UNIVERSITY OF TARTU
Institute of Computer Science
Computer Science

Luis Alejandro Velásquez Hurtado

Colombia and the intelligence cycle in the 21st century, the digital age

Master's Thesis (30 EAP)

Supervisor Olaf Manuel Maennel

Co-Supervisor Raimundas Matulevicius

Tartu 2016

Colombia and the intelligence cycle in the 21st century, the digital age

Abstract:

The intelligence cycle is the main process in developing and obtaining intelligence used worldwide. Currently, it has problems and is outdated because it was not created to face the challenges that technology and the digital age have brought about. Information moves and travels in cyberspace, which are current as well as the future land of conflicts. The intelligence cycle is using technology systems through different forms of intelligence taking advantage of current technological developments for the search, collection, analysis and dissemination, but is not being fully exploited. Cases have been observed, where intelligence failed because of not following the intelligence cycle due to the speed of information or lack of knowledge of technological systems at the service of intelligence. The intelligence process must be integrated and work hand in hand with technology and the cyberspace, developing intelligence for the 21st century. It is necessary to use all resources and integrate all existing technological sources starting from the core of the process. A complete process that integrates the process of obtaining intelligence with the use and exploitation of cyberspace and information technology is required for increasing, securing and exploiting all available information. In the development of this thesis, a new process of micro cycles for intelligence has been developed. It consists of five micro cycles and its purpose is to integrate intelligence processes and technology for better results in this new era of intelligence development in 21st century.

Keywords: Process, Intelligence, Counterintelligence, Planning, Collection, Analysis, Dissemination, Micro Cycle, Technological systems, Cyberspace.

CERCS-code: P170

Kolumbia ja luuretsükkel 21. sajandil, digiajastul

Lühikokkuvõte: P170

Luuretsükkel on luureinfo analüüsimise ja kogumise peamine protsess, mida kasutatakse kogu maailmas. Kuna see süsteem on vananenud, siis ei saa see lahendada neid ülesandeid, mida tehnoloogia areng ja digiajastu on kaasa toonud. Info liigub küberruumis. Luuretsükkel kasutab erinevaid luureinfo vorme, tarvitades otsingus, kogumises, analüüsis ja levitamises kaasaegseid tehnoloogilisi vahendeid. Luures on teada ebaõnnestumisi, mis tulenesid sellest, et ei suudetud jälgida luuretsüklit info muutumise kiiruse või olemasolevatest tehnoloogilistest süsteemidest puuduliku teadlikkuse tõttu.
Luureprotsessi tuleb integreerida tehnoloogia ja küberruumiga, et 21. sajandil luurevõimet arendada. On vaja kasutada kõiki ressursse ja integreerida kõiki olemasolevaid tehnoloogilisi allikaid põhilistest protsessidest alates.
Täielik protsess, mis ühendab luureinfo saamise protsessi küberruumi ja infotehnoloogia kasutamisega, on vajalik selleks, et olemasolevat informatsiooni kasutada ja kindlustada. See uurimistöö pakub uut, luure läbiviimiseks mõeldut mikrotsüklite protsessi. See koosneb viiest mikrotsüklist ja selle eesmärk on luure protsesside ja tehnoloogiate integreerimine, et saada paremaid tulemusi 21. sajandi luure arengutes.

Võtmesõnad: Intelligentsus, Vastuluure, Planeerimine, Kogumine, Analüüs, Levitamine, Mikrotsükkel, Tehnoloogilised süsteemid, Küberruum.

CERCS: P170

Table of Contents

Table of figures

1 Introduction

The intelligence cycle is the main process for obtaining intelligence and is used daily in multiple operations developed in Colombia. Currently, the cycle faces serious difficulties and problems that are affecting the obtained result for intelligence organizations; the information is the mainstay of intelligence and moves into a new operating environment, the cyberspace. The cycle uses several stages throughout the management, evaluation and interpretation of information to finally deliver a product called intelligence. The problem is that now, during the new age or, better said, digital age, the technology systems are used for information management, including the intelligence, demonstrating that the intelligence cycle is obsolete for the development of intelligence in the 21st century.

In fact, all technology that is used in the management of intelligence information, either data or intelligence product is vulnerable and in risk. The intelligence cycle as a process does not integrate technology and cyberspace as main tools for the collection, analysis, production and dissemination of intelligence and is also losing the benefits that it delivers.

The speed at which information travels into cyberspace, the existence of cybercrime, and the lack of knowledge of technological systems are examples of the various factors that endanger the intelligence and influence the intelligence process.

That is why the cycle is required to be reviewed and redesigned under the light of technology and information systems, in order to deliver a better – more useful, clear, accurate, concise and safe – product of intelligence, for better results and successes in the development of military operations.

This research describes and analyzes the problems that the intelligence cycle has in its current operation, analyzing intelligence in the digital age or in the 21st century, in order to show what the intelligence cycle faces in the digital age. In addition, as the main contribution, a new process of micro cycles for intelligence is presented. The process of micro cycles involves and integrates technological systems and cyberspace into the process of producing intelligence, starting from the basis of the current cycle and using technological concepts that allow the integration of technology and cyberspace in the core of overall process of obtaining intelligence.

The theories, analyses and opinions of recognized global experts of intelligence who have studied the problems of the current cycle, coupled with my 10 years work experience in Colombian intelligence using current cycle process, analyzing these problems and employing real cases, will show the flaws of the current cycle: the lack of integration and preparation for the new operating environment in the 21st century. Problems in planning, collection, analysis and dissemination were observed. Also, a case of operational intelligence and the results will be analyzed and compared, using traditional cycle and the new process, and showing the need for the update of the main process of intelligence development.

The study developed in this thesis is mainly based on the intelligence of Colombia, where the current conflict is extremely complex and has several courses of action. The current cycle is widely used by intelligence agencies of Colombia as well as in other countries for operations and intelligence activities. Strategy military planning and security in Colombia is achieved through the means of intelligence cycle, the organization and management processes for decision-making and the approach of objectives that lead to military success.

Something very important to consider in the development of the thesis is that when intelligence is the topic of thought, a wide range of categories and types of intelligence must be covered. The intelligence cycle is an adopted process for handling intelligence; it is widely adopted not only in Colombia, but worldwide as well. This sole cycle is used by the vast majority of agencies in Colombia and the whole world. Still, it is possible to find different types of cycles with varying phases or steps on the web, for example, the cycle of Cyber Intelligence, which has been adopted for the structures that are particularly involved in this type of intelligence. Nevertheless, the intelligence is integrated and is a wholesome, unique process, regardless of the ultimate goal. Currently, all available means are used to obtain a satisfactory result, so it is necessary to speak of intelligence as a full body that draws from its different forms, types, and classes.

This thesis is aimed at improving intelligence processes in order to be implemented in Colombia, where a fight against subversion, terrorism, and drug trafficking has been evolving for more than 50 years and will continue to do so. Another aim of this thesis is to carry Colombia's intelligence to a new strategic level within the Latin American Region, taking into account country's potential threats.

1.1 Definition

The intelligence cycle can be defined according with Sherman Kent as "the systematic series of stages through which the intellectual work of generating new knowledge develops, useful, truthful and adjusted to the requirements of intelligence previously defined by a user or ultimate consignee" [1].

The intelligence cycle is the process during which information is gathered, it becomes intelligence and is made available to users. Intelligence preparation can be divided into four phases [2]:

- A Search effort planning intelligence
- B. Information collection
- C. Analysis
- D. Dissemination and use

The intelligence cycle is a scientific method, which is based on phases of organization for analyzing and creating intelligence, from the base of information gathering, where four or more mental and physical processes are planned and executed, seeking to obtain result for the development of operations. Its importance lies in supporting the establishment of a

systematic process of intelligence production. It is a core process, with its activities supporting the intelligence. In Colombia, the intelligence cycle is the process, which allows organizing the work of intelligence and support phases step by step.

The problem today is that intelligence mutated in all its forms and is highly driven by technological systems. The cycle is being overtaken by this new digital age since it is not designed for evolution with which information is handled and different current intelligence systems.

1.2 Methodology

The methodology developed in this thesis is the qualitative of projection that allows the use of personal experience in the field of intelligence and clear understanding of how it is developing intelligence work in the current age. Also were used into the investigation the texts of intelligence experts who with their important and outstanding experience have taught the existing problems in the intelligence of the 21st century. An exploration of the best literature was developed in order to determine what would be useful and valid literature to support the ideas, arguments and projections for the solution of the problems presented in the thesis.

Through this methodology, a detailed analysis of the influence of technology and cyberspace was done, within the current intelligence and thus build a solution that improves the current process to obtain intelligence.

The problems and solutions are validated by external support from knowledgeable on the subject. Experts, who have remained for years in the environment of intelligence (In anthropology). Additionally, experience and participation of the author of the thesis in the different stages that the intelligence cycle has, where he has worked in the field for the collection of information, is an intelligence analyst, and for his range has supported the planning and advising the Commander. Finally, he has developed operational tasks in technical intelligence within the Navy of Colombia in the implementation and projection of the cybersecurity of the institution.

2 Background and Literature Review

In this chapter will be showed the background about the Intelligence in Colombia, how is working the Intelligence in the 21 century? How the intelligence cycle does work currently? And, the literature review used for the developing of the thesis.

2.1 History of the Intelligence Cycle

In 1949, Sherman Kent published a manual to mark a milestone in the discipline of intelligence [1]. Since then, many more manuals have been published, but Kent is still considered to be the father of intelligence analysis.

Operations that years later would be encompassed and defined by Sherman Kent under the term *intelligence cycle* were actually already outlined. An example of that is the theoretical contribution to organized and systematic conception of information and espionage carried out by the second section of Republican staff during the Spanish Civil War. Diego Navarro Bonilla gives this important information about the history "Under the leadership of Colonel Manuel Estrada Manchon, numerous reports, methods of action and proposals for reorganization preserved allude a well-established theory and suggest a method of not inconsiderable intelligence from a theoretical and conceptual levels" [3].

Similarly, in many countries and in various conflicts, intelligence strategies were a part of what made similar processes Kent was an explanation of the scientific method for implementing a systematic process leading intelligence operations.

On September 1st, 1981, NATO agreed upon the definition for the Intelligence Cycle. At that time, geopolitical and technological environment was very different from the current one [4].

2.2 Colombian Conflict and the Intelligence

Colombia is a democratic nation state, where different internal and external factors involved in the armed conflict are present. Unlike other countries in Latin America and the Caribbean, Colombia has spent more than 50 years facing the situation when the government and institutions have been fighting against illegal armed groups and terrorists while civilian population has been in the middle of the struggle.

In spite of drug trafficking, terrorism, corruption and all kinds of social problems, Colombia has an internal struggle in search of peace and tranquility of its people. This struggle has been beyond its borders with neighboring nations where ideologies and political thoughts have served as triggers for various diplomatic crises (Venezuela, Ecuador, and Nicaragua) [5], One of the examples is the intervention and continued support of the Government of the United States, whose foreign policy is to have Latin America as its regional ally and to prevent countries like China, Russia and Iran among others, from affecting its foreign policy. Within the context of this combination of situations where the American government is not widely accepted in Latin American countries with great

influence of leftist ideologies, Colombia has become the spearhead of the US to maintain regional control [6].

Another factor, which adds to Colombia's internal conflict and influences its diplomatic relations is drug trafficking. Colombia is the source of financing for illegal armed groups like narco-terrorists, apart from being one of the main causes of corruption in the country; within the frames of their own war against drugs, the US support and contribute lots of resources to Colombia to fight drug trafficking. Narco-terrorists and illegal armed groups in the country use the borders with neighboring countries for illegal drug trafficking or as hideouts; in many cases they take refuge in the Marxist revolutionary ideology that is supported by neighboring governments, to the Colombian borders, and base their governments on these kind of ideologies [7].

Such illegal armed groups have used revolutionary speeches and international propaganda to be seen as political agents, marginalized by the Colombian government, but their actions include kidnapping, terrorism and extortion – their daily tools used to provide financing for illegal drug trafficking. In addition to that, there is the legacy left by drug cartels of the 80s, e.g., the Medellin cartel, which introduced corruption on national scale (politics, police, justice) for many years to come, summarizing in an agile way the complexity of the Colombian conflict for more than 50 years [8].

The national government with its military and police forces have implemented harsh reforms and worked in favor of institutional transparency. Institutions constantly fight against the abovementioned threats to provide compliance with the constitution and security of the nation, while intelligence military and government forces have developed an extremely important role they play in the society, for which many resources have been assigned in this fight [9]. The Intelligence in Colombia has progressively modernized in order to achieve strategic, operational and tactical objectives necessary in the fight against drug trafficking, terrorism and subversion, but it is far from attaining fluency in the entire spectrum of existing threats today and referring to cyberspace and information management. Furthermore, the disputes and disagreements with neighboring countries like Venezuela and Nicaragua have to be taken into account, as Colombia has ongoing trials with these countries in the International Justice Court of the United Nations.

Intelligence agencies need to develop technologically, which would allow them to use the intelligence in the age of technological knowledge in a more efficient way, gain strategic advantage over their enemies, and deal with the threats they are facing.

Currently, Colombia does not have a cyber defense strategy that protects the country and its critical infrastructure and information against the threats. Although the country is working hard to improve, still more focus resources and effort are required. The Intelligence works with different technological resources, but the processes like intelligence cycle are not shielded and do not protect the information handled.

In Colombia denotes as I. Duyvesteyn, B De Jong, and J van Reijn, in their book "Many countries that have devote intelligence resources to identifying subversive groups. …. In

countries where democratic government is less firmly fixed, the fight against subversion often becomes the main issue for domestic security services [4]."

That is why Colombia, its security agencies and intelligence must seize this historic moment when the peace agreement with the FARC (Revolutionary Armed Forces of Colombia) is being discussed, and the eyes of the world and the Region are fixed on Colombia; it shall also strengthen its technological capabilities and extensive knowledge of information that today is affected by various sources of technology. Not forgetting that it must continue fighting against other groups such as the ELN (National Liberation Army), the criminal gangs working for drug traffickers and especially the external threats that use espionage or cyber espionage against Colombia. It is also necessary to turn great attention to the new battlefield that is being waged, the cyberspace.

I. Duyvesteyn, B De Jong, and J van Reijn, expose important projection of the new age in Colombia and their conflict, "Penetrating subversive groups and placing key actors under surveillance are effective methods for countering subversion. More and more, subversion groups are using social media to rally their followers." [4]

By developing a strong cyber defense strategy and updating its intelligence processes, Colombia will shield its security and gain strategic advantage over its current and potential enemies [5].

2.3 Intelligence in the 21 Century

The information is currently being managed primarily in cyberspace through the internet and the web as well as via many services, systems and equipment which have come into being as a result of technological development in Colombia and in several countries, mainly in the United States; these systems are used to promote the collection, analysis and dissemination of information technology.

Several years ago, the largest amount of intelligence was being collected and produced via the use of human resources with intelligence agents in the area; at present, these same agents use technological resources to obtain information during the development of the specialized operations.

It is a well-known fact that intelligence is a wholesome process, but it is divided into several parts depending on the current needs. However, above all, today we can witness the great influence that the existing technological resources have within the world of intelligence.

In a wide range of sources, intelligence information is usually categorized in terms of various "INTs" [10] around the world and used in Colombia. Phythian describes according "As outlined by the CIA, there are six categories of these, involving a total of nine INTs [10]:

- Signals intelligence (SIGINT) "is derived by interception of signals comprising, however transmitted – individually or in combination, all communications intelligence

(COMINT), electronic intelligence (ELINT), or foreign instrumentation signals intelligence (FISINT)" [10].

- Imagery intelligence (IMINT) "includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics". [10]

- Measurement and signature intelligence (MASINT) is "technically derived intelligence data other than imagery and SIGINT." The data results in intelligence that locates, identifies, or describes distinctive characteristics of targets. "It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences". [10]

- Human intelligence (HUMINT) is derived from human sources. "Collection includes clandestine acquisition of photography, documents, and other materials; overt collection by personnel in diplomatic and consular posts; debriefing of foreign nationals and citizens who travel abroad; and official contacts with foreign governments". [10]

- Geospatial intelligence (GEOINT) "is the analysis and visual representation of security-related activities on Earth." It is produced through an integration of imagery, imagery intelligence, and geospatial information. [10]

- Open-Source intelligence (OSINT) "is publicly available information appearing in print or electronic". [10]

"However, it should be noted that collection methods are constantly evolving in response to technological developments, and these developments can also affect the manner in which collection methods are categorized for instance, separate categories can emerge within existing categories as technological change impacts the volume of material involved and results in increased specialization of collection methods [10]".

There are other categories that are being used. For example, Aaron Brantley suggests adding [10]"CYBERINT as a discrete collection category, but it is one of the new forms being used globally and in Colombia, as it allows obtaining information by using various technological tools and using them in cyberspace". [10]

Likewise, the use of various social sources for the service of the intelligence within the web or cyberspace understands of social media Phyhian also describes that David Omand called this new tendency as "SOCMINT – the collection of information from internet social media, as a separate type of collection, fuelled by the rapid growth of activity in this area. News media: Newspapers, magazines, radio, television, and computer based information. Web-based communities and user-generated content: Social networking sites, video-sharing sites, wikis, blogs, and folksonomies. Public data: Government reports, official data (such as budgets), demographics, hearings, legislative debates, press conferences, speeches, marine and aeronautical safety warnings, environmental impact statements, contract

awards. Observations and reporting: amateur airplane spotters, radio monitors, and satellite observers. Professional and academic: Conferences, symposia, professional associations, academic papers, and subject matter experts. Commercial data: Insurance companies, international aviation organizations, transportation and shipping companies". [10]

This is why the methods and processes have undergone an evolutionary change that allows obtaining information in an agile and fast way, providing steady real-time flow of information for analysis.

They must now carry out more exhaustive analysis that necessarily considers human and technological interaction, especially the underpinning concepts such as effects-based thinking and network centric capabilities. Such developments are not altogether unexpected. Globalization and the impact of the Information Age have changed society's expectations of what we want to know; when we want to know it; and what we do with this information. The military's subsequent embracing of such developments is entirely reasonable. [11]

Likewise, it is required to point out that the new age is making giant strides, where the available information is immensely accessible and available to all. A growing accessibility to repositories of data and information can inspire the development of operating concepts in order to maximize the opportunities for exploitation. [11]

While a multitude of civilian professions, governments and businesses all attempt to take the fullest advantage of the Information Age, it is in relatively conservative organizations such as the military that the ramifications will be more acutely felt [11]. This is why Colombia, just like other Latin American countries is facing the world of technology, and their military forces should concentrate efforts to systematize and update systems and processes which develop activities such as intelligence.

A new relevant aspect related to this renewal and modernization of intelligence systems is the cyberspace, the new land of war and the new conflict panorama, where most conflicts in this age of technology will be developed. The Cyberspace has opened a big door where everything moves differently, becoming a new battlefield, gaining the same importance of land, air and sea and is full of cyber threats where cyberterrorism and cyber-intelligence are fighting for possessing more information either for good or evil. It is clear that it must be defended and makes it operational.

2.4 How the Intelligence Cycle does works currently?

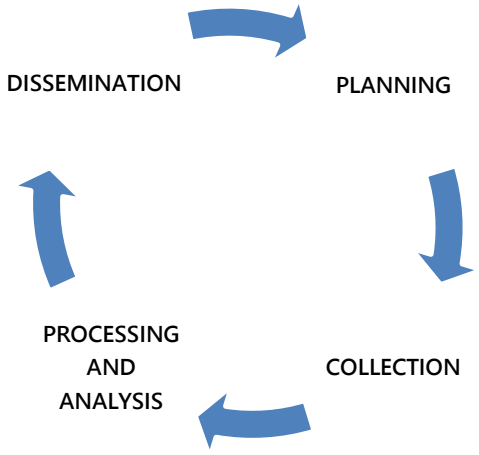

Figure 1 Current Intelligence Cycle

There are many ways to describe the current functioning of the intelligence cycle and you can find versions in different languages and with more descriptions as with other phases. Colombia is greatly influenced by the United States and many of its officers and NCOs (sub-officers) attend and have attended in that country for various preparations. This is why the most accurate description of how the cycle works was extracted from the Intelligence School of the Americas manual. Since the Intelligence Colombia manual is a classified document, the description shown below has been taken from the Intelligence School of the Americas manual.

"The intelligence cycle has 4 phases for obtaining intelligence and development operations, as described below. [2]

Planning

At this stage the needs are identified and the information they require recipients of intelligence at this stage are sorted and routed the objectives and targets high value required for mission accomplishment. [2]

Once the objectives set out, how to get the information is planned, a planning and organizational resources to obtain accurate occurs.

The strategic areas are set by identifying and ranking in priority levels of the policy areas of service and what information is desired, so set by the heads of the intelligence service and political bodies and, where appropriate, military they serve. The type and content of information that is available and the availability and reliability of sources and channels of communication is studied.

At this stage in the same way the participation of commanders and intelligence chiefs required and follow the guidelines of the security policy and military of the Force, Agency and Nation. It is required to be aligned with the national strategy. [2]

Collection

It is finding, obtaining and collection of the information necessary to produce intelligence, obtaining means are varied, and constitute the means and intelligence resources [2]:

- Through technical means
  - Interception of communications and strategic signals
  - Capturing images or satellite photographs
  - Microphones and other means of collection
- Through Human means
  - People who provide information to the center, and have positions in companies, agencies, factories, etc.
  - Through interrogations.
  - Follow-ups, infiltrations or specialized operations.
- Through the analysis of public information
  - Both mainstream media (newspapers, radio, television), and on the web or Internet.
- Through the data collected from other departments or agencies

  Or through other intelligence agencies or foreign body
- Others.

Analysis

Analysis and processing is the step by which intelligence is produced from data information. It consists of three steps: (1) recording of information for comparison with other items by hand; (2) assessment of information in order to determine the value of intelligence; and (3) interpretation of information concerning other information and intelligence hand in order to reach a conclusion as to its meaning. All this involves an assessment of all resources: decisions, external events, issues, geographical, political, cultural, economic, scientific, military, strategic or biographical, that cannot be ignored when dealing with information. The analysis is performed in three phases [2]:

1. The evaluation of the data is to discriminate which contribute to meeting the information requirements formulated in terms of reliability of sources, validity, timeliness, relevance, relevance and usefulness. [2]
2. The integration of data from different sources is based on a fundamental principle of intelligence: never accept a single information authority. It is getting a synergy where the combination of information from different means of obtaining a whole is most relevant and scope of the information each separately [2]. To describe the work of the departments of analysis. Integration can be a daunting and complex task when data from numerous sources have varied, so it is necessary to provide that much data and documents submitted to the lower levels of protection are spread horizontally among other analysts and departments. [2]
3. The interpretation of the data, with the dual aim of determining what is accurate and what is relevant to meet the political needs, which are usually alike, explanation and understanding of the phenomenon analyzed as a forecast about its consequences and predictable evolution. The interpretation is the task of experts in the field of analysis (politics, economics, technology, military, and terrorism) possesses both knowledge

and sufficient capacity for imagination and creativity to relate data, predicts events, and get into the mind of enemy. [2]

Dissemination

The next phase of the intelligence cycle is diffusion or dissemination and use of intelligence, which is the result of all intelligence activities. To be useful, it must be reported properly and in time the commander, his older and to those who need state. [2]

2.5 Problems of the Current Intelligence Cycle

In this section will be exposed the problems that has the Intelligence Cycle due the environment change, and what have been reviewed and analyzed for experts and their analysis**.**

2.5.1 Experts talking about the current Intelligence Cycle

The texts, documents and books consulted are the samples of existing analysis of the intelligence cycle and various intelligence processes that are used around the world by different agencies, including security agencies. The authors of these texts have experience in the area analysis of intelligence information and have been involved in intelligence cycle processes and systems.

There are debates about the problems of substance and form that in any case lead to faults and failures of intelligence, to misuse and misunderstanding of the phases that make up the intelligence cycle.It brings to light the weaknesses and problems that exist within the intelligence cycle to date, showing and evidencing the lack of knowledge and awareness, as well as obsolescence of existing operational environment in the 21st century.

In expert analysis that has been reviewed and will be described below, the technology supports the process and has become a priority in intelligence. The systems, tools, and equipment that are used in creating intelligence in all its phases and moments, are interconnected in many ways, but primarily within the cyber domain, the network and the Internet.

Intelligence information is collected, managed, analyzed by these systems and exchanged by people, for being within this international communication system, and is the core of the cycle and the process.

The text "*Sherman Kent and the profession of intelligence analysis*" [12], contextualize a historical concept, about intelligence, in the document the author allows to have a deeper and updated vision of the work done by Kent, and his contributions to intelligence and analyzing information to get to turn it into intelligence. This clearly describes the Processes That Kent developed to obtain the process of the intelligence cycle, and deeply ideas about analyzing the information. Moreover, the author talk about Kent´s during his work in intelligence and different works done in the intelligence structures, owing to which nowadays Sherman Kent is called the father of intelligence. [12]

This text is important in terms of the development of the thesis, for describing the concepts of information processing that were delivered by Kent, experience and knowledge that led to the development of the process to date and has addressed the work of intelligence and the process of information analysis. It also provides the knowledge of the history of the intelligence cycle.

In consideration of the method delivered by Kent, researching more thoroughly the current situation of intelligence and the intelligence cycle it was found that Arthur S Hulnick, whom could be said to be one of the main contradictory analysts dealing with the intelligence cycle in recent years in various texts and books, but mainly in his text "*What's Wrong with the intelligence cycle*" written in 2006 [13]. The text provides a thorough analysis of the main problems that the cycle has, since the world and intelligence are evolved in the digital age; A. Hulnick is a former agent of the CIA and analyst in the US air force, is a personage greatly respected for its expertise and experience, in intelligence, he is the author of another influential book on intelligence; "*Fixing the Spy Machine: Preparing American Intelligence for the 21st Century*" (1999) [13], which also shows the need to redesign and re-educate the intelligence in order to prepare for the changes that have been brought by the 21st century, mainly the technology. [13]

"*What's Wrong With the Intelligence Cycle*" [13], shows in context drawbacks, problems, weaknesses and vices that are typical of the intelligence and the current cycle of intelligence, talks about the problems that are typical of planning, collection and analysis information, the barriers that exist in the cycle and intelligence, also plays with the themes of counterintelligence, and covert operations arguing not to be parts of the cycle and the process. [13]

Following the idea that exposes Hulnick, there are various debates about the issues typical of the intelligence and its cycle. *The Future of Intelligence: Challenges in the 21st Century* [4] by Duyvesteyn De Jong and Van Reijn contributes to research in the area of intelligence, where theories, ideas and opinions of analysts and experts, are situated, in the book, issues of importance are taken, as new threats of intelligence and the world, the challenges which must be faced and opportunities that exist to face these threats. Just as, is studied the future of intelligence and the end of the current intelligence cycle, weaknesses and problems presented for decision making, analysis and production of intelligence. [4]

The book explains and puts on the table, major issues such as the importance of technology with the intelligence, this is presented as one of the threats in this new age of technological knowledge and the same time the advantages to produce intelligence with the use of technology and information systems alongside the cyberspace and the web, that are weapons and tools to strengthen the processes and the intelligence cycle, serving as tools to be used as an opportunity to face the different threats that has the intelligence and will confront in the future. [4]
The collection of these analyses supports the ideas, analyses and opinions set in the course of development of the thesis and clearly prove the importance of technology and its great contribution to modern and future intelligence.

In the text, "*Rethinking military intelligence failure-Putting the wheels back on the intelligence cycle"* [14]. By Evans, who is a renowned British researcher of military studies and defence, provides the evidence of the weaknesses that exist within the intelligence cycle and the relationship between commanders and their staffs, with the stages of the intelligence cycle, providing comparison between failure and success of intelligence operations related to the use of the intelligence cycle which has been observed. [14] Likewise, errors that are committed in planning and the relationship between the appreciations of the commanders as well as the results of the analyses delivered by the members of staffs are described; also, the author of the book speaks about changes in the operational environment within the context of the new information age. [14] The existent relation to the use of technology in intelligence processes and the flow of information on the net and the web, and how are affected all and each of the stages of the cycle and the members that are involved in this process. Puts in context the concept of intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) a process of closely related with the intelligence and which resembles the traditional intelligence cycle. [14]

On the other hand, although the author respects the arguments of Arthur Hulnick, he does not agree that the cycle is an outdated process, or that it no longer works, and he also disagrees with Hulnick to refuse to include counterintelligence, within the process of the intelligence cycle. [14]

The text allows for another point of view on current problems and weaknesses that exist within the intelligence cycle, in addition to supporting the idea of changing operational environment in which the intelligence is functioning with the use of technology in this new era of the 21st century. [14]

The text, "*Best Practice: Intelligence in the Information Age"* was also analyzed to continue the argument of the need to redesign the cycle of intelligence within a technological environment. [11] It is a document that allows have a clearer picture of the interaction of intelligence with technology, and with the use of technological systems in intelligence, is sought that the intelligence community mainly in US understand, how is the information into this new digital age?, [11] where all the information management is involved with information systems and web. In addition, the management of the information should be aware of the advancement of society, particularly the private sector, which is an example as first user of the intelligence technology when is required. [11] On the other hand, the text exposed the issue of counterintelligence that is taken as a process of searching and analysis information, in which the intelligence cycle is used but with some flaws. [11]

The technology in the new age is the pillar which allows the information to move. The information is processed, managed, and countless other activities are performed across the net and, the information systems. It is when the concept of cyberspace is enhanced; this entails that the intelligence is linked strongly to this technology in the 21st century, and this text tells the readers about the current symbiosis between intelligence, the cyberspace, and the digital age. [11]

Furthermore, it is important to comprehend what happens within the intelligence cycle. The text "*Understanding the intelligence cycle*" by Mark Phythian, analyzes the concept of the intelligence cycle shows its nature and different characteristics possessed by the intelligence and the process of the intelligence cycle, showing the importance of the cycle in the evolution of intelligence for many years. [10] Then describes different types of intelligence that currently exist and how they are related to the process of collection and analysis of information that is used in intelligence, demonstrating a better way to use computer networks and the cyberspace in the current intelligence. On the other hand, he also makes a comparison between private, business and military sectors, describing their characteristics, advantages, and disadvantages and uses. [10]

The author together with other experts prove that the intelligence needs to evaluate the use of intelligence technology systems to take advantage in this age and puts the idea in the context of the death of the intelligence cycle. [10] It should be pointed out that this text discusses the idea of the enhancement of Cyber Intelligence as well as that the cyber world excels into today's culture, thus allowing new threats and challenges to the intelligence community. [10] The use of the cyberspace and the Cyber Intelligence is analyzed where is required take advantage of using of networks and social media to increase and outstrip new threats that arise in the world. [10]

Important issue mentioned are the limitations of the current cycle of intelligence within the cyber world, where activities such as counterintelligence and undercover operations are extremely important for the development and dominance of the cyberspace. [10]

"The intelligence cycle: a differentiated perspective on information processing" by Peter Keen, it focuses on the use of analysis systems of information and its importance in helping to understand and analyze the data that analysts receive in all fields of intelligence. [15] Here the complex processes that possess the collection of information are described for its subsequent analysis where the information is surpassing the mental capacities of analysts and operators that are facing the problem of analyzing the amount of information that exists since the time when technological knowledge has opened the spectrum of the flow of information through computer networks. [15]

The paradox of man vs. machine is exposed, where a human being is limited by multiple characteristics of human nature, and the machine serves as an aid to support the understanding of the vast multitude of existing information. The needs that require intelligence and the cycle to lean on technology, using information analysis systems and other developments, are shown. Is studied, the complexity of the cycle is studied, to support the intelligence activity in the management of intelligence to decision-making. [15]

"The intelligence cycle is dead, long live the intelligence cycle: Rethinking intelligence fundamentals for a new intelligence doctrine" by Davies, Gustafson and Rigden. [16] This document is a collection of ideas, opinions, debates and solutions of the thinkers and experts around the cycle, but mainly is an analysis of the intelligence cycle. Several texts of the above-mentioned authors are referenced here. They talk about different existing standards within the cycle or intelligence processes, as used in Colombia and NATO,

DCPD (management, collection, processing and dissemination). [16] It is worth noting that the authors of the document emphasize the value of communication and interaction that must exist between the phases of the intelligence cycle, but in effect, the cycle must and needs to be modified to better serve its function, which does not mean that it should be abolished in its entirety. [16] On the opposite, it should focus on the new operating environment and needs to be redesigned to comply with the requirements where the participation of all those involved is important. [16]
The importance of commanders and decision-makers within the process stands out, requiring their addressing, support and tracing of all that is being developed in the process, in order to turn the rudder when it is losing the course. [16]

As a source of information and data feed of the thesis, the web-page of the CIA was used, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies, here we can find the center of intelligence studies, experts, and various authors as Hulnick, Phythian, Evans, and others are consulted. [17]

Articles by other authors are listed below, reinforcing the idea that technology is becoming increasingly important for intelligence, and it is included within the intelligence processes such as the intelligence cycle. [17]

- Some Far-out Thoughts on Computers Bringing the Computer into Intelligence Work by Orrin Clotworthy. [18]
- Managing the "Reliability Cycle": An Alternative Approach to Thinking about Intelligence Failure by Scott J. Hatch. [19]
- Autonomous Systems in the Intelligence Community: Many Possibilities and Challenges by Jenny R. Holzer, PhD, and Franklin L. Moses, PhD. [20]
- Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do about It by Marc Goodman (Doubleday, 2015). [21]
- The Case for Using Robots in Intelligence Analysis by Puong Fei Yeh [22]

The increase in the use of technologies and systems for data collection, data analysis and mining information, which allows to process, filter, and disseminate the intelligence information, leave the evidence of the need to merge the capacities of computer systems, such as autonomous systems, robots, software analysis and other applications, with the knowledge and rationing of analysts or agents who work on intelligence. [17]

The internet of things is something that proves that everything is situated connected to a network or signal, which is controlled or analyzed by a system of technological information, where it is known that there are threats and vulnerabilities that may affect our organizations, highlighting once again the importance of the cyberspace in the intelligence process.

2.5.2 Analysis of the problems of the intelligence cycle at the technological edge

In previous chapters, the current functioning of the intelligence cycle is described in each of its phases, its features and tasks that are performed during the execution of the process that an intelligence agency goes through to obtain a record of intelligence that may lead to operating income, tactical or strategic, depending on their importance or value.

In similar manner, within the generalities that have been exposed, the author is going to talk about a major change in the environment of intelligence, about the new digital and technological age, where almost everything nowadays is associated with some kind of technology, and about transmission, analysis, acquisition, description and information management.

Nowadays, intelligence in a large percentage, if not all of the information, involves some kind of technology that allows handling or treatment where this new age or digital age has affected the process of the intelligence cycle in each of its phases problems, errors and shortcomings in operations or other activities can be observed, where it has used the cycle process, as this is not prepared for or focused on multiple changes experienced by the world and the operational environment. [10]

Since this change in the operational environment where the technology has bound the process participants that the information dealt should be of digital nature, and the cyberspace is deeply involved as a permanent war field.

The intelligence cycle and its phases, by the use of technological systems moving in the environment of cyberspace, have been overtaken by the revolution of technology and information, revealing its current complex situation. It has been observed that the cycle is taken as a reference by intelligence agencies, but in many cases, their phases are not fulfilled, because the Internet or the Web has completely changed the landscape of information management.

Intelligence now gathers information from technological media almost entirely, the various forms of intelligence called the "INTs" [10] have demonstrated this, and signals intelligence, Cyber Intelligence, social media intelligence, geo-intelligence, to name a few, use all kinds of systems technology for the collection and analysis of information, improving and increasing information resources that will be used in intelligence.

Technology changed the way of doing intelligence radically, revealing the obsolescence inherent in intelligence processes by the intelligence cycle, as follows:

1. The flow speed of the digital information that is collected, processed, analyzed and diffuses, exceeds the capabilities of the cycle.
2. The security of intelligence information is weak and is not aligned with the threats and risks of the environment where it moves, the cyberspace.
3. The amounts of data and current information are enormous and overload the capacities of the collection, processing and analysis of intelligence.

4. Lack of knowledge of resources and technological advantages and security of the cycle and those who develop it. Just as the techniques of collecting and analyzing information, through the use of technological systems.
5. The lack of communication and communication channels between the different phases of the cycle and those who develop it.
6. Barriers between the phases and stages of the intelligence cycle.
7. The phases are working in parallel, leading to the duplication of functions.
8. The challenge of technology.
9. Assumptions, estimates, beliefs and stigmas of the people involved in the intelligence cycle.
10. Lack of control and direction in the process of the intelligence cycle.

Considering everything above-mentioned, it is possible to analyze in detail the problems that the cycle has at present, and also build this analysis on the findings of intelligence experts that have described the problems, focusing primarily on the use of technology in intelligence.

During the process of the intelligence cycle, problems of transmission and transmission of information at each of the phases during the development of the operations or missions are observed, information travels at high speed via digital media, resulting in the information becoming too vulnerable to be lost or other situations as when the recipient gets incomplete or unclear information.

In different operations that occur in the world but mainly in Colombia, in each of its processes, the cycle has undergone some changes because of the speed with which it is acquired and the information is processed. Steps or stages are obviated, thus allowing a disconnection in the process, with partial or superficial reports and records.

Within the intelligence cycle there is nothing to secure the information, allowing it to be managed in insecure forms within each of its phases, it does not exist within the doctrine of the cycle, part or section to teach or deliver security awareness during the process, this must accompany each of the steps and phases and always present in the head of an officer or an analyst.

In many cases, lack of knowledge about how the cycle works and how it is organized can be evidenced, agents mix up phases or obviate these sub-processes or phases, because they have not been clearly indoctrinated, and do not know how to respond to the requirements that are developed during the process.

Communication channels must exist within the doctrine of the intelligence cycle as well as in organizations and their manuals, but currently, the cycle does not talk about it only takes them into account superficially within each phase, allowing confusion and mismanagement in the handling of intelligence information.

One of the problems of the cycle is the immediate need for compliance with orders or instructions, chiefs and commanders often ask for hasty results, regardless of the process of

the intelligence cycle, which results in carrying out the analysis, collection and diffusion only partially and without much accuracy or clarity when making decisions.

Within the processes and phases that are developed in the cycle, it is necessary that each person or agent involved knows his or her duties and obligations. A common problem observed in the cycle is that people without required training or without due permission are involved in the process, which allows the cycle phases, regardless of where such people are involved, to obstruct or spoil the work that is being developed for intelligence purposes.

The intelligence cycle is limited to serve as a service process, which seeks to organize in detail how the information collected should be handled to become intelligence, and at present, this requires revision. According to Rob Johnston in the center of studies of the CIA, "The traditional Intelligence Cycle model should either be redesigned to depict accurately the intended goal or care should be taken to discuss explicitly its limitations whenever it is used … If the objective is to capture the entire intelligence process, from the request for a product to its delivery, including the roles and responsibilities of Intelligence Community members, then more is required. This should be a model that pays particular attention to representing accurately all the elements of the process and the factors that influence them". [23]

Therefore, it is important to note down what was said by Geraint Evans, who did a military research, in his book "Rethinking Military Intelligence Failure–Putting the Wheels Back on the Intelligence Cycle". [14] And "It is clear from the discussion that the Intelligence Cycle is not an omnipotent, all-encompassing capability. It needs to be focused in the right place and at the right time, for intelligence requirements will be met only if sufficient and appropriate collection resources have been made available, this is a principle necessarily applicable at the strategic, operational and tactical levels of command. It is a critical consideration given that the apportionment of collection assets may not always be possible. Operational restrictions on movement of intelligence-gathering platforms, environmental obstacles and the physical breakage of collection assets coalesce to reduce available collection coverage. Critically, this fosters intelligence gaps which can lead to failure if left unanswered." [14]
Consequently, "The Intelligence Cycle has a limited capacity which, if not properly scoped, may directly lead to failure. The accessibility to collection assets, and their operational effectiveness, presents a major challenge that can only be adequately resolved through the use of significant planning time and preparation." [14]

Where planning and preparation should be equally focused on the challenges currently presented, challenges such as technology, that lead to having a faster and easier access to information to various forms, all coming together in the use of systems and equipment technology. [14]

This allows enter in what Mark Phytian talk, the challenges of complexity, where is important stand out the challenge of technology [10].They mainly talk about the form that the new digital age must be put it into service of the cycle and intelligence, directly affecting the process and those involved in the cycle, the technology is being paramount to

the development of intelligence activities, and its current application highlights the shortcomings that are currently inherent in the cycle within each of its phases.

2.5.2.1 Planning

Planning or direction is the primary driver of the Intelligence Cycle, without which the remaining elements are pointless and self-serving. Not only does this focus effort, but its very nature means it can be altered to suit the operation being undertaken. This has a fundamental impact on how the remainder of the Intelligence Cycle would function under different circumstances. It must be remembered that the mainstay of intelligence is to ask the following essentials: Who, What, Why, When, Where and How. [14]

During the planning stage, commanders tend to observe and hear arguments or ideas on what is needed and required to do in intelligence, presented by people at senior levels who don't know how the process works, which leads to non-use of the process. Hulnick talked that the "Intelligence managers have to make decisions about the subjects that ought to be covered. Often, this is driven by world events. However, none of this provides guidance for intelligence collection". [13]This is because they prefer to make decisions that allow for immediate actions and results to meet the political needs of the moment.
Consequently, Hulnick also talks that the planning is affected by issuing orders that lead to the projection of gathering information, "Which are not focused properly and let information gaps throughout the process, so in some cases are seen where that the collection agents cannot wait for guidance in regard to intelligence gaps in the data base to begin the collection process. The gaps will be filled once the collection process is under way following their beliefs. Without waiting for orders or other possible analyzes that are being made". [13]

Moreover, these problems lead to the fact that planners or managers may begin to act on the so-called "raw reports" without waiting for the analysis to take place. In the electronic era this happens quite rapidly, thus putting intelligence analysts at a disadvantage. [13]

According with Hulnick is necessary note "Commanders do not welcome intelligence that is nonconforming, perhaps because the large egos that brought them into positions of power do not permit admissions of ignorance" [13]. This is one of the main problems that is inherent in the cycle because they are human beings performing these activities, and when we are tested, or the knowledge or wisdom are compromised, they enter a state of protection or defense, and, more importantly, the reputation or honor become the real purpose of the mission. The application of the Intelligence Cycle cannot be done on a whim – it must be planned and resourced accordingly. [13]

So, it should be remembered that there are resources such as technology that were created to help human beings and prevent them from falling on assumptions and other vicious valuations.

2.5.2.2 Collection

The agents that collect information, although being provided with an opportunity to act independently, should be guided by their area manager or other people in charge, stating their plans and next steps in the activity. Then Hulnick notes that "Many people tend to use technological means through the web, open source intelligence (OSINT) to collect information, which has been given new life in recent years because of the proliferation of information on the Internet, but planning is required to ensure access to needed materials. Intelligence managers need sophisticated software to mine the data because there is so much of it" [13].But the drawback is that agents are sent to analyze these amounts of information collected without regard to the precepts of mining information or without having the resources available to secure their work. [13]

So the lack of knowledge of the technological means for gathering information leads to collecting information that is incorrect or unnecessary for the process. The Intelligence Cycle is weakened by the lack of understanding of what collection assets can actually do and what kind of advantages they provide us with respect to potential targets as well as the advantages give us against potential targets [14].

Technical collection systems have also changed over time. During the cold war, only the most sophisticated and advanced intelligence systems could intercept communications or other electronic signals, mostly using satellites for the purpose [13]. Now, most intelligence systems can engage in cyber espionage – hacking is the more common term – to penetrate an adversary's communications. [14] As increasingly advanced encryption systems are developed to protect communications, hacker's glory is being able to break into those systems to steal data and obtained more economic resources to increase their capacities [11]. This requires special attention because technological progress goes faster than the policies and strategic planning, enabling vulnerabilities in intelligence processes, as in compliance with the intelligence cycle. [11]

As explained above, in the new intelligences the technology is used daily for searching and collecting information, and intelligence uses all kinds of resources to obtain information. For example, the Open source intelligence, once focused largely on print and broadcast media, has become increasingly web-based. Where Berkowitz notes that, "The advent of electronic media provides almost universal access to news and developments to intelligence services that were once dependent on their respective overseas missions for exploiting local open sources. The downside of this development is the proliferation of electronic media often overwhelms the collectors who gather this material" [11]. Allowing lack of clarity in the information that is really important for mission.

2.5.2.3 Analysis

In the intelligence cycle, Mr. Peter Keen in his book "*The Intelligence Cycle: a Differentiated Perspective on Information Processing"* clearly describes one of the main problems that the analysis of the intelligence faces, namely man vs machine. [15] The analysis is one of the stages of the cycle, the assessment of interpreted information; this

usually results in some conscious decision. Discovery is mainly perceptual and therefore hard to observe or make explicit, but the analysis is generally conscious, methodological and sequential. It is concerned more with the use of information than the information itself. Its operators include "evaluate," "compare these alternatives" and "test the impact of—and of course "what if." [15] The tools of management science—optimization and simulation models—obviously support these. It is not clear where man outperforms machine or vice versa. Many problem-solvers prefer to rely on their own intuitive methods, although in structured situations they will rely on formal models. Because analysis is conscious and sequential, it is often constrained by time and computational effort [15]. Keen notes "In many cases, we simplify the problem to the point where it is feasible for us to handle its demands, even if this involves misrepresentation—and sometimes perversion" [15].

For analysts the analysis of the information that they receive, or, in some cases, collect, is enormous, as they receive the information from different sources, and the problem is that they do not always know how to filter, interpret or evaluate all this vast amount of information to finally deliver a product of intelligence. [15] [13] But, additionally, it must be remembered that each of the resources used in the analysis allows to the analyst a good performance without falling into the error of interpretations, evaluations and superfluous analyses based on no feasible argument. [15]

As Hulnick notes about the form of the information travel from collection to analysis "Intelligence moves from collection to analysis, as the intelligence cycle holds, but analysts do not always need new intelligence material to understand world events. The data base is already so large that a competent analyst could write about most events without any more than open sources to spur the process. The incremental addition of new intelligence from human sources may be unimportant, instead, it can delay the process, which would take extra time" [13]. Still, it is important to note down that in the analysis, there must always be an open space to receive new information from human sources and other means, not before without prior evaluation, interpretation and classification.

Working in parallel….
When data collectors send information to the analysis sections, they also send it to Directors or Planners with its preliminary analysis, torpedoing the analyst's work and creating mental images in Directors, heads before having a real analysis [13]. According with Hulnick, Duyvesteyn, De Jong and Van Reijin explain "In reality, the reports that are generated reach policy officials at about the same time as intelligence analysts receive them in most systems today….. The analyst's process works in parallel with the collection process" [4]
In the majority of cases in Colombia, before becoming analysts, specialists work as field agents who collect information, so that as analysts, they know how to collect information just like the agents in the field, using sources such as open source intelligence or social media intelligence. They can improve and get information for analysis to complement the intelligence that is obtained by collector's agents.

All this information collected or that needs to be collected should be clear and complete, so that the analyst would not confuse the information between what, how, when and why it is

important for the case under consideration. The reports should be organized and related to the objectives set in the previous planning, in this special topic Hulnick notes that the ""raw reports from human sources or technical sensors are sometimes fragmentary, biased, contradictory, or just plain wrong". "In order to analyze the data, the analyst compares the new material with the existing data base and previous analysis". Likewise, "it is important to note down that raw reporting from the collection process set up into standardized formats usually goes to policy officials as well as to analysts at about the same time"" [13].

Also "Since intelligence collection and intelligence analysis operate in parallel and should be co-equal, one would expect that there would be a great deal of information sharing between the two. Regrettably, this is not always the case. Because of restrictions of information sharing, psychological barriers, fears of compromising sources, and security concerns, the intelligence collection process and the intelligence analytic process not only operate in parallel, they are sometimes quite independent of each other" [13]. Hence, the problems in communication and understanding are noted while the information is being analyzed and collected.

There are many mental difficulties among agent's collectors and analysts. There must be compartmentalization of information as well as the environment that allows for the flow of secure information. Among other difficulties, there are physical or mental barriers standing between them when it comes to sharing information [13]. Hulnick explain this saying "Physical barriers, manned by armed guards, used to prevent analysts and operations officers from visiting each other's offices. Later, the physical barriers were removed, but the psychological ones remained. Operational people feared that somehow analysts would mishandle reports from the field and reveal the identity of clandestine sources. Analysts mistrusted operations officers because they were thought to be devious and untrustworthy" [13].This increases the lack of clarity of the information and loss of confidence in the results of the analysis of any kind information and also leads to fragmentation in communication channels.

Analysts, as well as field agents or collectors must be guided by a plan and the plan, must be responsible. Sometimes, there are analysts who analyze documents without following the planning and follow their own idea of how things should work, not realizing that there is already a clear process to follow [15]. And is supported by Hulnick saying that the "Commanders sometimes request these in depth studies, along the lines suggested by some versions of the intelligence cycle, but in many cases, the studies are produced because analysts are directed by intelligence managers to write them, or analysts themselves believe they should be written" [13].

Analysts are receiving large amounts of information as well as make use of many forms of collection and therefore sometimes are overwhelmed and tend to ignore the information that could be critical [15]. Many commentators have emphasized that data becomes information by being filtered through some mental model that provides it with meaning and relevance. The mind outperforms most computer-based tools in this process, which relies on alertness, pattern-creation and pattern-recognition. [15] Of course, human limitations on

memory, attention span and capacity for assimilating large masses of data make machine support invaluable in many instances [15].

2.5.2.4 Dissemination

To describe what is happening in the stage of dissemination Duyvesteyn, D Jong and Van Reijin note that "when intelligence products are finally delivered, they most often go to the staff rather than to the Directors. If the products agree with what the staff has already concluded, then the intelligence is of little use. If the intelligence disagrees, then the staff may either suppress the intelligence, or deliver the product to show the intelligence stands at odds with what the policy officials wanted" [4]. This is the part of the intelligence cycle model that has caused the most trouble. Analysts have all been trained to believe that the cycle actually works and the policy officials are waiting for delivery of intelligence products before deliberating on policy [4]. Then they note that "In reality, policy officers often have an agenda that has nothing to do with intelligence, and make decisions based on a variety of inputs. Their staffs often have access to the same intelligence inputs as intelligence analysts and are able to advise policy officials well before intelligence products are delivered" [4].

This is partly because through the use of technology a system does not have a control and pre-established rules for handling the flow of intelligence that could help to avoids these drawbacks in the dissemination of intelligence information [15].

2.5.2.5 Counter-intelligence

Within intelligence and mainly in Colombia, there is a type or process that is immersed within intelligence, which is counterintelligence. This is an important part of intelligence work since it is responsible for protecting the same intelligence and security institutions of the state and in turn uses the intelligence cycle to develop its reporting process.

In the book "What's Wrong with Intelligence Cycle" [13], A. Hulnick is talking about the importance of counterintelligence within the intelligence process, and how it serves as protection. "Leaving aside the collection and analysis processes in intelligence, one cannot understand the entire intelligence system without looking at counterintelligence. Counterintelligence is largely defensive in nature, and it is not part of the traditional intelligence cycle" [13].

It should be clarified that Hulnick believes that counterintelligence is totally different from intelligence, and that it is even greater than this, and that it is not part of the intelligence cycle, because they are different in their tasks and functions [13]. Consequently, he explain that "when one looks at the pattern of counterintelligence functions, it does not look like the intelligence cycle at all. Instead, it may be seen as follows: identification penetration exploitation interdiction claim success" [13]. However, Berkowits and Goodman talks that Hulnick considers the basis of such arguments from a national intelligence perspective and ignores several realities of intelligence in the military context [11]. Moreover, counter-intelligence is the activity that works using information and intelligence provided through the execution of the intelligence cycle, or helps to obtain the information that feeds it [11].

According to Berkowitz, counterintelligence is an essential part of intelligence and is submerged in the cycle because it uses the same steps for planning, collecting, analyzing and disseminating the information, and since it takes longer, planning is a little different [11].

In Colombia, as noted above, these two activities are acting in parallel and under the doctrine of intelligence, but the current cycle by understanding and experience, the counterintelligence, uses the steps and phases of the cycle, but falls short because it needs certain steps to complete its function. This sometimes works according to the Cyber Intelligence and steps that Hulnick talk about "(identification, penetration, exploitation, interdiction)" [13], without leaving aside the traditional steps of the cycle.

It is through the summary of all of the above mentioned that it is important to note what Keen said down the following, regarding the problems the cycle: "None of our tools can support the full Intelligence cycle, nor should we assume that they are other than building blocks [15]."
Intelligence information collected and managed during the process must comply with the confidentiality, the integrity and the availability required for their use, also allowing for fulfillment of the legal and safe regulations of intelligence work. According to the analysis conducted, is possible see what is going wrong and why the intelligence cycle needs to be redesigned, so that the technology, which is an active part of intelligence, should support the process and facilitate the work, as well as assist the people involved in the intelligence process.
For this reason is important to remember according with Berkowitz that "The Information Revolution is not just about cheaper communications or faster computers. The Information Revolution is also changing how people use information. As a result, organizations such as the intelligence community must change their modus operandi in order to provide it. The Information Revolution is bringing into question many of the basic principles about how intelligence is supposed to work. To adapt, the intelligence community must abandon many of these principles, replacing them with a new approach [11]."

The integration of efforts, systems, methods and operations is required for the potentiation of intelligence. As have been showed the new age develop a new type of intelligence where the intelligence cycle cannot support the requirements that the intelligence needs from the process of information.

2.6 Scenario

To demonstrate and put more clearly these shortcomings, weaknesses and problems that owns the current cycle of intelligence, is shown as analysis test three real examples of situations presented in the world and Colombia, where intelligence failure, for lack of updated in the 21st century, the new digital age.

2.6.1 Case Snowden

The case of Edward Snowden, a former member of the CIA, the NSA the US and computer analyst contractor defense firm Booz Allen Hamilton shows how Snowden collected

different sensitive information about surveillance activities and intelligence of the American government, to later filter the public opinion these documents, creating a diplomatic crisis for the government of the United States and protests within the country, Snowden who worked for several years in intelligence, managed, analyzed and collected sensitive intelligence information, this case serves for example to analyze the problems that can be presented in intelligence, where the result is leakage of information and sabotage against the intelligence, causing serious consequences [24].

Snowden, being an active member, of intelligence agencies in the US, is a clear example of the shortcomings and weaknesses that affects the intelligence and their processes in the world of technology, Snowden has a preparation in digital information systems, knowledge used for personal purposes, as the scandal leaks is concerned, it is not the intention of this thesis to debate whether it was or was not good, or whether it was legal, what is to be evaluated here are the fault presented in this case with respect to intelligence and its interference with the process of the intelligence cycle [24].
It is clear that the reserve and information security was totally broken; this information was stolen illegally, by the use of cyber espionage, since it was stored in various storage systems of intelligence agencies.

This demonstrates that the changes in technology and the appearance of new adversaries going along with old ones continue to pose problems [24]. Constant problems that involves the entire chain of the process of intelligence, since the planning of the operations that were developed and Snowden had knowledge, reflecting the possible disagreement of Snowden, during developed his work, together with the tasks that he development in the collection and analysis of information assigned to him, using systems Cyber Intelligence had access to databases of all kinds of people, allowing to observe that the planning was not the right track, or in several cases was directed to fulfill any special requirements, without putting into consideration the principles of intelligence and monitoring the intelligence operation, situations that made Snowden act that way [24].

It is clear that the use of technology must be done responsibly, avoiding that the agents and operators who are involved in the system find themselves in dilemma, thinking whether they are acting correctly [25].
In intelligence and counterintelligence is due using all available resources to protect and safeguard the citizens of a country or nation. This present age calls to make use of all existing information sources, using the cyberspace in all fields of war. The surveillance and data access requires a particular study in the field of intelligence, but specialized operations such as monitoring and surveillance must be taken into account when information is collected, and the use of technology is very important [26].

It is not possible make mistakes in planning, or data collection operations, which go against the principles and values of the agents. The intelligence cycle or process must be implemented transparently, allowing making next steps clear, showing the agents a simple road to obtain intelligence [26].

Around the world after Snowden case revelations and other scandals where intelligence agencies have been involved, new policies have been established and the procedures of the use of technologies in intelligence have been reviewed. In Colombia, legislative and organizational changes in the intelligence services took place.

2.6.2 Case Saddam Hussein

Saddam Hussein, a dictator in Iraq between 1979 and 2003, was characterized by permanent violations of human rights, censorship, torture, persecution of political opponents directing the dictatorship to his downfall and subsequent death by special operations of the United States army. This case is important because in intelligence studies and especially the intelligence cycle is observed during the planning process, collecting and analyzing intelligence information vices of value were presented, resulting in operations against the military leader and political [13].
In the case and in relation to intelligence operations that were carried out, the planning shows interests of high strategic level and where information that was collected was used biased and addressed, in order to get the results that best accommodated political interests of the US and its foreign policy [13].

It was established that the commanders directed the search and analysis of information, bypassing the cycle and its phases, arguing that Saddam Hussein and his regime possessed weapons of mass destruction, information collected through technical and human intelligence, justifying the need for intervention, something very similar to the case presented in Afghanistan and terrorism. It is here where is required to analyze how the current process is running intelligence, because if it is distorted tends to show his darker side [27] [13] [28].

The Intelligence operations were addressed without following the correct form the intelligence cycle, the systems were used as a tool to obtain the information that the high interests wanted. The agents didn't respect the procedures and followed the superior orders, in the end although the result of the operation was successful was demonstrated that Hussein didn't have WMD. The Intelligence was discredited.

2.6.3 Case Illegal interceptions for D.A.S (Administrative Department of Security)

The illegal interceptions, scandal of DAS, was in 2009 in Colombia for telephone interceptions and illegal surveillance carried out by the former Colombian intelligence agency, the Administrative Security Department (DAS) during the government of President Alvaro Uribe. The DAS as an entity of state intelligence became embroiled in the scandal reported and published by one of the most popular magazines Colombia, Semana magazine, it is said to one of the biggest failures and mistakes of intelligence in Colombia, this due that the DAS used technical and technological resources of the state at the service of intelligence to intercept, spy and conduct illegal surveillance of members of the political opposition, journalists, politicians and generals of the Armed Forces, as a result of this scandal, the entity was dissolved and brought to judgment several of their Directors, for crimes against privacy and spying [29].

These case evidenced errors in the intelligence process, bringing to the complete failure and discrediting the legitimacy of a government and its security institutions.

Problems of management, control, objectivity, planning, and analysis and data collection were observed in all directions and at all levels. The resources and intelligence agents were used incorrectly, the planning were vitiated at outside interests where the objectives of D.A.S. were completely diverted, the interception equipment were used against groups of persons protected by the Constitution of Colombia, as politicians, journalists and others never consulted with the analysts of the situations who might have had recommended to redirect the target of operations. But the worst part was that everything was fulfilled by orders in favor of people external to the intelligence, and the process of intelligence [29] [30]. It denotes a total and complete lack of knowledge of intelligence and intelligence cycle process. And as important data the intelligence information that it was collected ended up being filtered from the same agency at the Semana magazine, main magazine of the country for analysis and opinion [31].

As can be observed in the three exposed cases, problems of organization guidance, planning and lack of knowledge of intelligence and the intelligence cycle where technology was used improperly, as well as the phases of collection, analysis and dissemination of information, also emphasizing the fragility of the intelligence cycle, and the security of digital information that moves in the process [30].

2.6.4 Case 1

Next will be used as a case for study the Thunder Operation, it is an example of one case created with names and imaginary situations, to show the shortcomings of the current intelligence cycle. Although the results of this are not bad in the end, will be compared with the results of the same case but using the new process that will be proposed in the development of this thesis:

Thunder Operation.

The Armed Forces of the Republic of Topaipí, daily confront the terrorist group UTIL (Union of Independent Workers for the Liberation), which is led by the Central Command composed of seven ringleaders of mobile guerrillas, that are distributed in different regions of the country. Within the planning established by the intelligence agency of the Armed Forces of Topaipí, the main objective is to identify, penetrate and neutralize the heads of the Central Command of the UTIL.

The Net of Intelligence of the North, through activities of human intelligence, penetrated a human mail of the terrorist, alias Jacob, which acted as a ringleader of the guerrilla # 6 of the terrorist organization of the UTIL, this human mail motivated by economic remuneration becomes a source of occasional information for the intelligence; through interviews and monitoring with accompaniments to the source, other members of support networks of the terrorist organization of the UTIL are identified. One of the members recently identified is known as "Patriarca" and is a confidant of the ringleader JACOB guerrilla leader # 6 of UTIL; it was planned to penetrate the structure of the guerrilla # 6 of

UTIL and their leader by delivering a USB Kingston Data Traveler 4000G2 device with supposed fictitious information of the Armed Forces of Topaipí in the north area; a scenario was created, according to which the source delivers the USB to alias "Patriarca" in exchange for $ 20,000, claiming that the USB had been sold to the source by a member of the Command of the Armed Forces of Topaipí. The source who serves as a human mail for the terrorist organization of the UTIL meets with alias "Patriarca" and informs him of a person who has access to military data, and as an operational proof gives the USB-memory-stick that contains relevant information about military security as well as the information about officials and members of the Armed Forces, but in fact, the information is fictitious, hiding a malware of the Worm type and the Trojan horse with remote access, Backdoor.SDBot.A0779760, Backdoor.Win32.Codbot, reveals Keylogger 2.10, compatible with Windows 7 and integrated security software, XTSEncryption, which allows to establish a remote connection, perform information theft and determine the GPS location of the device it is connected to.

Once the USB-memory-stick is given to alias "Patriarca", the terrorist travels to the northern area of Topaipí, where alias Jacob is hiding, and gives him the USB-memory-stick; alias Jacob connects the USB device to his computer and checks the files on the USB, and this is when the malware affects the PC of alias Jacob immediately and initiates remote connection with the intelligence agency of the North of the Armed Forces, who store information on a remote server for private storage, thus gaining access to the terrorist plans that the UTIL has prepared in the northern area of the country as well as to the information that apparently relates to businessmen and members of the Police of Topaipí who collaborate with the terrorist group, additionally establishing the positioning and location of alias Jacob.

From his PC, alias Jacob sends an email to alias "Patriarca", informing him that he will meet him and other deputy heads of the guerrilla in the rural area of Pasacaballo on Thursday at 3:00 pm, where they will discuss the terrorist plan and actions against the city hall and the police of the northern capital of Topaipí; the intelligence immediately begins planning the Thunder operation to neutralize Jacob, the Patriarch and three heads of the UTIL who will attend the meeting. It has been ordered to perform the BETA (bombing) operation and send a group of special operations command from the army for the recovery of bodies and elements for intelligence, at the end of the operation.

On Thursday at 3:00 pm, Jacob’s PC emits a signal from point " El cerrito" in the rural area of Pasacaballo, and this is when the Commander of the 2nd Army Division accompanied by the Chief of Intelligence Network of the North, order to initiate the Thunder operation, deploying two Tupolev Tu-160 bombers and the two special operations commands of the army. The bombing is released annihilating Jacob, the Patriarch and eleven more terrorists who were at the meeting; the special commands get into the area where the bodies are recovered along with 4 PCs, two hard drives, and six USB devices.

After the end of the operation, the national news report the death of four children and two women in the area of Pasacaballos during clashes between the Army and terrorists of the UTIL, likewise, the special commands that collected the computers, they damaged two of the collected computers and the death of the human source that collaborated with the

intelligence Group of the North in the area is reported, to the Commander and the Chief of Intelligence Network of the North.

When the judicial proceedings against the collaborators and the police officers who have been helping the UTIL are initiated, are placed at the disposal of the process the elements found in the operation, the judge decides that they are not admissible for investigation and trial evidence, because they do not have the proper chain of custody, and some of these devices are damaged.

Twenty days after the Thunder operation by intelligence signals and interception of communications to the Central Commander of the terrorist organization UTIL, it is possible to determine that alias JACOB was planning a meeting with the Supreme Commander of the UTIL 10 days after the meeting in Pasacaballos to establish new objectives and terrorist plans.

Technical equipment used in this intelligence operation:

1. USB: Kingston DataTraveler 4000G2

• Capacity 16GB

• Firmware 3.0.5

• Integrated Security Software XTSEncryption

2. Software: Exploit.DComRpc.B

Type: Worm and Trojan Horse Remote Access

Alias: Backdoor.SDBot.A0779760, Backdoor.Win32.Codbot.y.

Platform: Windows

Size: 58,880 bytes

• Keylogger 2.10 reveales compatible with Windows 7.

• USB Script.

• AceVPN Ultimates.

Servers in 24+ countries, more than 40 locations

Super Secure Encryption

OpenVPN, IPSEC IKEv2, L2TP, PPTP and VPN Stealth

3. Remote Server Russian Private Storage

• Limited time 6GB Memory

• Space 50GB SSD Solid State

• Intel Xeon processor - 1 CPU 2.8GHz

• Windows Operating System

• Backcup Type: Snapshot

• Dongee High Availability: In case of failure of one of the storage disks has a backup with the same feature and information.

3 Improving the Intelligence Cycle

In this chapter, the new process for the intelligence of the 21st century and the concepts that always must accompany this process are presented.

3.1 Intelligence Processes in the 21st century

Colombia and its intelligence agencies should take advantage of its current and future situation where the reorganization of institutions and the turning of the conflict is taking place, forcing to update the processes. That is why the current problematic to which the intelligence cycle faces, being the main process of obtaining intelligence, coupled with the irruption of technology is necessary redesigning the process. The cyberspace makes the handing, treatment and information flow digital, demonstrating that the intelligence cycle has become obsolete as intelligence process to resolve and face the challenges that the intelligence of the 21st century, the information revolution, and digital age experience.

Although the cycle and its phases should be not refused completely, it is necessary to redirect and redesign the process on the basis of the cycle and its four phases, in order to improve, increase and produce a better result of intelligence, hand in hand with the integration of technology.

The redesigning or changing of the processes or procedures requires the commitment of all stakeholders in the process because intelligence is a complex process which is designed in detail in a naval, military or air environment but also serves the private sector. That is why each of the steps that occur in intelligence is studied carefully as any mistake leads directly to failure and disastrous consequences in many cases [32].

Intelligence walks on thin line of what is legal or illegal, so it needs to use all sources of help available, for supporting and build better intelligence with better results, protecting agents, commanders and directors from failure and all kinds of risk, also protecting the existing legal and proportionality principles [32].

Nowadays, technology and the cyberspace enable people to improve themselves in all fields of knowledge; going hand in hand with learning, advancement, and technological development, achieving unimaginable results to support human beings in their daily work.

For this purpose, a new process was elaborated, that allows to bring closer and integrate technology with intelligence and the whole process of obtaining intelligence, exploiting the advantages offered by technological developments and existing and potential capabilities, that are inherent in different types of intelligence (INTs) [10], where each step, phase, process, or stage of the process involves the use and utilization of all resources, both human and technical.

It is a process of micro cycles of intelligence for obtaining intelligence through the integration of the technology into all environments, tactical, operational, strategic, and mainly for intelligence that is now being developed in the cyberspace, which is the new terrain of war in the 21st century and the near future.

Thus, responding the wars of the fifth generation that will develop in the world, affecting all existing battlefields (land, sea, air, political and economic) where in the cyberspace electronic resources and massive communication are used to generate the destabilization of the population through prolonged psychological operations; It is intended to affect the collective psyche, affecting rationality and emotionality, also contributing to political erosion, loss of resilience, weakening of critical infrastructures and the general volition [33].These wars gradually involve the use of technology weapons for the cyberwar by weakening the critical infrastructure of the enemy in all possible ways, obtaining a great amount of information that is moving in cyberspace and sabotaging all vital resource.

The process of micro cycles of intelligence is also accompanied for fast adaptation of several concepts that support the constantly changing of the operating environment, which depends on the use of technological systems, supporting the new landscape of conflict.

NEW PROCESS INTELLIGENCE MICROCYCLES

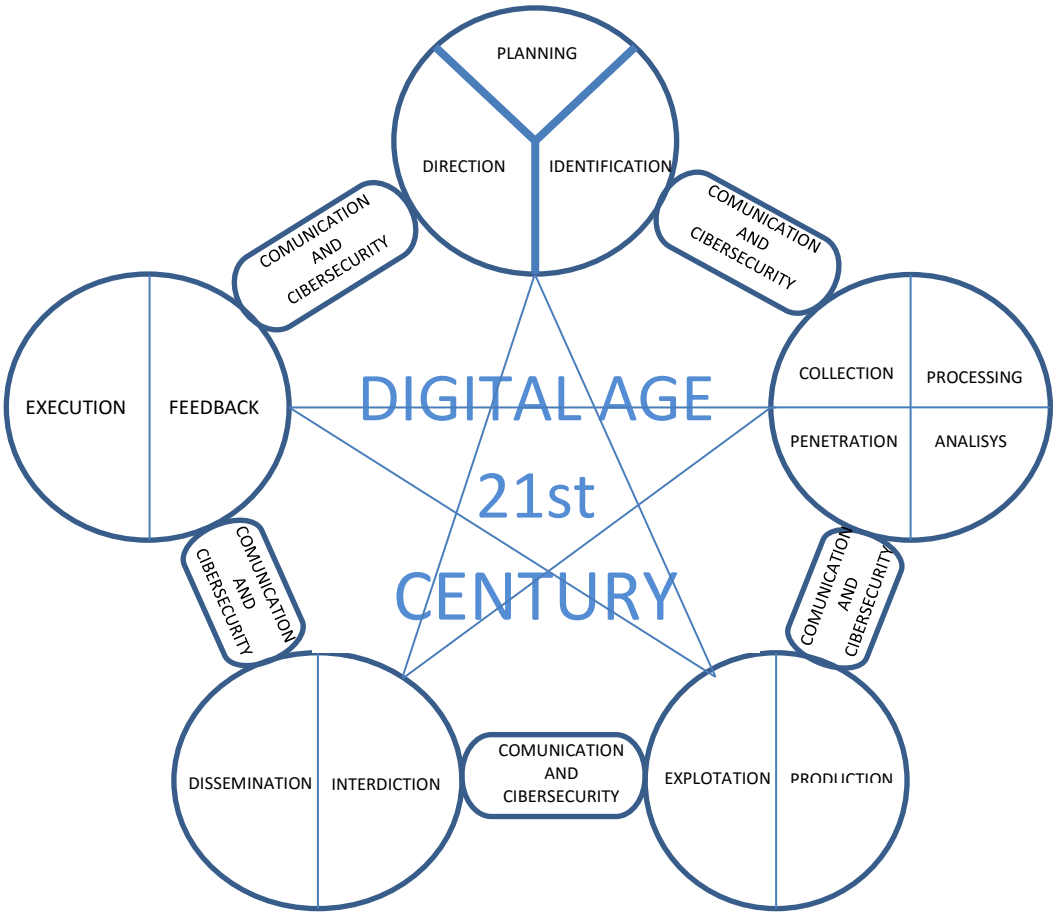

Figure 2 Process of Micro Cycles for Intelligence

3.1.1 Micro Cycle of Planning, Direction and Identification

In this first micro cycle the three aspects of direction, identifying and planning are combined. As is well known, this is the phase where the new process involves commanders and directors with their staff, it is from this point that the operations, missions, and requirements will be issued and where orders need to be clear, precise and concise. With good planning and directing, the end results will be better, and the shadow of a doubt that leads to failure decreases significantly.

From this point, the use of technology and technological intelligence systems is integrated; when an intelligence process starts, the first thing that is required is a clear understanding of situational awareness, a preliminary study of the area where we will develop operations and prior knowledge of the enemy. The identification of the threats and targets plays an important part in this micro cycle because with the use of technological systems and equipment , may be identified preliminarily and put in context to the Commander or Director; information as: weather, terrain, statistical indices, knowledge of the area of operations, knowledge of the enemy and their capabilities, open source information, social media information, records and databases, thereby preparing a clear picture of situational awareness the Commander [16].

Once the objectives, targets, advantages, risks and existing threats have been identified, the planning starts, and the Commander emits his intention with the main objectives and the articulated operating lines .

Then the intelligence requirements are sorted and the EEI (essential elements of intelligence) are formulated. The human and technical resource teams are chosen to achieve the targets and the suitable intelligence architectures facilitating like this the functioning of the entire intelligence process [16].

Once planning has been initiated, the direction takes part in the micro cycle, it is consisting of the explanation of intelligence requirements, the selection and prioritization of available databases, platforms, sensors and sources for the direction of a general objective or, in particular, the creation of a human source, the selection of ORI (other intelligence requirements) and finally the verification and the provision of legal advice concerning the rules and laws that must be taken into account during the intelligence processThe final issuing of orders for a clear definition of the objectives and priorities of the commander is performed also at this time, the advice and support is given to the commander by his staff, improving the planning [14] [16].

Similarly, this is the point where the first micro cycle is related to other micro cycles within the process, since the direction of the commander, must be constant and permanent throughout the process that is being developed.

3.1.2 Micro Cycle of Collection, Penetration, Analysis and Processing

It could be said that this is the micro cycle is the one that feeds and where the process is largely supported. Within this micro cycle, the collection, processing, the penetration and analysis of information have been placed in order to establish a better relationship between

these activities, allowing for better communication, clarity, use of information resources and agility in obtaining intelligence, and it is clear that within this process is required to start with the collection of data and information .

After planning is completed, and once the orders and instructions to be followed are received, the collection uses every existing resources, and it is at this point that the information that is going to be acquired is searched for, using the designating and giving priority to the sources of collection, the deployment of platforms/sensors or contact with an agent [14]. Raw information obtained is sent to the processing elements for future action, just like the communication channels are opened by analysts and operators for combining efforts and avoiding the duplication of information or sending irrelevant information.

The harnessing of technological intelligence equipment allows agility and precision in information collection, and it also contributes to the personal security of field agents. The use of open source intelligence, social media intelligence and cyber intelligence expands the range of opportunities related to the collection of intelligence information. At the same time, it is by collecting information, and by clear understanding of the objectives of the mission systems that the technology penetration into enemy systems or target is utilized, and at the same time, the field agents perform their functions to penetrate enemy structures [13].

When it is started the sending and management of information collected by the different sources of information and penetration, the processing of information it is opened. This involves the conversion of raw data collected into a form that is suitable for the analysis [13].

Into the processing, the interpretation and classification of information are important for purposes of data validation, which is why the use of technological intelligence systems supports these two elements and allow clarifying the relevance and importance of all data collected. The mining data, storage in databases, the reports from indexes and incident reports will enable to the analyst observe the highlights of information or obtain critical data to make predictions and issue new intelligence requirements, or build intelligence records [16].

The Analysis; at this particular stage of the process, the information will become intelligence, based on the integration, analysis, and evaluation of cross-reference data from all sources. The use of matrixes, software, and analysis systems are important because they allow the analyst to clarify the projections and understand the ways that facilitate the process. It is at this point that the intelligence product must be able to withstand scrutiny and establish whether it meets the original requirements for the fulfillment of the objectives [14]] [16].

The analyst must maintain constant communication and monitoring of sources of information to complete and fill in the missing information as well as to be able to collect relevant data that is needed for final analysis required. The communication between collectors and analysts needs to be agile and secure, with the use of encryption systems and

data protection. The Cybersecurity must take care that all of the information that is handled and processed is kept secure without leakage problems.
This micro cycle constantly is repeated because always is being collected more information, and requires permanent analysis, should also be addressed and verified by designated commanders and superiors.

Also the union of these four stages in one micro cycle allows improving the problems of the speed of the information, because the communication and the constant control among the analysts and agents. As the information travels fast in all sides of this micro cycle, here the use of the systems to control the information and constant reports about what happened and the persons who receive the information, gives control and fixes problems of security

3.1.3 Micro Cycle of Exploration and Production

Once the analyses and the necessary intelligence collection have been carried out, it is time to exploit the advantages acquired through the penetration and analysis of information. At this point, the analyst who has clarified his analysis has the ability to exploit weaknesses, vulnerabilities, and errors of the enemy or target, to learn and get the advantage over them, before moving against them, or them moving against us. So, the analyst begins the production and preparation of intelligence reports in the formats conforming to the requirements and the diffusion media of the user [13] [14].

These intelligence reports or records must be clear and precise, so that when they get to the commander, he or she do not waste time asking for explanations and could address decision-making properly. Reports or records, not only should be forwarded to the commander or director, in some cases, they must also be sent to the agents, so that they could redirect their tasks related to exploitation using the analysis made [13] [16].

Again, this micro cycle must be accompanied by communication and security at any given moment, and the cybersecurity and management analysis, within the cyberspace, will allow for successful operations and achievement of objectives.

3.1.4 Micro Cycle of Interdiction and Dissemination

The diffusion and dissemination of records and intelligence reports, which involves the delivery of intelligence to commanders, directors or agents, who will use it in their missions or operations, will be done using the formats established by each agency or institution and with the use of the secure communication channels to provide fast delivery to recipients. The intelligence produced can now be used to meet the initial demand.

This is the stage where more care should to be taken into account, since it is the moment when an attack or information leakage could damage the whole process. The Cybersecurity is obliged to shield this micro cycle, putting at the service of process all resources and security capabilities that the agency has.

Each and every one of the members who are involved in the process and in this micro cycle should know and have full knowledge (technical, technological, legal and general), of the canals of disseminating and the procedure of sending the information, regardless of

destination [14].That is why each and every one of the operators involved in the process must be trained to handle new technologies and the knowledge about cybersecurity measures and applications, thereby protecting the intelligence information. Each procedure performed at this stage, just like in each of the previous stages, it must be recorded, stored, encrypted and secured for use, preservation and care.

Once the records or reports, have been sent and disseminated, the continuous monitoring of the information must be done, in a way that allows permanent control, where any possible leakage or theft of information can be detected then acting through the interdiction, which refers to the detention of violators of the law or regulations. Protecting the secret and degrees of classification of information established for the information management, reducing like this the system failures, espionage and sabotage [16].

The use of equipment and security programs such as IDS (intrusion detection system) or IPS (intrusion prevent system) will increase the security of the system and the process, while the use of systems such as honeypots allow knowing who is behind the intelligence, identifying the capabilities and vulnerabilities of the enemy. It is required to invest in good cybersecurity technology systems and integrate the use of technology into the process, which would guarantee the dissemination, because this is where the most important information flows in different directions and which must be the most secure [14].

3.1.5 Micro Cycle of Execution and Feedback

When intelligence and its end result are delivered to decision makers, whether they are commanders, directors, or other parties involved is due order the execution of missions and operations necessary for the fulfillment of the planned objectives maintaining control and monitoring their development in real time [14].

The execution of missions and operations must be done after the operational security measures have been taken and by shielding the intelligence information by using devices of communications security for permanent coordination during development, maintaining confidentiality, integrity and availability of the information. The use of the encrypted communication via radios, telephones, emails and chats supports the idea of how technology and cyber security, optimize the processes of intelligence and operations [14].

At the end of the whole process, feedback should be given about each of the micro cycles, containing all positive and negative points, disadvantages and problems that occurred during the development of the whole process. At that point, it is required that the intelligence produced is evaluated [14]. It will be necessary to determine whether it has answered the question or original problem, and if the result of the operations or missions was the one that had been expected. It should also consider establishing if the requirements have been complied with conclusively. All of this continuously improves the process and allows the calibration and updating of technological systems used in intelligence process [16].

3.1.6 The Concepts That Must Accompany the Process

Technology, communication, security, cyber defense and cyber security should support the new process of micro cycle for intelligence as follows.

3.1.6.1 The Technology

With the involvement of technology and the use of technological systems can deliver better results to the point of execute large-scale operations without a considerable displacement of men and resources [34]. The information is a fundamental piece and the pillar number one in intelligence work. It flows and moves in the cyberspace, so the management needs be framed within a process that fully involves the use of computer systems that operate into cyberspace.

The management systems, storage, analysis, data transmission and protection of digital and computer information are in constant development; they are moving exponentially and delivering even greater benefits to intelligence. The huge amounts of existing data that must be handled by intelligence agencies have opened a world of possibilities in terms of resources, sources and solutions that enable better analysis and better communication channels.

The cyberspace has delivered a new operational environment to intelligence agencies, since, through its enormous capacity for global information flow, it has placed the intelligence into uncharted territory but with great potential for the use and application of intelligence in the 21century [34].The cyberspace requires that the intelligence adapt this environment, and, therefore, the intelligence process must change and project itself as a technological intelligence process, leading to the integration of man and machine in function to obtaining the results that will lead to success, both operational and strategic [34].The new intelligence process is clearly explained and tuned to existing technological capabilities, where the systems of collection, analysis, projection and dissemination of the intelligence information would be integrated in an agile, confident and secure way in all fields and with all types of intelligence.

3.1.6.2 Security, Cyber Defense and Cybersecurity

As well as technology, cyberspace and allows the new digital world to possess new advantages and place a new operational environment for the benefit of intelligence, but it also expands exponentially the risk and latent threats to information and intelligence agencies.

Being interconnected the information systems and critical infrastructure mainly, the information of any kind and operability, is vulnerable to thousands of attacks of all kinds, where the use of various technological tools is observed; example is a man sitting in front of a computer, hacking with the ability to generate chaos [35].

That is why any country or institution must have a cyber defense strategy; responsible for stipulating and address the protection of cyberspace. The current process intelligence and

the future involve the information, management and treatment, so that whoever owns the information obtained the superiority of global and regional strategy, forcing it to protect itself in all forms [35].

In the strategy of cyber defense, the counterintelligence as part of intelligence is responsible for protecting and developing all kinds of protection activities, it must be oriented with the cybersecurity, to close the most of existing vulnerabilities and clearly identify the latent risks, as each of the threats, potential and existing, which the intelligence and information has.

Cybersecurity and counterintelligence, strengthened and technologically advanced, further shielding the intelligence process where information becomes the main asset of value, so should join the whole process of intelligence..

3.1.6.3 Cyberspace and Cyber Intelligence

The complexity of cyberspace currently make to observes its many features, where a new war front has opened in the eyes of world; being all interconnected by the Internet, the web and in general the cyber world, forces nations, governments and organizations, to engage further in the management of the information that they have, so that knowledge of the land where develops this new stratagem requires great efforts. Operations against general awareness by attacking the enemy's critical infrastructure or target, identified allow the weakening of this, leading the strategic positioning to a higher level [34].

The Cyber Intelligence increases its importance in this new age of technological development, since its proper use allows obtaining strategic results without the use of large resources, achieving savings of resources and efforts to the defense [34]. The development of a process of intelligence attached to the Cyber Intelligence and the use of technology, in cyberspace, enhances the projections of intelligence in search of greater effectiveness, efficiency achieving greater effectiveness in the new field of war for the 21st century.

Planning, direct, identify, collect, process, penetrate, analyze, exploit, transmit and execute intelligence hand in hand with the use of technological systems, Cyber Intelligence and Cybersecurity, at each step, permits treatment of the intelligence available more clear, precise, fast and potentially successful for the fulfillment of the objectives. The Cyber Intelligence should be extended to the help and support other types of intelligence (HUMINT-SIGINT-OSINT, etc) that converge on increasing sources and resources in the collection, analysis and processing of information.

3.1.6.4 Communication

A process where the information is involved, whatever is its purpose, must be based on a good communication system, which must be supported by the resources and technological sources that allow for the transmission and flow of the information, simple but what is more important, secure. With the use of different types of intelligence (INTs) [10], where technological intelligence systems are connected and available to users anywhere, the

awareness of communication, constant and secure at all levels of command should be present always, contributing equally to feed and feedback of the process.

This good and secure communication will maintain constant control and direction of the intelligence process, preventing the loss of the ultimate goal, the leak of information, the general or particular disconnection of the process and providing the necessary feedback for continuous improvement.

Finally…..

In general, if the whole process is clear and transparent within the law and objectivity of intelligence work, the members involved can carry out their work in a secure and reliable way. The accompaniment to the process of micro cycles by the laws and rules established in the labor of intelligence will give legitimacy and will avoid counterproductive situations of process and system intelligence.

With this methodology and development of this new process, seeks to achieve more security, clarity, organization, communication and modernization, which would result improving the intelligence process and the product of intelligence, in order to have intelligence with higher levels of confidentiality, integrity, and availability in the new operating environment.

Also, is important to note that this new process with the integration of the technology and the cyberspace, forces and allow having better knowledge of the technological resources that are used in the intelligence. Work all time with the intelligence systems and learn how the intelligence works does? Show to the agents, analysts and Commanders the importance to be updated in the use of all technological systems.

It is important to implement the new process and make a study and analysis of the results gained in the operations where it is implemented, searching with this continuously improving.

The integration of the classical intelligence cycle, the phases of cyber intelligence, cyber security, counterintelligence and the use of technological intelligence systems within a process of micro cycles allow to expand the outlook for intelligence, taking advantage of the qualities, advantages and capabilities of each part of the process in order to improve the final product of intelligence, reducing the risk of failure and proposed success.

As Evans said "If one remains realistic when considering the implications for adopting new doctrine, some factors must be deliberated. Time and resources will play a large part in developing new capabilities for intelligence production, all of which serve to impose operational parameters and timelines as a result [14]". Then it is necessary to start now for a new doctrine, process and new way of seeing things. Enter into the technological world must be the main beginning.

3.2 Scenario in the 21 Century (Case 1)

Now will be showing the case 1 but using the new process of micro cycles and the concepts to improve the results in the Thunder Operation:

Thunder Operation.

The Armed Forces of the Republic of Topaipí daily confront the terrorist group UTIL (Union of Independent Workers for Liberation), which is led by the Central Command composed of 7 ringleaders of mobile guerrillas, that are distributed throughout various regions in the country. According to the plan developed by the intelligence agency of the Armed Forces of Topaipí, the main objective is to identify, penetrate and neutralize the heads of central command. The Net of Intelligence of the North, through activities of human and technical intelligence and missions to identify the support networks of the UTIL, could identify an individual, by analyzing cyber intelligence and open source intelligence who serves as a human mail for the terrorist organization UTIL in the northern area of the country. This individual used mail accounts to buy secondhand cell phones for the communications of UTIL; the members of human intelligence were able to penetrate this individual, who has contact with the structure of the terrorist, alias JACOB, the ringleader of the guerrilla # 6 of the terrorist organization UTIL. This human mail motivated by their participation in the support to terrorist acts committed by UTIL. He decided becoming an occasional source, offering information and collaborating with justice through identifying infiltrators and helping to capture or neutralize the alias JACOB. Carrying out specialized intelligence activities (interviews and follow-ups) and with accompaniment to the source, using cyber intelligence was contacted a close member of the terrorist JACOB. With those activities, was possible to identify two members of support networks of terrorist organization, UTIL, alias "Patriarca" and alias "James", the second in command of the logistics for the group, and intelligence chief of the terrorist group, confidence men of ringleader JACOB.
With the help of the information collected and by electronic control of several emails and accounts of the terrorist organization, it was conducted meeting with the experts in cyber intelligence as well as the analysts from the intelligence unit. During the meeting, it was decided that the best way to get more detailed information about the plans of the UTIL terrorists is to penetrate the ringleader alias JACOB. This will be done by delivering a USB Kingston DataTraveler 4000G2 device with supposed fictitious information about the Armed Forces in the northern area of Topaipí; the scenario was created, according to which, the source has to deliver the USB-memory-stick to alias "Patriarca" in exchange for $ 20,000, claiming that the USB had been sold to the source, by a member of the Command of the Armed Forces of Topaipí.

The source who serves as a human mail for the terrorist organization UTIL meets with alias "Patriarca" and says that there is a person named "JOSE" who has been given the identity of an operator of the Army headquarters, who has access to military data; the source delivers the USB-memory-stick, which contains the information about Operative Security as well as the information about officials and members of the Armed Forces, but in fact, the information is fictitious and the USB-memory-stick hides a malware of the Worm type and the Trojan horse with remote access, Backdoor.SDBot.A0779760, Backdoor.Win32.Codbot, reveales Keylogger 2.10, compatible with Windows 7 and integrated security software, XTSEncryption, which allows to establish the remote connection, do information theft and determine the GPS location of the device it is connected to.

Once the USB-memory-stick has been given to alias "Patriarca", he travels to the northern area of the jungle of Topaipí where alias JACOB is hiding and delivers the USB to him, who connects the device to his PC, checking the files that are on the USB, and immediately the malware infects the PC of alias JACOB and initiates remote connection with the Net of intelligence of the North of the Armed Forces, who store information on a remote server for private storage, thereby obtaining access to the plans of the terrorists, and the members of the UTIL, in the northern area of the country as well as the information about entrepreneurs and companies that serve as a front for the UTIL. Besides, the contacts in the Police of Topaipí who collaborate with the terrorist group are revealed as well as the positioning and location of JACOB.

The related companies in the PC of JACOB are TECNOPOR and ASES, dedicated to the commercialization of domestic appliances, and are fully identified by open source intelligence. Six individuals are also identified who work in these companies, and with the use of social media intelligence, their names, and current residences are determined, but additionally have frequented places of the last two terrorist attacks perpetrated by UTIL. In addition to that, through the use of the information collected and by reviewing databases, three police officers working as infiltrators for the UTIL, are identified, who have pictures of celebrations of TECNOPON and ASES or with the workers identified as members of the UTIL on their walls in Facebook.

Alias JACOB sends an email to alias “Patriarca” from his PC, informing him that he will meet with him and other deputy heads of the guerrilla in the rural area of Pasacaballo on Thursday at 3:00 pm, where they will discuss and plan terrorist actions against the city hall and police of the Northern capital of Topaipí. With this information at hand, the intelligence analysis group meets with the commander of the intelligence unit to plan the actions to follow and set new requirements for the source intelligence infiltrated in the UTIL organization in the area.

At the same time, emails are sent to JACOB by intelligence, and by interception of radio communications between the central command and the guerrilla of the North intelligence is able to penetrate communications and cut off the channel between the two points of the organization thus getting control over JACOB.

The Commander of the 2nd Army Division, advised by the intelligence, ordered that the source would attend the meeting using a GPS device in his boot, to establish the exact point of the meeting. Besides, the preliminary survey of the area of Pasacaballo meeting point is performed, where the existence of a school at the distance of 3 kilometers away from the point where the meeting will take place, is established.

The plans are to neutralize JACOB and his men through the Thunder operation. The development of the BETA (bombing) operation is ruled out due to the risk for the nearby population. Instead, two groups of special commands with snipers are sent out for neutralization and capture of those attending the meeting. The intelligence chief orders to include two specialists in management and collection of digital material in the group, taking into account the fact that the location of the PC of alias JACOB has been determined, and to assign a bailiff who is responsible for the chain of custody.

On Thursday at 3:00 pm, the JACOB's PC emits a signal from the "El Cerrito" rural area of Pasacaballo, plus the GPS source confirms its presence in the same place, and the Commander of the 2nd Army Division with the chief of the intelligence Net of the North ordain to start the Thunder operation, deploying two special commands. In the development of the operation, JACOB, the "Patriarca" and six terrorists are eliminated, seven terrorists are captured, bodies are recovered, and the lifting of the chain of custody of 4 PCs with two hard disks and six USB is done.

After the end of the operation, the national news informs the public about combats in the area of Pasacaballos between the army and the terrorists of the UTIL, and radio communication with the central command of the UTIL is performed immediately, using signal intelligence, to report that JACOB escaped the fighting without problems. This considering the interception of the communications that it has the intelligence about UTIL.

The collected material is delivered to judicial authorities, who, through the use of forensic analysis, investigate the implication of the two companies TECNOPON and ASES and the links between the police and the UTIL.

Twenty days after the Thunder operation, by signals intelligence and interception of communications of the Central Commander of the terrorist organization UTIL, is delivered to intelligence, the location of the meeting where alias JACOB should attend with the Supreme Commander of the UTIL this because intelligence has control of communications between the group of Jacob and the UTIL central command. This information triggers new successful operations against the terrorist organization UTIL.

4 Final Comparative Analysis of Results

The actual cases presented present faults or failures as a final result and demonstrates the procedural problems in the development of the operations or during the intelligence activities, and exposing the obsolescence of the traditional intelligence cycle.

The case of Edward Snowden showed the current weaknesses in the management of intelligence because the classified information was leaked and directly affected the CIA and the American government; cases in Colombia as the D.A.S, showed at the same time, the failures in the process of intelligence, triggering the total elimination of the agency and the discrediting of this state. In those cases, the intelligence information was used in a wrong way and the persons involved never followed the traditional cycle.

Additionally, as a final result, the scenario analysis Case 1 is shown and the results obtained by applying the current cycle and the new process of micro cycles for the intelligence:

Results of Case 1: using the traditional intelligence cycle.

> During the development of the BETA operation aimed at the elimination of alias JACOB, four children, and two women who apparently lived near the area of operations die. This shows ignorance of the area of operations and reconnaissance, intelligence also

does not provide all of the information necessary for the operation, leaving aside, the clear information about area thus generating the illegitimacy of intelligence and discontent of the civilian population.

The human intelligence source also dies in the area. Poor communication between analysts and agents in the field does not allow informing the human source about the operation that is going to be developed. The analysts receive the information about the meeting of alias JACOB and inform the commander, who plans an operation immediately, without verification and communication of the whole situation.

The special commands that had been sent damaged two PCs while collecting the evidence in the area. A proper chain of custody to the elements collected was not conducted for later use as evidence at trial. Ignorance of the digital collection procedures and electronic equipment testing is denoted.

There was no deep analysis of intelligence information and the meeting in Pasacaballos, where the human source and the use of USB, could have provided more information to intelligence to plan and manage better strategic results against the terrorist organization UTIL.

The analyses are not deep and are too weak during the planning of operations, allowing failures of procedures. Besides, there is no clear understanding of the objectives of fighting against the terrorist organization UTIL. The objective was Jacob but the information was not studied well, only searching an opportunity result and not trying to get the real advantage over the enemy.

Results case 1: using the new process of micro cycles for intelligence with the use of technological resources.

The planning of the operation was supported by technical intelligence, signal intelligence and cyber intelligence, obtaining better sources of information because they allow clear and agile information, contributing to complement the human intelligence developed in the field of operations, thus enhancing the results and promoting the achievement of the objectives of high strategic value

With the use of geo-intelligence and intelligence technical, some preliminary knowledge about the area of operation could be obtained, gaining strategic advantage over the target, thus preventing collateral damage against the civilian population and maintaining the legitimacy of intelligence.

With constant communication between analysts and agents, using the source penetrated for obtaining further information properly, at the same time maintaining the safety of the source and the agents.

It was possible to exploit the information obtained through the use of cyber intelligence. This information served as support of the intelligence gathered against collaborators and infiltrate cops, taking more proofs of the relations with UTIL.

The knowledge of the rules and procedures for collecting digital evidence as well as technical knowledge allowed to safeguard the integrity of the information found, later used as material evidence in criminal investigations.

The uses of technology intelligence systems to be involved in the process facilitate the verification of databases and other records for the correlation of information, facilitating the analysis.

Taking into account the results obtained within the presented scenario (Case 1), using the two processes, in both cases the operating results are obtained that are aligned with the proposed objectives. However, the scenario of the traditional cycle, although technological intelligence systems were used, demonstrates communication failures in terms of planning, collection and analysis of the Thunder operation, plus there is incomplete information and ignorance in handling and following the procedures for the use of systems and technology resources, because the use of technological systems and the cyberspace was not into the process, leaving aside the cyber intelligence and cyber defense, using them only as tools of collection and in some cases for analyzing and forwarding the information.

When the new process of micro cycles was used, this showed notably better communication and control of the information speed among the parties with greater agility and security, respecting the confidentiality, integrity and availability of information. It is possible to see that the process already includes technological systems, and the cyberspace is used as support and field support at multiple stages. Moreover, the information is collected by different sources, and it is clearer, allows better planning and analysis in the development of the operation conducted; the exploitation of the information obtained allows to project new objectives while excellent results are obtained, ensuring the information and the development of all intelligence work.

In the real cases described above, the inclusion of technology and the cyberspace within the intelligence process would probably have provided greater security of the information that was handled, optimizing the planning, collection, analysis and dissemination of information, exploiting its advantages and making sure that the full processes would lead to better results without scandals and failures as well as maintaining the confidentiality, integrity and availability of information intelligence, which is the main asset of the work that is done in intelligence.

5 Conclusions

The intelligence cycle is obsolete, because it is an ancient process that takes place in digital world, without taking into account the fact that the information, being its main asset, is managed and moves into digital form using all types of technology within the new operational environment, the cyberspace.

Today, everything is about the internet of things, where every single thing is related to some kind of technology and the vast majorities are connected to each other in some way. The intelligence has been modernized and uses many sources to face current challenges, revealing inherent weaknesses of intelligence cycle in terms of planning, collecting, analyzing, and disseminating the information in the 21st century.

Digital information is collected, analyzed and sent through cyberspace, also, technological resources for management and treatment are used, requiring special care, supported by cyber intelligence to exploit and protect cybersecurity.

The unification and integration of the processes using technology in the field of cyberspace provides better opportunities for collection, analysis and dissemination of intelligence information, as well as helps obtaining results with more operational success; but it also increases the existing risk of new threats in cyber world, so it is necessary to protect intelligence through cybersecurity and technology.

The confidentiality, integrity and availability of intelligence information can only be supported by the integration of information technology systems. Consequently, a good cyber defense strategy shields the intelligence structure, and cybersecurity protects the confidentiality of the intelligence information from leakage, theft or sabotage. Using systems of classification and evaluation of the information, with the encryption programs for information transmission, it is protected as well, keeping it safe and unabridged, avoiding it from being modified by third parties in the process; similarly, with the use of databases and secure communication channels for consultation and management, the information is available permanently.

The new process of intelligence micro cycles integrates technology in the process of obtaining intelligence by prioritizing the use of cyber intelligence and other intelligence techniques, such as cybersecurity, to protect the process by maintaining the confidentiality, integrity and availability of intelligence information. Improving the control over the speed of the information securing it at the same time, the communication among the stakeholders into the process is better for the knowledge of how is being used the information in each step. Since the planning the process and who develop it use and know how to use the technology systems.

Colombia needs to update its intelligence, to face the new operational environment and new challenges, where the battlefield is the cyberspace. It should start from updating the processes and procedures to make intelligence and integrating with technological resources is extremely important.

The new process of micro cycles for intelligence needs to be implemented and put into practice to evaluate their performance, validity and effectiveness.

6 References

[1] J. Davis, "Sherman Kent and the Profession of Intelligence Analysis" Occasional Papers: Volume 1, Number 5, (2002).

[2] "Escuela de las Américas. Inteligencia de Combate", *Derechos.org*, 2016. [Online]. Available: http://www.derechos.org/nizkor/la/libros/soaIC/cap3.html. [Accessed: 16-May- 2016].

[3] D. Navarro Bonilla, "El Ciclo de Inteligencia y sus Limites", (2004).

[4] I. Duyvesteyn, B De Jong, and J van Reijn. *The Future of Intelligence: Challenges in the 21st Century*. Routledge, (2014).

[5] H. M Urigüen. "*Colombia y sus vecinos frente al conflicto armado"*. Flacso-Sede Ecuador (2005).

[6] A. Bonilla "Percepciones de la amenaza de seguridad nacional de los países andinos: regionalización del conflicto colombiano y narcotráfico". *GÓMEZ, José Maria (Comp.). América Latina y el (des) orden global neoliberal. Hegemonía, contrahegemonía, perspectivas. Buenos Aires: CLACSO*. (2004).

[7] S Granada., J. Restrepo, &, A Vargas. "El agotamiento de la política de seguridad: evolución y transformaciones recientes en el conflicto armado colombiano". *Guerra y violencias en Colombia: herramientas e interpretaciones*, 27-124. (2009).

[8] J. Gentry and D. Spencer, "Colombia's FARC: A Portrait of Insurgent Intelligence", *Intelligence and National Security*, vol. 25, no. 4, pp. 453-478, 2010.

[9] D. M Rojas. "Estados Unidos y la guerra en Colombia". *Instituto de Estudios Políticos y Relaciones Internacionales, Nuestra guerra sin nombre, Bogotá, Universidad Nacional/Norma*. (2006).

[10] M. Phythian, *"Understanding the intelligence cycle*. Routledge". (2013)

[11] B D. Berkowitz, A. E. Goodman. "*Best truth: Intelligence in the information age"*. Yale University Press, pp.21–2. (2000).

[12] J. Davis, "Sherman Kent and the Profession of Intelligence Analysis" Occasional Papers: Volume 1, Number 5, (2002).

[13] A. Hulnick, "What's wrong with the Intelligence Cycle", *Intelligence and National Security*, vol. 21, no. 6, pp. 959-979, 2006.

[14] G. Evans, "Rethinking Military Intelligence Failure – Putting the Wheels Back on the Intelligence Cycle", *Defence Studies*, vol. 9, no. 1, pp. 22-46, 2009.

[15] P. G. Keen "The intelligence cycle: a differentiated perspective on information processing". In *Proceedings of the June 13-16, 1977, national computer conference* (pp. 317-320). ACM. (1977).

[16] P. H. Davies, K., Gustafson, I. Rigden "The intelligence cycle is dead, long live the intelligence cycle: Rethinking intelligence fundamentals for a new intelligence doctrine". (2013).

[17] "Studies in Intelligence: Table of Contents — Central Intelligence Agency", *Cia.gov*, 2016. [Online]. Available: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies. [Accessed: 19- Apr- 2016].

[18] O. Clotworthy, "*Some Far-out Thoughts on Computers Bringing the Computer into Intelligence Work"* Studies in Intelligence: Table of Contents — Central Intelligence Agency", *Cia.gov*, 2016. [Online]. Available: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies. [Accessed: 19- Apr- 2016].

[19] S. J. Hatch. *Managing the "Reliability Cycle": An Alternative Approach to Thinking About Intelligence Failure* " Studies in Intelligence: Table of Contents — Central Intelligence Agency, *Cia.gov*, 2016. [Online]. Available: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies. [Accessed: 19- Apr- 2016].

[20] J. R. Holzer*, PhD, .F L. Moses, PhD "Autonomous Systems in the Intelligence Community: Many Possibilities and Challenges".* Studies in Intelligence: Table of Contents — Central Intelligence Agency", *Cia.gov*, 2016. [Online]. Available: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies. [Accessed: 19- Apr- 2016].

[21] M. Goodman. *Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do about It (Doubleday, 2015), 392 pp.* Studies in Intelligence: Table of Contents — Central Intelligence Agency", *Cia.gov*, 2016. [Online]. Available: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-

studies/studies. [Accessed: 19- Apr- 2016].

[22] P. Fei Yeh. *"The Case for Using Robots in Intelligence Analysis"* Studies in Intelligence: Table of Contents — Central Intelligence Agency, *Cia.gov*, 2016. [Online]. Available: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies. [Accessed: 19- Apr- 2016].

[23] R. Johnston, 'Testing the Intelligence Cycle through Systems Modelling and Simulation', in Analytic Culture in the US Intelligence Community (CIA Centre for Studies in Intelligence 2005) Online version at⟨https://www.cia.gov/library/center-for-the-study-ofintelligence/CSI-publications/books-and-monographs/analytic-culture-in-the-U-Sintelligence-community/chapter_4_systems_model.htm⟩, accessed on 11 May. 2016

[24] M. V Hayden. "Beyond Snowden: an NSA reality check." *World Affairs* 176.5: 13+. *Academic OneFile*. Web. 24 Mar. 2016, (2014)

[25] B. Gellman, E. Nakashima. "US spy agencies mounted 231 offensive cyber-operations in 2011", documents show. *Washington Post, 31*. (2013).

[26] S. G. Vombatkere. "Edward Snowden's Wake-Up Call–Cyber Security, Surveillance and Democracy". *Countercurrents. org*. (2013)

[27] U. Bar-Joseph, R. McDermott. Change the analyst and not the system: A different approach to intelligence reform. *Foreign Policy Analysis*,*4*(2), 127-145. (2008)

[28] P. Gill, M. Phythian, "*Intelligence in an insecure world"*. Polity. (2006)

[29] D.C. Cortés González. "Bajo la alfombra del DAS recuento de los hechos relevantes que marcaron la vida del Departamento Administrativo de Seguridad." (2012).

[30] J. D. Laverde Palma. "*Un sistema de inteligencia torcido: el DAS como instrumento de un proyecto presidencialista autoritario"* (Doctoral dissertation, Universidad Nacional de Colombia).

[31] P. C. Bravo Medina." Historia de un escándalo". (2010).

[32] E. T. Barrett. "Warfare in a new domain: The ethics of military cyber-operations". *Journal of Military Ethics*, *12*(1), 4-17. (2013).

[33] D. Trujillo, "Traduciendo la realidad: Guerra de 5ª Generación; la conquista de las mentes", *Lugrogeopolitica.blogspot.com.ee*, 2013. [Online]. Available:

http://lugrogeopolitica.blogspot.com.ee/2013/06/guerra-de-5-generacion-la-conquista-de.html. [Accessed: 10- May- 2016].

[34] F. J. Cilluffo, S. L. Cardash. “Cyber Domain Conflict in the 21st Century”. *Seton Hall J. Dipl. & Int'l Rel., 14*, 41. (2013).

[35] J. H. Eom, N. U. Kim, S. H. Kim, T. M. Chung. “Cyber military strategy for cyberspace superiority in cyber warfare”. In *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on* (pp. 295-299). (2012).

Glossary

C.I.A	Central of Intelligence Agency
F.A.R.C	Fuerzas Armadas Revolucionarias de Colombia (The Revolutionary Armed Forces of Colombia)
E.L.N	Ejercitó de Liberación Nacional (The National Liberation Army)
I.T.S.A.R	Intelligence, Surveillance, Target Acquisition and Reconnaissance
D.C.P.D	Direction, Collection, Processing and Dissemination
D.A.S	Departamento Administrativo de Seguridad (Administrative Department of Security)
U.T.I.L	Unión de Trabajadores Independientes para la Liberación (Union of Independent Workers for the Liberation)
E.E.I	Essential Elements Intelligence
O.R.I	Other Requirements Intelligence

Counter-intelligence: Intelligence activity that seeks to defend, protect, and shield the organization of subversion, sabotage, infiltration and terrorism.

E.E.I: The Essential Elements of Intelligence, are the requirements, questions and minimum data that required the intelligence to carry out their work, what ?, why ?, how ?, where ?, who ?, when ?, for what ?.

Guerrillas: Illegal armed groups in Colombia in opposition to a legitimate government normally with Marxist or Leninist ideologies.

Human mail: Person who serves the narco-terrorist groups in Colombia to carry and bring information or materials.

Intelligence Cycle: Process through which intelligence is developed and produced using the available information, divided into four phases, planning, collection analysis and dissemination.

Narco-terrorist: Person belonging to an illegal armed group dedicated to drug trafficking and terrorism.

Net of intelligence: Special group belonging to an intelligence agency, responsible for carrying out intelligence work in a particular area of responsibility.

NCOs: Staff sub-ranges pertaining to the Military Forces of Colombia, who serve as technical and executors of the orders given by the officers.

O.R.I: The Other Requirements for Intelligence is data or additional information, which is required in the intelligence process to complete the planning or intelligence analysis.

Operation BETA: Code name given to the military operation on which bombing is made to a particular area or target.

Ringleader: Chief or commander of an illegal armed group.

License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Luis Alejandro Velasquez Hurtado**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:
   1.1. Reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and
   1.2. Make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

Of my thesis

Colombia and the Intelligence Cycle on the 21 Century, the Digital Age,

Supervised by Olaf Manuel Maennel

Raimundas Matulevicius

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **30.05.2016**