorist threats and reduce intelligence failure. On the other hand, the Intelligence community holding the orthodox point of view, have placed the stress not on the importance of the technology but

[63] Hulnick, "Fixing the Spy Machine", p. 91.
[64] Bell, J. Bowyer: "Toward a Theory of Deception", *International Journal of Intelligence and Counterintelligence,* Vol. 16, No.2 (Summer 2003).

on the cognitive limitations and human perceptions. The traditional intelligence paradigm has held the view that enemy's capabilities are more important than assessing its intentions. Now terrorism may be turning this model on its head. In the past, surprise attacks have often produced little more than tactical success. The global terror threat is therefore nothing more than a political threat, because it is not a military threat and not an economical threat, but a new kind of threat where the only route to success is the tactical success. The nature of surprise is different in terror attacks; the surprise is often in the tactical specifics of the attacks, such as the technology or methods used.

Both branches of the orthodox approach and the optimistic one, point out that; intelligence failures are inevitable as they are a part of human activity and as such are imperfect. Intelligence is not perfect and it is not a science[65], mistakes within an organization as a whole could occur. But the different schools differ in the way that they look after the main responsibilities of the failure and how both schools face the different scenario of the threats of the 21st century t and the changing characteristics of these threats as terrorist.

Despite the traditional focus of intelligence failures being on the analytical process, today it is fundamental to face new threats with effective collection in vast networks. In discussing the new threats, one of the main problems is the collection of information rather than the analysis of them. These new threats are very much diverse, therefore greater emphasis must be placed on identifying an adversary's intentions rather than its capabilities. It is of greater difficulty to assess the intentions of a terrorist group rather than its capabilities. Although there may be strategic indicators of terrorist threats one would expect to see fewer tactical intelligence indicators of terrorist attacks. Human intelligence will therefore be vital in collecting information on these new kinds of threats.

Bibliography

Journal articles

Allison, Graham T.: "Conceptual Models and the Cuban Missile Crisis". *The American Political Science Review* 63, No.3 (1969): 689-718.

Augustini, Jeff: "From Goldfinger to Butterfinger: The Legal and Policy Issues Surrounding Proposals to Use the CIA for Economic Espionage", *Law and Policy in International Business,* 26, No. 2 (1995) 459-495.

Bell, J. Bowyer: "Toward a Theory of Deception", *International Journal of Intelligence and Counterintelligence,* No.16 (2003), pp. 244-279.

Ben, Zvi Abraham: "A conceptual framework for the analysis of surprise attack", *World Politics,* XXVIII (April 1976).

Betts, Richard K.: "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable". *World Politics,* 31, No.1 (1978), pp. 61-89.

—: "Surprise Despite Warning: Why Sudden Attacks Succeed", *Political Science Quarterly,* 95, No.4 (1980), pp. 551-572.

[65] Random, H. A.: "Intelligence as a Science", *Studies in Intelligence* (Spring 1958), p. 76. Declassified.

Brady, Christopher: "Intelligence failures –Plus Ca change", *Intelligence and National Security,* Vol. 8, No. 4 (October 1993).

Callamari, Peter and Reveron, Derek: "China's use of Perception Management", *International Journal of Intelligence and Counterintelligence,* No.16 (2003), pp. 1-15.

Chan, Steven: "The Intelligence of Stupidity: Understanding Failures in Strategic Warning", *The American Political Science Review,* 73, No.1 (1979), pp. 171-180.

Daugherty, William J.: "Behind the Intelligence Failure in Iran", *International Journal of Intelligence and Counterintelligence,* No.14 (2001), pp. 449-484.

Deconcini, Dennis: "The Role of U.S. Intelligence in Promoting Economic Interests." *Journal of International Affairs,* 48, No. 1 (1994), pp. 39-57.

George, Roger Z.: "Fixing the Problem of Analytical Mind-Sets: Alternative Analysis". *International Journal of Intelligence and Counterntelligence,* No.17 (2004), pp. 385-404.

Gunter, Michael M.: "The Iraqi Opposition and the Failure of U.S. Intelligence", *International Journal of Intelligence and Counterintelligence,* 12, No. 2 (2002), pp. 135-167.

Handel Michael: "Intelligence and the problem of strategic surprise", *Journal of Strategic Studies,* No.7 (3 Sep 1984), p. 230.

—: "The Yom Kippur War and the Inevitability of Surprise", *International Studies Quarterly* (September 1977).

Hopple, Gerald W.: "Intelligence and Warning: Implications and Lessons of the Falklands War". *World Politics,* 36, No.3 (1984), pp. 339-361.

Hulnick, Arthur S.: "The Downside of Open Source Intelligence", *International Journal of Intelligence and Counterintelligence,* No.15 (2002), pp. 565-579.

Jevis R.: "What is wrong with the intelligence process", *International Journal of Intelligence and Counterintelligence,* Vol. 1 (Spring 1986).

Johnson, Loch K.: "Preface to a Theory of Strategic Intelligence", *International Journal of Intelligence and Counterintelligence,* No.16 (2003), pp. 638-663.

—: "Spies", *Foreign Policy*, September (2000): 18.

—: "Analysis for a new age", *Intelligence and National Security,* Vol.11, No. 4 (October 1996), p. 663.

—: "Seven Sins of Strategic Intelligence". *World Affairs,* 146, No. 2 (1983): 176-204.

Kahn, David: "The Intelligence Failure at Pearl Harbor", *Foreign Affairs,* Vol.70, No. 5 (Winter 1991/1992)

Knorr, Klaus: "Failures in national estimates" *World Politics,* XVI (April 1964).

Lefebvre, Stéphane: "A Look at Intelligence Analysis", *International Journal of Intelligence and Counterintelligence,* No.17 (2004), pp. 231-264.

Levy, Jack S. "Misperception and the Causes of War: Theoretical Linkages and Analytical Problems". *World Politics 36,* No.1 (1983): 76-99.

Marrin, Stephen: "CIA's Kent School: Improving Training for New Analysts", *International Journal of Intelligence and Counterintelligence,* No.16 (2003), pp. 609-637.

—: "Preventing Intelligence Failures by Learning from the Past". *International Journal of Intelligence and Counterintelligence,* No.17 (2004), pp. 655-672.

Martin, Rachel S.: "Watch What You Type: As the FBI Records Your Keystrokes, the Fourth Amendment Develops Carpal Tunnel Syndrome", *American Criminal Law Review,* 40, No. 3 (2003): 1271+.

Mobley, Richard A. "North Korea's Surprise Attack: Weak U.S. Analysis?". *Journal of Intelligence and Counterintelligence,* No.13 (2000), pp. 490-514.

Nye Joseph S. and Owens, William A.: "America's information edge", *Foreign Affairs,* Vol. 75, No. 2 (March/April) 1996.

Pipes, Richard: "What to Do about the CIA", *Commentary*, (March 1995) 36+.

Poleat ,H George.: "The intelligence gap hypothesis an the process of surprise". *International studies*. Notes.3 (Fall 1976).

Pringle, Robert W.: "The Limits of OSINT: Diagnosing the Soviet Media, 1985-1989". *International Journal of Intelligence and Counterintelligence,* No.16 (2003), pp. 280-289.

Random, A.: "Intelligence as a science", *CIA Studies in Intelligence* (Spring 1958): 76.

Ransom, Harry Howe: "Strategic Intelligence and Foreign Policy", *World Politics*, XXVII (October 1974).

Rieber, Steven: "Intelligence Analysis and Judgmental Calibration". *International Journal of Intelligence and Counterintelligence,* No.17 (2004), pp. 97-112.

Russell, Richard L.: "Intelligence Failures; the Wrong Model for the War on Terror", *Policy Review,* 18 November 2004.

Shlaim, A.: "Failures in National Intelligence Estimates: The Case of the Yom Kippur War". *World Politics* 28*,* No. 3 (1976), pp. 348-380.

United States Commission on Organization of the Executive Branch of the Government (1953-1955): *Intelligence Activities: A Report to the Congress*. Washington: U.S. Govt. Print. Off, 1955.

Vital, David: "Images of Other Peoples in the Making of Intelligence and Foreign Policy". *International Journal of Intelligence and Counterintelligence,* No.16 (2003), pp. 16-33.

Wettering, Frederick L.: "(C)overt Action: The Disappearing 'C'", *International Journal of Intelligence and Counterintelligence,* No.16 (2003), pp. 561-572.

Books

Bar-Joseph, Uri (1995): *Intelligence Intervention in the Politics of Democratic States: The United States, Israel, and Britain*. University Park, PA: Pennsylvania State University Press.

Berkoviz, Bruce (1989): "The cycle of Intelligence", in *Strategic Intelligence*. Princeton, Princeton University Press.

Betts Richard (1982): *Surprise attack: Lessons for Defence Planning.* Washington D.C., The Brookings Institution.

— and Manken, Thomas G. (2001): *Paradoxes of Strategic Intelligence*. Frank Cass.

Brecht, Arnold (1959): *Political Theory: The Foundations of Twentieth-Century Political Thought*. Princeton, NJ: Princeton University Press.

Dahl, Erik J (2004): *Warning of Terror: Explaining the Failure of Intelligence Against Terrorism.* The Fletcher School, Tufts University.

Davis, James Kirkpatrick (1992): *Spying on America: The FBI's Domestic Counterintelligence Program*. New York, Praeger.

Foerstel, Herbert N (1991): *Surveillance in the Stacks: The FBI's Library Awareness Program*. New York, Greenwood Press.

Gillespie, Diane (1992): *The Mind's We: Contextualism in Cognitive Psychology*. Carbondale, IL, Southern Illinois University Press.

Handel, Michael (1985): *Military Deception in Peace and War*. Jerusalem, Magnes Press,.

— (1989): *War, Strategy and Intelligence.* London, Frank Cass.

Heidegger, Martin (1962): *Kant and the Problem of Metaphysics*. Bloomington, IN, Indiana University Press.

Herman Michael (1996): Chapter 13, in *Intelligence power in peace and war.* Cambridge, Cambridge University Press.

Hulnick, Arthur S. (1999): *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century.* Westport, CT: Praeger.

Kent Sherman (1949): *Strategic Intelligence for American World Policy*. Princeton University Press Princeton, New Jersey.

Klee, Robert. (1997): *Introduction to the Philosophy of Science: Cutting Nature at Its Seams*. New York: Oxford University Press.

Kubálková, Vendulka, Onuf, Nicholas and Kowert, Paul (eds.) (1998): *International Relations in a Constructed World*. Armonk, NY, M. E. Sharpe.

Laqueur, Walter (1985): *A World of Secrets*. New York, Basic Books .

Levite, Ariel (1987): *Intelligence and Strategic Surprise*. New York, Columbia University Press.

Lowenthal, Mark M. (2003): *Intelligence from secrets to policy.* Washington DC, CQ Press.

— (1992): *U.S. Intelligence: Evolution and Anatomy*. Westport, CT, Praeger.

—: "The Burdensome Concept of Failure", in Maurer, Alfred C., Tunstall, Marion D., and Keagle, James M. (eds.) (1985): *Intelligence: Policy and Process*. Boulder, CO, Westview Press.

Marchetti, Victor and Marks, John D. (1974): *The CIA and the Cult of Intelligence*. New York, Dell.

Maurer, Alfred C. and Keagle, James M. (1985): *Intelligence—Policy and Process*. Boulder, CO, Westview Press.

Oseth, John M., and Hilsman, Roger (1985): *Regulating U.S. Intelligence Operations: A Study in Definition of the National Interest*. Lexington, KY: University Press of Kentucky.

Overton, Willis F (1990): *Reasoning, Necessity, and Logic: Developmental Perspectives*. Hillsdale, NJ, Lawrence Erlbaum Associates.

Richelson, Jeffrey T. (1995): *A Century of Spies: Intelligence in the Twentieth Century*. New York, Oxford University Press.

Sarbin, Theodore R., Carney, Ralph M., and Eoyang, Carson (eds.) (1994): *Citizen Espionage: Studies in Trust and Betrayal*. Westport, CT, Praeger.

Seliktar, Ofira (2000): *Failing the Crystal Ball Test: The Carter Administration and the Fundamentalist Revolution in Iran*. Westport, CT, Praeger Publishers.

Shulsky, Abram (1991): *Silent Warfare: Understanding the World of Intelligence.* Brassey's.

Stanger, Roland J. (ed.) (1962) *Essays on Espionage and International Law*. Columbus, Ohio State University Press.

Treverton, Gregory F. (2001): *Reshaping National Intelligence for an Age of Information*. Cambridge, Cambridge University Press.

Valcourt, Richard R., and Hulnick, Arthur S. (1999): *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*. Westport, CT, Praeger.

Van Dyke, Vernon (1960): *Political Science: A Philosophical Analysis*. Stanford, CA, Stanford University Press.

Wolsteller, Roberta (1962): *Pearl Harbour: Warning and Decision.* Stanford, CA, Stanford University Press.

Zegart, Amy B (1999): *Flawed by Design: The Evolution of the CIA, JCS, and NSC*. Stanford, CA: Stanford University Press.