International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 9 No. 2 Nov. 2014, pp. 906-912
© 2014 Innovative Space of Scientific Research Journals
http://www.ijias.issr-journals.org/

Preventing the surprise attacks by warning and others indications provided by the intelligence

Dr Dicko Abdourahamane

Université de Zinder, Niger

ABSTRACT: The warnings provided by intelligence are the backbone of any antiterrorist device, as it seeks to remove the element of surprise on which terrorism draws to hit and hurt. By definition, terrorism is effective in the abruptness and unpredictability of its shares, more than in its destructive capability. The effectiveness of an attack is based primarily on the shock set up within a group or society. We will go even further by saying that direct damage caused by the terrorist act (victims, destruction) are less important than the psychological impact it generates. Regarding Threats of warning, the central analytic task is to peel back substantive Uncertainty about the Meaning of Past Developments and the prospects for future world Developments That Could Endanger interest. Prescient, timely, convincing analysis imminent and potential dangers Regarding Can Be important year for the world Officials multiply force by Reducing the likelihood, first, of incident surprise and, second, of inadequate defensive Preparedness for Effectively dealing with high-impact potential Threats. The notion of warning is responsible for interpretations, and that the wave warning system plays its full role we have already mentioned above, it is important to make a semantic distinction between tactical warning and Strategic warning. The tactical covers everything or dangers that threaten the security of the world (military attack, terrorism, WMD developments, illicit transactions, and political crises abroad). How to analyze and assess risks is the central question that the tactical warning should provide clear answers.

KEYWORDS: terrorism warnings, indications, surprise attack, intelligence, prevention.

1 INTRODUCTION

The end of East-West antagonism accompanying the fall of the Berlin Wall in 1989 and the terrorist attacks against the United States September 11, 2001, bring the world in new era. The confrontation between the two blocks where each of the protagonists knew and his enemy against whom and what it fought, has given way to a situation largely disturbed by the emergence of new dangers, from actors ever more numerous and very difficult to predict. New forms of economic rivalry, transnational criminal organizations, violent extremists, appeared at the same time that globalization and today represent a major threat internationally. But in recent years, it is Islamic terrorism become our central concern. This represents the threat with the strongest power to harm. The 3000 deaths of the attacks of September 11, 2001, and the hundreds of victims to mourn over the world each year, terrorism make this element of destabilization potentially the most formidable, as the most newsworthy. This diffuse opponent, ill-defined and properly using all possibilities offered by globalization in the broadest sense (including those from the revolution in information technology), evolves into a new environment, characterized by either the ideological confrontation but by the overlap of issues and the proliferation risk. The break with the Cold War period is complete. Today, the first threat is primarily asymmetrical and it requires reconsidering the means obtained in defense and security of States, to continuously adapt. Thus, the fall of the Berlin Wall, but even more since the attacks in New York and Washington in 2001, states and international organizations, have undertaken to upgrade their devices to fight against terrorism.

The adaptability of Islamic terrorism is very fast, it is his greatest strength, and is an ongoing challenge for those who fight it. Anticipation is key and vital intelligence to prevent terrorist operations and thwart. It is virtually the only effective way to prevent these actors take action. Intelligence agencies, responsible for collecting, analyzing and transmitting useful information to policymakers, therefore become very important. They have to adapt, to emerge from decades of Cold War that had seen them grow and take shape under and around their original mission, namely a function of defense, turned on the outside and military purposes. But what place the intelligence occupies in the fight against terrorism? What is its role? What changes have occurred since September 11, 2001 and globally since the end of the bipolar world in 1989? What are the desirable and possible prospects for intelligence in the fight against transnational terrorism? At first, we'll see a general point of view what is intelligence, what are his means, his organization but also its specific countering. We focus on the post-September 11, 2001, which marks a real acceleration in the evolution of intelligence, to adapt to the threat of Islamic terrorism. Understand the measures implemented by the United States and international organizations to change the intelligence cycle, how have organized international cooperation, will some of our topics for discussion in this second stage. Finally, we will try to take stock and to create opportunities. What solutions can be envisaged to continue to advance the collection, analysis and transmission of information, as part of the fight against terrorism? Finally we discuss the ethical issues raised by the intelligence, but also its institutional control by its privatization, or future pathways offered by open source or the Intelligence-Led Policing.

2 The information and warnings: pillars of the Combating Terrorism.

Overview of intelligence

Definition of Intelligence

Intelligence gathering is not new. It can even be considered one of the oldest human activities, knowing that it could take many different forms over time. This activity satisfies a need for knowledge or even curiosity about a thing, person, and group. However intelligence is distinguished from simple information from the moment it becomes an issue of power, and gives rise to the creation of methods, tools and services specific to its collection and operation. It is primarily an aid to decision making in various fields and varied: Economy, Industry, Diplomacy, Security, Defense, etc.., All are likely to use the information as part of their activities. Intelligence informs about the intentions of someone or an organization to have the autonomy and knowledge necessary for decision making and therefore the action.

2.1 Intelligence cycle and the notion of warnings

There are different types of approaches, but the intelligence cycle is organized around four major phases: definition of research. This is the expression of a need that in the case of counter terrorism emanates from political authority. The intelligence, especially the agent (or agents) therefore knows what to search for and in what direction. The action or the collection: This is the time of the search for the information itself, and various means by which it occurs (activation sources, illegal search). The exploitation / analysis: This is the work of analysts who must sort information useful, relevant and separate from the rest. Dissemination: This is the last phase of the cycle, or that the information collected is transmitted to policy makers who decide to run (or not) a share. It is in this phase that the information truly becomes a tool for decision. The information may be obtained from a variety of tools, methods, sensors from two main types of sources: the sources said open and closed source. The former are all means of information available to all, free or not. Today it is estimated that nearly 80% of useful information to intelligence agencies in the fight against terrorism, comes from these open sources, primarily the Internet. Sources closed to encompass all means of clandestine collection of information they are illegal or not. The essence of this closed source based on the secret, the discretion is important and is not spotted by the target. The ways of research have dimensions: technical and human.

The technical information consists essentially of two areas: signals intelligence (SIGINT Signal Intelligence) which includes both electronic intelligence (ELINT, electronic intelligence) and intelligence community (COMINT Intelligence community); Imagery intelligence (IMINT, Image Intelligence). Inside each of them, it is possible to establish other categories employed by the specifically means: Intelligence laser signatures electromagnetic, optical, acoustic, photographic, radar. The technical information most commonly used aircraft, satellite systems (satellites, UAVs), cryptography and wiretapping COMINT (Communication Intelligence). Most nations of the Western world have a special department of technical information, or an interception system. Like examples, we can note the GCHQ (Government Communications Head Quarters) in Britain, the NSA in the U.S. and the FAPSI in Russia. The benefits of information technology are manifold: it provides concrete information, reliable, near real time and anywhere in the world while avoiding the difficulties inherent in the political, geographical or environmental context. Especially the collection of information can be done without endangering human lives, and without being detected by enemies (Human Intelligence (HUMINT or HUMINT). It’s obtained through intelligence agents using the methods of collecting legal or illegal. It encompasses both the information acquired by a conversational mode in which a human sensor interrogates a source, and the information obtained by observation without contact with the opponent. Human intelligence includes the name MICE: Money, Ideology, Forced, and Ego by reference to four main methods of collection used by HUMINT: Money describes the purchase of information by paying money. Ideology refers to obtaining information by sympathy or ideological conviction. An individual agrees to transmit information to the enemy because he rejects the values of society or government. The force requires the use of methods of blackmail, intimidation or torture (though it concerns specific cases), to obtain information. Ego means an individual lure by flattering his ego, his megalomania by maintaining and / or promising him a large personal recognition.

2.2 SPECIFIC INTELLIGENCE IN THE FIGHT AGAINST TERRORISM

Intelligence is the lifeblood of every anti-terrorism system because it seeks to remove the element of surprise on which terrorism draws to hit and hurt. By definition, terrorism is effective in the abruptness and unpredictability of its shares, more than in its destructive capability. The effectiveness of an attack the first is based primarily on the shock set up within a group or society. We will go even further by saying that direct damage caused by the terrorist act (victims, destruction) are less important than the psychological impact it generates. As its name implies, terrorism means terrorize, cause doubt and fear in a population. It’s a multifaceted and diffuse threat that accounts the post-bipolar world; it’s probably the most emblematic. Today the main challenge for security forces and defense policy is to first find the enemy, even before to consider obtaining more precise information on it, to take action to counter it. The threat is not only unpredictable, it’s transnational. At a time when terrorism knows no borders as well as its targets for its locations, the concept of sanctuary land is no longer relevant and intelligence gathering, but also cooperation between the departments concerned, whether within the state or between states themselves, has become an absolute necessity and priority. It has also greatly expanded since the end of the Cold War and since September 11, 2001. In this context intelligence, information transmission is absolutely central. Regarding the fight against terrorism, intelligence has to understand the networks, in order to know their capabilities, motivations, operations preparation, potential targets, etc. It’s the center of any action against terrorism, and any judicial or police operation can be initiated without the input of intelligence, whose primary mission is to find that invisible opponent.

The information acts upstream of terrorist action, in logic of prevention, to allow police to break up operations in preparation, disrupt networks. But it’s also present downstream that support action against armed groups (military intelligence plays a central role), assist police in investigations for the condemnation of criminal’s actors. The strengths and intelligence unlike its weaknesses in fighting terrorism, compared to other types of actions that can be taken against terrorism (police, judicial, military).Technical intelligence overcomes the impossibility almost total infiltration of terrorist networks, are structures extremely tight. But it requires the acquisition of technology often expensive and highly specialized that few States in the world are able to fund. In addition, it delivers information frozen in time from which it’s difficult to extrapolate and obviously it cannot reach the underground area in which many terrorists find refuge. But the major drawback comes from the amount of information, which is now far greater than the analytical capabilities of the intelligence services; Communications are too many each day.

Human intelligence is based on means of raising humans who can anticipate the intentions and explain the actions of the opponent. They provide access to factual information which, contrary that one obtained technically can fit into a global environment and then allow a better view and an assessment in situations of crises or problems whose complexity and dispersion have become the dominant features. In addition, as part of the fight against terrorism specifically human intelligence proves relevant to the technical information. Indeed, many network members have returned in recent years the use of basic communication modes based on oral transmission or through present standard technologies (eg walkie-talkie). They understood that they would benefit from an option allowing them to protect their activities, without being spotted by the intelligence services, who themselves have largely tended to focus on technical means of interceptions in the last decade. But human intelligence also has significant weaknesses. Firstly it involves men and women in sometimes very dangerous situations. More importantly, the collection of information by the infiltration of networks is virtually impossible, especially for Western officers. Indeed the Islamist terrorist networks, including work in an extremely narrow. The members have known for years and often they come from the same regions or even the same villages, speak the same dialect, infiltration is practically impossible for intelligence agents and especially extremely dangerous.

3 WARNINGS FACING THE EMERGENCE OF NEW THREATS AND NEW ACTORS

The fall of the Soviet Union ended the ideological confrontation that had endured for nearly 50 years. But the desired stabilization of the world is not achieved and contrary, crises and conflicts are developed. The economy emerged as the major area of competition between nations and new non-state actors emerge on the margins of the States (there are rather non-governmental actors who assist the State, NGOs in the first place). During the history, the United Nations has always been disputed whether by religious group's opposition movements. These new threats disrupt deep international politics and therefore the practice of intelligence.

3.1 The Types of Threats

The new threats that disrupt international politics and the practice of intelligence are:

Islamic terrorism: personified by Al-Qaeda terrorist organization, is a new type which is not supported by any state. But Al Qaeda is primarily a central support, in which there is no hierarchy nor truly concerted strategy, and showing no territorial claim. Only targets and inspiration of the fight against the West are common to different cells or subsidiaries claiming the organization worldwide. Some experts even argue that it fulfills a symbolic role for apprentice's terrorists. The fact is that Al Qaeda is present in over 60 countries, and its power to harm indisputable

Transnational crime: As Islamic terrorism, it took advantage of all opportunities offered by globalization, especially those from the revolution in information technology and the democratization of transport. Indeed, thanks to globalized economic networks, it could develop its business relating to the international level, arms trafficking, drug, human and sometimes representing nearly 6% of the global economy. These criminal organizations are a strong source of instability especially in areas where the state is built on shaky foundations. Indeed, their primary purpose is not in the conquest of power for political purposes. But indirect control of territories gives them the upper hand on institutions and on companies. Weaken the state is a way for them to establish their business and maximize profits

Proliferating technologies: nuclear proliferation, always present in this post-Cold War world despite having changed. Indeed, it remains one of the major concerns of the international community. Today, the most feared risk is no longer a major nuclear confrontation that could jeopardize the survival of a part of humanity but a terrorist act perpetrated by means of an atomic weapon. At the Wall, equipment and fissile material disappeared from former Soviet facilities, and a number of scholars have put their experience to proliferating states. If currently producing a nuclear weapon remains at the stage of science fiction since the process requires resources and know-how that only states are able to mobilize, its flight is a dangerous assumption and very realistic. And an attack through a dirty bomb containing fissile material is also the realm of possibility. But other types of proliferating technologies such as biological, bacteriological and chemical methods are equally likely to be employed in an attack.

The new economic rivalries: the end of the bipolar world and the advent of globalization have shifted the competition between nations, from military to economic. Today, more than the power of his army, the economic influence of a country determines its position internationally. To integrate this profound change, the Western intelligence services have also shifted their activity from the 90s.

Competition for access to resources and energy policy: It relates particularly oil (but also gas) that can cause tension in some cases open conflicts between states not only to ensure its operations but also its transit. This will be probably even more in the future, as resources will diminish and will make this material an even more coveted than it is today. Many interns or regional conflicts in the world concern these issues. It can also be an indirect vector of rising tensions. China has significantly increased its military budget in recent years to ensure security of energy supply. Because overall competition between countries to access these materials means reinforcing safety and therefore to develop their military forces, which has the effect of creating fear among the states and creating tension .

4 US Intelligence vulnerability before 9/11

Americans based their information gathering electronic espionage by considering the pursuit of traditional intelligence, as obsolete, expensive and dangerous, diplomatically. They neglected the infiltration of Islamist networks in favor of an electronic surveillance. The budgets of the intelligence services (especially human intelligence) have been seriously reduced. Today, they are looking for help from the public to glean intelligence since their budgets cannot fill their gaps. On top of that, although aware of the risk of terrorism, Americans were primarily focused on the risk of chemical or biological attacks, or new risks related to cybercrime. Air terrorism was not their concern. Some U.S. intelligence experts attribute the reasons for this failure on the bureaucratic hurdles and regulatory constraints associated with it the rivalries between intelligence agencies, the lack of resources and poor coordination for sharing information between the various intelligence agencies. Others cite the lack of qualified staff and a culture of intelligence. They also accuse intelligence officers and the officers responsible for enforcement who didn't take enough risks with numerous alerts, to prevent attacks of September 11.

4.1 LACK OF PERSONNEL TO ANALYZE INFORMATION

The U.S. intelligence agencies, like most intelligence services of the world are inundated with information and there are not enough actors qualified to process this information and make it useful. American intelligence falls down into the trap of the information paradox. This paradox is generated by the rise of information technology. On the one hand, we witness the increasing availability of information; the information technologies greatly facilitate the collection and storage of information, whether from the wiretap, sensors and satellites. But, on the other hand, these technologies generate perverse effects as a proliferation of data sources and too rapid growth of the importance of these technologies. The intelligence services should have foreseen that the glut of information would require an extremely laborious. too much data and information to be processed, but not enough qualified actors to analyze them. The authorities are overwhelmed and become unable to meet the challenges of technology. American services have almost all the necessary information on the terrorist threat, but they were unable to process it, analyze it and pass it into a product relevant to policy makers. A U.S. intelligence expert quoted by The New York Times, June 9-10, said "We did not know what we knew." In other words the U.S. intelligence services were unaware they have in their drawers a lot information about Al Qaeda and bin Laden. Not treated their pus masses of information, this information has served only to see the damage.

4.2 CONFLICTS AND LACK OF COOPERATION BETWEEN AGENCIES AND LACK OF RESOURCES

The information acquired by one agency may be kept secret and not necessarily transmitted between agencies. The FBI and the CIA had all the pieces of puzzle but they were unable to meet because of lack of cooperation between them. In addition to this lack of cooperation there are red tape (which complicate the searches and arrests of suspects) and the lack of resources. The U.S. intelligence agencies, including the CIA, do not currently have enough agents to infiltrate terrorist groups. The failure of American espionage is edifying. The CIA does not have a single Arab officer with real skill and a Middle Eastern culture that can pretend to be a fundamentalist Muslim and would volunteer to penetrate terror networks. September 11 has in fact proved, alas very tragically, the difficulty of intelligence and U.S. Securities send a common picture of the threat, mainly due to a lack of cooperation and communication. Better sharing of data would probably (but not with certainty) allow an increase of vigilance, and therefore a reduced risk. According to Tom Ridge, the first director of the Department of Homeland Security: It is the lack of communication between U.S. intelligence agencies before September 11 which can partly explain why the threat was not perceived at fair value and that Operation could not be countered. It is also indicative of the great difficulty of a large bureaucracy to adapt to a rapidly changing environment.

Faced with this failure, the explanation most frequently cited indicated that the United States intelligence dropped human intelligence and focused their energy on technological formations. But it's more likely that the excessive preponderance of tactical intelligence on/over the strategic intelligence is the determining factor. In the United States before 9/ 11, many intelligence agencies have tactical and very specialized competence. There are few analysts who have a strategic overview of the terrorist phenomenon and can see things that analysts can’t determine. For example, the FBI before September 11 has ten tactical analysts for a strategic analyst. And this deficit has considerably limited analytical capabilities of the political world to understand the nature and intensity of the problem and make decisions. The lesson learned from 9/ 11 shows that the anticipation of the tactical action is often impossible, which gives a strategic anticipation role. Not the American intelligence only is concerned by this observation because 9/ 11 signaled the bankruptcy of an entire system.

4.3 THE ROLE OF WARNINGS IN THE PREVENTION OF TERRORIST ATTACKS

The world faced new threats, primarily the threat of terrorism, but also weapons of mass destruction, proliferation, illegal trafficking, etc. That is why the Intelligence Community must also evolve and adapt via a new strategy that emphasizes collaboration between relevant agencies but also by integrating the businesses that can contribute also to national security. The charge has been repeatedly made after September 11. The failure of the international security system is primarily the lack of collaboration, dialogue between the intelligence agencies. The terrorist threat has placed the information in the center of national security concerns. Its effectiveness has become essential in preventing attacks. The intelligence services obviously remain discreet about their activities; have seen their interest increased with the strengthening of credible terrorist threats after 2001. Major issues of security and the fight against terrorism are actually indeed the center of the action of American intelligence. Emphasis is first placed on the identification of threats, for example by monitoring electronic communications. Three key questions emerge: coordination of intelligence services, which fall within the Ministries of Defense, Interior and Finance, strengthening the means allocated to them and cooperation with foreign partners. The development of their action about anti-terrorism policies also raises more acutely the question of their control, particularly with the senate. The intelligence services are actively engaged in fighting terrorism. The document on National Strategy for

Homeland Security for example developed and updated after the attacks of 11 September by the Government about the internal and external US security recalls the importance of the continuous adaptation of the American system. In the prevention of risk, it places particular emphasis on capacity building of the intelligence services and security. The effectiveness of intelligence and police are the ability of these services to anticipate the violent action and to analyze all the mechanisms that contribute to the development of the phenomenon of terrorism and other criminal activities to better address them. This justifies the improvement of monitoring capabilities of electronic communications, facilitation of access by intelligence and security to certain administrative data and to better identify dangerous travelers. The notion of surprise attacks appears repeatedly in the debates. Its success proves that it expresses an intuition shared by many, although it suffers from a lack of conceptual strength. Indeed, the notion of uncertainty (surprise) that strategic perspective is: any strategic situation involves an element of uncertainty, not least because it brings into confrontation actors with different interests, varied means and so many initiatives. Basically, the strategy is always to produce strategic calculus facing uncertain situations, the decision makers to choose actions that improve their situation. There is much truth in the notion of strategic surprise, the truth should be revealed. The concept of surprise is actually quite old: from the Cold War in retrospect thought as a stable situation, everyone feared a surprise, with such a nuclear surprise attack that could upset the existing strategic balance. The concept has changed for example, in the 1990s, to fears of a major computer attack. In such catastrophic scenarios, considering this concept of decisive battle that remains, it must be remembered a very questionable concept and little discussed. However, the sharpness of strategic surprise peaked September 11, 2001. The specialists were already discussing asymmetric wars over symmetrical wars. However, no one had seen the emergence of a brutal hostile actor who suddenly succeeds in becoming the number one public enemy and polarize towards it hostility of the world in general and American in particular. This war against terrorism and organized crime has burdened the strategic debate for ten years, and we are just beginning to liberate ourselves. A mode of action based on the psychological effect, especially if it’s obtained by surprise, no longer works: first we are neither surprised nor psychologically reached (even if we can be shocked, because it is not to deny the feelings of victims). Brice makes a major contribution in understanding the phenomenon of surprise attack. The mapping of this enigmatic problem by Brice allows us to identify all the nature and status attacks. He clearly identifies the types of actors: non-State and State and the kind of war: Conventional and unconventional, (Brice, 2003, 8) another factor that does not appear in the matrix and that Brice himself admits is playing important role in the determination of surprise, is the error calculations. He said the wildcard in Assessing << year's adversary intentions and the likelihood of miscalculation >> surprise is. The perception appears in this dialectical logic, as a critical variable that provides explanations to the problems of miscalculation. So Brice simply argues that to understand the problem of miscalculation must first understand the perception. The human cognitive competence is subject to two influences, conscious and unconscious. We'll just have to understand that not all information collected overstaffing that are obvious, complete and truthful. Some information is often false, unfounded. When we base our analysis on such information, we inevitably fall into errors of calculations. Perception is therefore a factor which can make and win a war. The father of the Observation-Orientation-Decision-Action (OODA loop), John Boyd strongly supports this idea and we will admit with him that only Humans fight wars and that other factors such Circumstances, land, and no weapons are not sources or priorities. The importance of information for intelligence is the second aspect on which Brice has directed his thoughts. This analysis is practically important and deserves to be included in this analysis that I present. The importance of intelligence in preventing criminal acts is accepted by all, but we have difficulties to formalize the basis of rational use of accurate intelligence. The major responsibility of intelligence is to collect data and provide information to decision makers. Brice, present in this paper the different levels of information. In this representation pyramidal submitted by Brice, we distinguish five levels hierarchy information: Truth, Wisdom, Knowledge, Information and Data.

In the Jack Davis analysis, we find a role devoted to intelligence. According Jack, the intelligence analysis must fulfill two main tasks. Both tasks are, to warn about the dangers US Officials to national security and to alert them to Perceived openings to advance US policy objective (Jack Davis 2003, 3). Also, we totally agree with Jack, when he asserts that << Regarding Threats of warning, the central analytic task is to peel back substantive Uncertainty about the Meaning Of Past Developments and the prospects for future US Developments that Could Endanger interest. Prescient, timely, convincing analysis imminent and potential dangers Regarding Can Be important year for US Officials multiply force by Reducing the likelihood, first, of incident surprise and, second, of inadequate defensive Preparedness for Effectively dealing with high-impact potential Threats >>. The notion of warning is responsible for interpretations, and that wave warning system plays its full role we have already mentioned above, it’s important to make a semantic distinction between tactical warning and Strategic warning. The tactical covers everything or dangers that threaten the security of the United States (military attack, terrorism, WMD developments, illicit transactions, and political crises abroad). How to analyze and assess risks is the central question that the tactical warning should provide clear answers. This analytical perspective will provide the event, to confine and contain the damage. The second tactic is called strategic. The strategic tactical main objective, policy development, coordinated, reliable which can defend and manage potential emergencies. Finally, we will retain the collection, analysis and transmission of information is absolutely vital intelligence. Yet the rules, mechanisms and practices are still too often marked by the period of the Cold War, and prevent or limit sharing. Must be redefined, and adjust it, finding the right balance between the need to produce the necessary information to decision makers and the risk that it could threaten the sources, methods, civil liberties or serve to the opponent . The plan proposes several initiatives: Create an information environment that is unique and common practice facilitate access and use of databases, developing an information technology with non-members of community, develop a single classification guide for intelligence.

5 CONCLUSION

9/11, was a huge shock to the world. The scale of destruction, the death toll, but also the huge psychological impact, gave this event a still unpublished which propelled terrorism, and especially the fight against terrorism at the forefront of international priorities. As we know, the responses to the attacks were organized around the American military interventions in the context of the war against terrorism in Afghanistan and Iraq but also in many other parts of the world. But beyond these important actions, reflecting overall development started to try to glimpse the reasons for the inability of U.S. authorities to anticipate and prevent these attacks. Intelligence and deficiencies regarding its transmission clearly emerged as the major elements of this bankruptcy. From on 9/ 11 emerged as the symbol of a world that had changed significantly since the fall of the Wall in the early 90s. These attacks marked the failure of intelligence and security could not understand a particular event (September 11), and beyond, have failed to properly fit the new situation of this post-Cold War world. In this new environment, characterized by threats emanating from now and transnational actors most often non-state, the information is of paramount significance for the entities entrusted with the defense and state security, including through the fight against terrorism. Changes were necessary and were undertaken around the world since 2001. The United States, has disputed the existence of major intelligence agencies (CIA, NSA, FBI, DIA) but they have already provided funding much higher than they were in the past in the field of terrorism against and intelligence. But mostly they have created the position of Director of National Intelligence (DNI) in order to establish a real exchange and share information internally but also externally with foreign services. 9/ 11 did not reveal the inadequacy of services to acquire information but their inability to pass them correctly and hence the overlap in order to anticipate and prevent attacks. But a general point of view, what conclusion, what conclusions can be drawn from developments that affected the information in the fight against terrorism since the events? In many cases, some progress has been made and the place overall intelligence is better today than it was several years ago. Not only its now probably the first pillar of the fight against terrorism, but beyond that, it has become a major element in the defense and state security. We understood that the information was probably the best defense against new threats that have developed from the end of the Cold War. But often the way interviews and plotted on a theoretical level could not be carried out in reality, or at least were not fully up to expectations, mainly due to the reluctance or slowness in within administrations or bureaucracies.

REFERENCES

[1] Brice, M., Strategic Surprise in an Age of Information Superiority: Is it Still Possible?, Alabama: Air War College, 2003.

[2] Davis, J., Strategic Warning If Surprise is Inevitable, What role for Analysts?, Washington, DC: US Central Intelligence Agency,2003.

[3] Tenet, Written Statement for the Record of the Director of Central Intelligence before the National Commission on Terrorist Attacks Upon the United State, 2004.

[4] 500 DAY PLAN Integration and Collaboration, United States Intelligence Community, 17p, 2007.

[5] Marchand., Intelligence : Led policing : Stratégie policière ou mission de renseignement ?, CF2R, 2p, 2007.

[6] Negroponte, J., Les services de renseignement sont mieux préparés, The Washington Post, 2006.

[7] Palluault,O.,. Le 11 septembre 2001, une rupture dans la pratique de l'anti-terrorisme, Technologie et Armement, 2005.

[8] Testimony of the Honorable Tim Roemer, Center for National Policy, Before the House Permanent Select Committee on Intelligence Subcommittee on Intelligence Community Management, 6/12/2007.