

ANTONY ANTONIOU (OSINT Security Analyst)

OPEN SOURCE INFORMATION, THE FUTURE OF INTELLIGENCE



EUROPEAN INTELLIGENCE ACADEMY E-BOOK

No. 1
MAY 2013

OPEN SOURCE INFORMATION, THE FUTURE OF INTELLIGENCE

ANTONY ANTONIOU
(OSINT Security Analyst)

Preface.

People from ancient times to our days had understood the importance of information and the significant role that valid information can play in all fields of human activities (politics, economy, during wars etc). References to spies, and their methods – techniques and means that they used can be found in historical texts from antiquity until today, also known theorists of war have addressed and reported (in their writings), the importance of information and the necessity of an enemy misinformation (we will mention two of them of Carl Von Clausewitz¹ and Sun - Tzu²).

The intelligence services began to take shape during the Second World War. Pioneers at the “intelligence field” were the Germans (in espionage, cryptography - cryptology, propaganda and generally speaking at the development of the appropriate techniques – methods and instruments – means), followed by British. Americans because of their non-participation in the war had left behind in the development of techniques and means for collecting and processing information. This changed after the Japanese attack on Pearl Harbor³ and the American entry into the war⁴. The USA intelligence

¹ Carl Philipp Gottfried von Clausewitz (1 July 1780 – 16 November 1831): was a German-Prussian soldier and military theorist who stressed the "moral" (in modern terms, psychological) and political aspects of war. His most notable work, “Vom Kriege”, (On War), was unfinished at his death.

² Sun Tzu or Sunzi: was an ancient Chinese military general, strategist and philosopher from the Zhou Dynasty. He is traditionally believed to be the author of “The Art of War”, an extremely influential ancient Chinese book on military strategy. Sun Tzu has had a significant impact on Chinese and Asian history and culture, both as an author of The Art of War and through legend, his work continues to influence both Asian and Western culture and politics.

³ The surprise attack leads by the Japanese on 7 December of 1941, except from triggering America's entry into the war had also revealed a significant failure on the part of the U.S. intelligence apparatus. Investigations had shown that intelligence had been handled in a casual, uncoordinated manner, and there had been insufficient attention to certain collection requirements. The lack of coordination among intelligence agencies, (principally the Army and the Navy), caused a failure to provide timely dissemination of relevant information to key decision – makers. This has led to the establishment of a more centralized intelligence structure (after the WW II ended).

⁴ In July 1941, in response to **William J. Donovan*** urging, Roosevelt appointed Donovan as Coordinator of Information to form a non-military intelligence organization. The Coordinator of Information was to “collect and analyze all information and data which may bear upon the national security” for the President and those he designated. The Coordinator was given the authority, “with the approval of the President,” to request data from other agencies and departments, but was specifically admonished not to interfere with the duties and responsibilities of the President's military and naval advisers. Borrowing heavily from the British intelligence model, Donovan created a special staff to pull together and analyze all national security information and empanelled an eight-member review board, drawn from academia, to review analysis and test its conclusions. In concert with the Librarian of Congress, COI Donovan organized the Division of Special Information at the Library, to work with Donovan's analytical staff and to coordinate scholarship within the Library and in academia. * **William J. Donovan**, was an aficionado of intelligence and a veteran of World War I, whom Roosevelt sent to Europe in 1940 to gather information on the stability of Britain and again in the spring of 1941 to gather information on Italian Dictator Mussolini, among other matters. Upon his return, Donovan lobbied hard for the creation of a centralized, civilian intelligence apparatus to complement that of the military.

capacity (both military and civilian) was developed during the war⁵. In the aftermath of World War II⁶, with the Cold War looming on the horizon, the United States began the process of developing an elaborate peacetime intelligence structure that would extend across a number of governmental services and agencies⁷.

After the end of WW II and during the Cold War era the world was divided into two "spheres of influence", countries which "bound" to the American "bandwagon" and those which "bound" to the former Soviet Union "bandwagon". Thus began a struggle between Western and Eastern intelligence services and agencies about which will prevail. This struggle became more and more intense, rapid technological development have led to the development of new techniques – methods and means of collecting intelligence and the search for countermeasures to deal with them, thousands of man hours, and trillions have been wasted in the effort of prevalence. While it has had various incarnations over the years, intelligence has historically played a key role in providing support to the military forces and also shaping the foreign policies towards other countries for both USA and former Soviet Union (and their allies). The competition between the two coalitions (North Atlantic Treaty Organization – NATO and Warsaw Pact⁸), lasted from the decade of 1950 to 1990 (it peaked in the decade of 1980, during the presidency of Ronald Wilson Reagan⁹). The technological development has led to the emergence of new intelligence services – agencies and intelligence disciplines (such as ELINT, SIGINT, GEOINT, etc).

Another key point to the intelligence evolution and transformation, (by adapting to new developments and upcoming threats), took place from late 1989 to 1995. Three years after the Presidents Bush election, profound changes emerged all over the world. Those changes have had enormous impacts on the Intelligence Community through out the world. The "Trigger event" of those changes was the fall of 1989, the Berlin Wall "breaking"¹⁰, this lead Germany to begin the

⁵ America's entrance into WW II created an immediate need for intelligence. Although the Army and the Navy maintained their own intelligence organizations, none were prepared to provide the kind of intelligence effort needed. To bolster this effort, in June 1942 the Office of Strategic Services (OSS) was created under the recently established Joint Chiefs of Staff to succeed in the Information Coordination effort. William Donovan remained in charge of the reorganized unit. In addition to assuming the analytical role of its predecessor, the OSS was chartered to carry out clandestine operations against the Axis powers on a worldwide scale. Despite it's obvious utility, the new Service faced strong competition from the FBI and the Army's intelligence organization.

⁶ The end of the war automatically caused a reduction in the immediate needs for intelligence, a vigorous and heated debate ensued between those who favoured the Donovan idea of an independent, civilian intelligence organization reporting directly to the President and those who favoured retention and control of intelligence by the military.

⁷ The National Security Act of 1947, signed into law by President Harry S. Truman established the Central Intelligence Agency (CIA), headed by the Director of Central Intelligence (DCI), who was given the responsibility of coordinating all the agencies and services of US national intelligence community. It is the descendant of the Office of Strategic Services (OSS) of World War II, which was dissolved in October 1945 and its functions transferred to the State and War Departments. The National Security Act of 1947 had also established both the National Security Council and the Central Intelligence Agency. Rear Admiral Roscoe H. Hillenkoetter was appointed as the first Director of Central Intelligence.

⁸ The Warsaw Treaty Organization of Friendship, Cooperation, and Mutual Assistance (1955–1991), was a mutual defense treaty between eight communist states of Central and Eastern Europe in existence during the Cold War. The founding treaty was established under the initiative of the Soviet Union and signed on 14 May 1955, in Warsaw. The Warsaw Pact was the military complement to the Council for Mutual Economic Assistance (CoMEcon), the regional economic organization for the communist states of Central and Eastern Europe. The Warsaw Pact was a Soviet military reaction to the integration of West Germany into NATO in 1955, per the Paris Pacts of 1954.

⁹ The US President Ronald Reagan, had made the revitalization of intelligence part of his campaign. Intelligence budgets were increased, and new personnel were hired. On 4 December 1981, President Reagan issued his Executive Order on Intelligence. With this E.O he managed to reaffirmed the functions of intelligence agencies and continued most of the previous restrictions, but it set a more positive tone than its predecessor. He also gave to the CIA greater latitude to gather foreign intelligence within the United States and to provide assistance to law enforcement.

¹⁰ The Berlin Wall: was a barrier constructed by the German Democratic Republic (GDR, East Germany) starting on 13 August 1961, that completely cut off, (by land), West Berlin from surrounding East Germany and from East Berlin. In 1989, a series of radical political changes occurred in the Eastern Bloc, associated with the liberalization of the Eastern Bloc's authoritarian systems and the erosion of political power in the pro-Soviet governments in nearby Poland and Hungary. After several weeks of civil unrest, the East German government announced on 9 November 1989 that all GDR citizens could visit West Germany and West Berlin. Crowds of East Germans crossed and climbed onto the wall, joined by West Germans on the other side in a celebratory atmosphere. Over the next few weeks, a euphoric public and souvenir hunters chipped away parts of the wall; the governments later used industrial equipment to remove most of the rest. The physical Wall itself was primarily destroyed in 1990.

process of reunification. Influenced by these political developments the other Communist regimes of Eastern Europe started their democratization. The event that radically changed the orientation of the Intelligence Community occurred at the mid of 1990, this event was the collapse of the former Soviet Union (almost all the former Soviet Republics have started to declare their independence), before 1991 ends, the Communist rule ended in Russia. The collapse of the Soviet Union caused “shock” to the intelligence community (both Western¹¹ and Eastern), the necessity of maintaining intelligence capabilities has been challenged strongly (especially in the USA), this in turn caused both the reduction of the available funds and personnel as well¹². The collapse caused chaos in the former Soviet intelligence services as well. The Komitet Gosudarstvennoy Bezopasnosti¹³ (KGB), was

broken up into five services¹⁴ and although thousands of former KGB professionals left the service in the 1990s, some of the most effective Russian assets remained in place¹⁵, this coupled with the election of President Putin, (a former KGB officer), who took over from Boris Yeltsin in 1999, reinstated Russian espionage efforts back at “Cold War levels”, and the Federalnaya Sluzhba Bezopasnosti Rossiyskoy Federatsii¹⁶ (FSB), was demonstrating the ruthlessness of its predecessor.

On the contrary the western intelligence organizations (especially in the USA), didn’t manage to adapt to the new challenges¹⁷. In their effort to react intelligence chiefs of staff began streamlining their services and agencies and reorienting toward new missions, with a greater focus on transnational threats. Despite their efforts, the U.S. intelligence agencies entered the twenty-first century still having the “heavy” and “stiff” organizational structure that is “inherited” from the “Cold War” era¹⁸. The non-successful (in a short period of time), reorganization and necessary transformation, (adopting “flexible” organizational structures and an “Information Sharing Policy” between the services and agencies), had led to the second biggest failure of the US Intelligence apparatus since the Pearl Harbor attack. This failure led to the second biggest terrorist attack on American soil¹⁹, which was the attack on the World Trade Center on the 11 September of 2001. Sharp criticism brought upon the Intelligence community, which charged the detection failure and the

¹¹ The Dutch foreign intelligence service was for a short time actually abolished. Richard J. Aldrich: “Beyond the Vigilant State: Globalization and Intelligence,” *Review of International Studies*, Vol. 35, 2009.

¹² Although the current budget and personnel size of the intelligence services and agencies are classified, both budgetary and personnel figures are headed downward. Each agency is smaller than it was in the late 1980s, and further cuts have been mandated (a 75 percent cut of 1985-89 levels).

¹³ Komitet gosudarstvennoy bezopasnosti (KGB: was the main security agency for the Soviet Union from 1954 until its collapse in 1991. It was the chief government agency of “union-republican jurisdiction”, acting as internal security, intelligence, and secret police. The KGB also has been considered a military service and was governed by army laws and regulations. Its main functions were foreign intelligence, counterintelligence, operative-investigatory activities, guarding the State Border of the USSR, guarding the leadership of the Central Committee of the Communist Party of the Soviet Union and the Soviet Government, organization and ensuring of government communications as well as fight against nationalism, dissent, and anti-Soviet activities.

¹⁴ The five agencies were the following: SVR (foreign intelligence), FSB (internal security), FAPSI (communications), FSO (federal protection), and GUSP (special programs). Military intelligence, the GRU, was left largely untouched. Robert W. Pringle, “The Intelligence Services of Russia,” in Loch Johnson (Ed.), *The Oxford Handbook of National Security Intelligence* (Oxford: Oxford University Press, 2010).

¹⁵ In 1995, the CIA discovered that Aldrich Ames had been spying for the Russians for 10 years and a few years later Robert Hanssen, (an FBI agent), has been arrested, accused of spying for the Russians for 20 years.

¹⁶ Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii (FSB): is the main domestic security agency of the Russian Federation and the main successor agency of the Soviet Committee of State Security (KGB). Its main responsibilities are counter-intelligence, internal and border security, counter-terrorism, and surveillance.

¹⁷ With the end of the Cold War, the overriding threat of the Soviet Union (and their allies), has been replaced by an increasing array of smaller threats, (such as people trafficking, drug smuggling, regional conflicts, “low intensity conflicts”, piracy, terrorism, etc), each requiring attention from the intelligence community.

¹⁸ Many services - agencies, (such as: Director of National Intelligence, National Intelligence Council (NIC), National Counterterrorism Center (NCTC), National Counterintelligence Executive (NCIX), Central Intelligence Agency (CIA), National Security Agency (NSA), Defense Intelligence Agency (DIA), Federal Bureau of Investigation (FBI), Defense Protective Service (DPS), often with overlapping responsibilities, competitive spirit, and without an “Information Sharing Policy”.

¹⁹ The Oklahoma City bombing was a terrorist bomb attack on the Alfred P. Murrah Federal Building in downtown Oklahoma City on the 19th April of 1995. It’s considered as the most destructive act of terrorism on American soil until the 9/11 terrorist attacks. The Oklahoma blast claimed 168 lives, (including 19 children under the age of 6), and injured more than 680 people. The blast destroyed or damaged 324 buildings within a sixteen-block radius, destroyed or burned 86 cars, and shattered glass in 258 nearby buildings. The bomb was estimated to have caused at least \$652 million worth of damage.

unsuccessful tackling of the upcoming danger²⁰. All the facts sawn that the conventional belief that terrorists “want to draw peoples attention but without casing a lot of casualties among them” was no longer applicable. Powerful non-state actors were now capable of wreaking havoc on a global scale and posing a major threat to international security without the need of being “sponsored” by “great powers”. All those dramatic changes (globalization, the emergence of new threats, etc), “forced” the intelligence community to transform and adapt. For half a century intelligence services and agencies had developed a labyrinth of classifications during collection, processing and intelligence exploitation²¹. But this system was now preventing the information sharing needed to address new potential enemies and threats. Intelligence services and agencies now had to balance their traditional need for “secrecy” with the new need to form “horizontal” information sharing in order to produce intelligence – knowledge.

The new types of threats require continuous collection - processing and exchange of information between the intelligence organizations (both civil and military,) in order to achieve the quickest detection and management of these threats (while reducing the costs of acquisition and management of the information needed). It became obvious that the intelligence services and agencies had to stop using clandestine gathering and collecting methods and moved to an all sources gathering – collection model, and also reform their structure in order to adapt to this model.

The only intelligence discipline that combines most of the above requirements is the Open Source Intelligence (OSINT), discipline. Although open sources were frequently used in the intelligence process, their value was seen as secondary. Classified information was deemed more valuable and often more credible. The systematic acquisition of non-classified information was rarely seen as an intelligence priority. In our days things have changed²², OSINT’s importance is widely acknowledged²³. Summarizing, we can say that the main reasons highlighted the significance of OSINT as an Intelligence Discipline are the following three:

- The broadening of the security “agenda” over the past two decades. This broadening causes by match the expansion of the issues range that the intelligence organizations have to deal with. These issues include, among others: Terrorism, the proliferation of weapons of mass destruction (PWD), organized crime, illegal immigration, energy security, etc). As a result, information services and agencies have to cope with the increased need for more and larger inflow, (collection, processing and analysis), of information, which in turn has fostered a growing appreciation of the value and utility of OSINT.
- The evolution of the internet and the emergence of the collaborative web have alerted security actors to the potential of new tools and technologies for collecting, analyzing, and distributing knowledge on global affairs. The information revolution through Internet evolution led to the creation of a growing market for commercial intelligence vendors offering products and services previously restricted to the public sector.

²⁰ Since the 1990s an increased frequency of terrorist attacks has been observed around the world, in Bombay, Calcutta, New York, Khobar, Nairobi and Dar es Salaam. While these events garnered increased attention, it was the sarin gas attack in Tokyo (1995), and especially the 9/11 attacks, that revealed the power of religiously motivated terrorism in the post-Cold War world. Paul R. Pillar: “Dealing with Transnational Threats,” in US Department of Commerce, Directorate of Intelligence 1952-2002: Fifty Years of Informing Policy (Springfield, VA: National Technical Information Service, 2002), Todd and Bloch. Pillar: “Dealing with Transnational Threats”. D. Howard and James J.F. Forest: “Weapons of Mass Destruction and Terrorism”, McGraw-Hill, New York, 2012.

²¹ In order to minimize the possibilities of successful Soviet espionage.

²² The development of the Internet, and it’s universal usage and application in an increasing range of human activities, and by extension the sheer volume of migrant through this information helped to highlight the significant role of OSINT as an information gathering – collecting discipline.

²³ Estimates sawn that OSINT provides between 80 and 90 per cent of the information used by the intelligence community.

- The intelligence apparatus failures led to 9/11 attacks and to the Iraqi invasion have also contributed to this development²⁴. Particularly in the US, these failures have prompted a thorough reassessment of the way in which intelligence is used to shape the policy – making process.

The scope of this paper, other than to highlight the significance of open intelligence sources as an intelligence discipline, is also the ability of been used as a basic intelligence manual for the reader or to “newcomers” in the “wonderful world” of intelligence.

Executive Summary.

As we have already mentioned in the previous section, the secondary objective of this study is the ability of been used as a basic intelligence manual – guide, to achieve this purpose we will not only hawker issues regarding open sources of information, but we will try to gradually introduce the reader to the variety of issues related to information and intelligence management and processing.

At the first chapter we are going to present the definitions of the terms relating to information, intelligence and their management. Some of those terms are: data and data analysis, information and types of information sources, how to evaluate those sources, methods of information analysis and information assessment, the scope of intelligence, intelligence as a finished product, etc.

At the second chapter we will proceed to the presentation of the main intelligence disciplines, their principals, techniques and methods and how those disciplines can be applied by the intelligence analysts to the Intelligence Cycle. We are also going to present issues that are related to intelligence such as Espionage, Industrial Espionage, and Propaganda. We will also refer to the principles underlying the above issues and the techniques – methods and means used in their application.

Finally, at the third chapter, we will focus on issues that are exclusively related with open sources intelligence as a discipline, while demonstrating the significance of OSINT.

The paper ends with a short conclusion epilogue. The documentation of those listed, has been done using the Harvard system. This concerns the parenthetical reference of the author, year and page, immediately after those in need of documentation, this enables the interface with the indicated literature. For reasons of flexibility, it has also been used the system of Leipzig, with the index reference number coincides with the one in footnote index.

CHAPTER 1.

Defining The Basic Concepts.

To understand the fundamentals which are governing the open intelligence sources we shall proceed to the presentation and explanation of some basic concepts and definitions.

1.1 Data.

The word data is the plural of datum, neuter past participle of the Latin “dare”, which means “to give”, hence “something given”. In discussions of problems in geometry, mathematics, engineering, and so on, the terms givens and data are used interchangeably. Such usage is the origin of data as a concept in computer science or data processing: data are numbers, words, images, etc., accepted as they stand. So Data are values of qualitative or quantitative variables, belonging to a set of items. Data processing are represented in a structure, often tabular (represented by rows and columns), a tree (a set of nodes with parent-children relationship) or a graph structure (a set of interconnected nodes). Data are typically the results of measurements and can be visualised using graphs or images. Data as an abstract concept can be viewed as the lowest level of abstraction from which information

²⁴ An Open Source Center was established by the US Director of National Intelligence in November 2005. Since then, the number of OSINTpositions in the US intelligence community has grown.

and then knowledge are derived. Raw data, i.e., unprocessed data, refers to a collection of numbers, characters and is a relative term; data processing commonly occurs by stages, and the “processed data” from one stage may be considered the “raw data” of the next. Field data refers to raw data collected in an uncontrolled in situ environment. Experimental data refers to data generated within the context of a scientific investigation by observation and recording. Data is most often used as a singular mass noun in educated everyday usage. In scientific writing data is often treated as a plural, as in these data does not support the conclusions, but it is also used as a singular mass entity like information, for instance in computing and related disciplines²⁵.

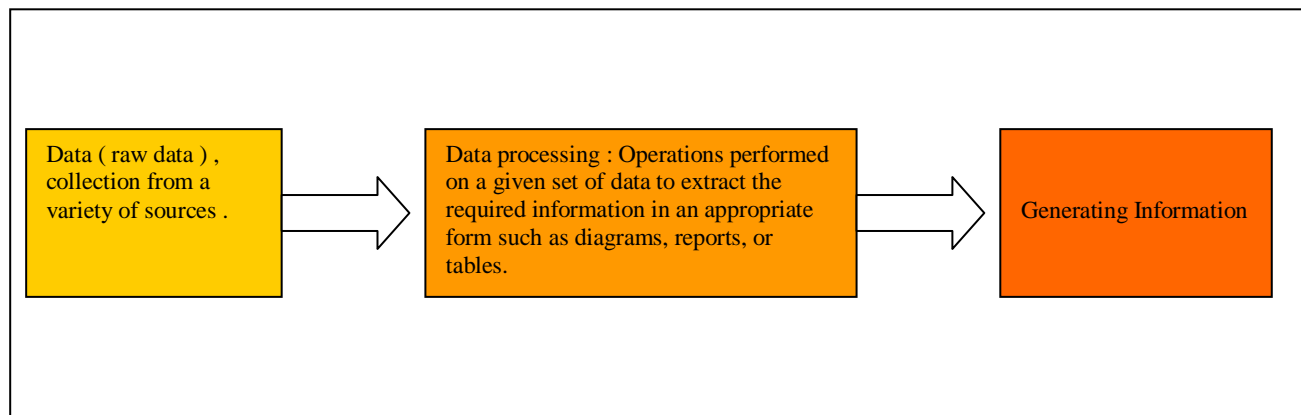


Table 1: Generating Information from “Raw Data” .

1.1.1 Data Processing.

Is any process that uses a computer program to enter data and summarise, analyse or otherwise convert data into usable information. It involves recording, analysing, sorting, summarising, calculating, disseminating and storing data. Because data are most useful when well-presented and actually informative, data-processing systems are often referred to as information systems. Nevertheless, the terms are roughly synonymous, performing similar conversions; data-processing systems typically manipulate raw data into information, and likewise information systems typically take raw data as input to produce information as output. Data processing may or may not be distinguished from data conversion, when the process is merely to convert data to another format, and does not involve any data manipulation²⁶.

1.1.2 Data Analysis.

When the domain from which data are harvested is a science or engineering field, the terms data processing and information systems are considered too broad, and the more specialized term data analysis is typically used. Data analysis, arguably a special kind of data processing, focuses on highly-specialized and highly-accurate algorithmic derivations and statistical calculations that are less often observed in the typical general business environment. A divergence of culture between data processing in general and data analysis is exhibited in the numerical representations generally used; In data processing, measurements are typically stored as integers, fixed-point or binary-coded decimal

²⁵ R.W. Burchfield, (1996): Fowler's Modern English Usage (3rd ed.). Oxford: Clarendon Press. pp. 197–198. ISBN 0-19-869126-2.

²⁶ www.en.wikipedia.org

representations of numbers, whereas the majority of measurements in data analysis are stored as floating-point representations of rational numbers²⁷.

1.1.3 Open Source Data (OSD).

Open Source Data is the raw print, broadcast, oral debriefing or other form of information from a primary source. It can be a photograph, a tape recording, a commercial satellite image, or a personal letter from an individual²⁸.

1.2 Information.

The English word was apparently derived from the Latin “informatio”, this noun derived from the verb “informare” (to inform) in the sense of “to give form to the mind”, “to discipline”, “instruct”, “teach”. The verb is inform, which comes, (via French informer), from the Latin verb informare, to give form, to form an idea of something. Furthermore, Latin itself already contained the word informatio meaning concept or idea, but the extent to which this may have influenced the development of the word information in English is not clear.

Various definitions have been proposed and "classifications" of the concept of information. The meaning or semantic content reflect the main concept but there are many ways given the practical importance of information²⁹:

- ❖ In strictly technical terms we perceive information as a sequence of symbols that reflect or transmit a message.
- ❖ In general terms information affects non random evolution of any system.

As a meaning, regards or is associated with:

- transmission of messages,
- interpreting data (which have been evaluated qualitatively or quantitatively, and have been impressed time),
- identification of hidden identity variables with actual figures (pattern theory),
- visualization / animation symbols,
- the form they take in mind the stimuli from the sensory organs,
- perception,
- meaningful performance,
- the doctrine,
- knowledge acquisition,
- organized control (managed by RBI, directs or controls) himself or another system,
- the degree of statistical dependence between the variables of a system (information theory),
- especially, organization, order and complexity.

So in general we can claim that:

“Information is defined as knowledge element which transforms and gives value to things that become important.”³⁰

²⁷ www.en.wikipedia.org

²⁸ NATO OSINT Handbook .

²⁹ Luciano Floridi, (2005): Is Information Meaningful Data?, paragraph: 2. The Standard Definition of Information, Philosophy and Phenomenological Research, pp. 351 – 370.

Regarding the issue of our study, we can claim that:

“Information are the results of the data collection, data processing and evaluation in order to produce knowledge (intelligence in our case)”.

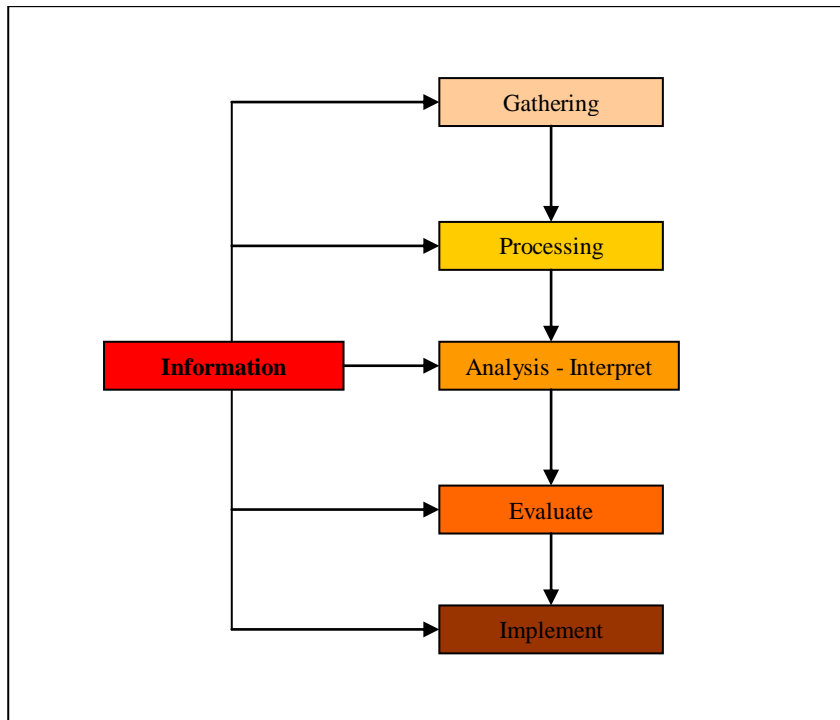


Table 2: The Information Environment.

1.2.1 Types of Information Sources.

There are a number of different definitions for primary, secondary and tertiary types of information sources. Those definitions vary according to academic discipline in which they referred to (i.e. science or humanities). So in general terms of speaking:

- Primary sources:
 1. Normally is evidence or accounts of the events, practices, or conditions being researched.
 2. Present information in its original form, not interpreted or condensed or evaluated by other writers.
 3. Are created by a person (s) who directly experienced that event.
 4. However, what constitute a primary source of information depends on the discipline or context (how the material is used).
- Secondary sources :
 1. A secondary source of information is one that was created by someone who did not have a first-hand experience or participate in the events being researched.
 2. Are generally accounts written after the fact with the benefit of hindsight.

³⁰ TheFreeDictionary, Library & Information Center, University of Thessaly, ARISTOTLE UNIVERSITY OF THESSALONIKI – “Informatics and Management”, in Application Development Programming Environment, collective writing of textbooks - Edited by Spyros Dukakis.

3. Secondary sources describe, analyze, interpret, evaluate, comment on and discuss the evidence provided by primary sources.
 4. They are not evidence, but rather commentary on and discussion of evidence.
 5. A secondary data is one that has been collected by individuals or agencies for purposes other than those of a particular research study.
 6. Examples are: textbooks, bibliographies, biographical works, commentaries, criticisms, dictionaries, encyclopedias.
 7. What constitutes a secondary source of information depends on discipline or how the information is used.
- Tertiary sources :
 1. These are works which list primary and secondary resources in a specific subject area.
 2. Materials that index, organize and compile citations to, and show how secondary (and sometimes primary) sources could be used.
 3. These are materials in which information from secondary sources has been “digested” - reformatted and condensed, and put into a convenient, easy-to-read form.
 4. Examples include: almanacs, directories, population registers/ statistics, fact books, abstracts, indexes, bibliographies, chronologies, classifications, handbooks, guide books and manuals.

The main differences between primary, secondary and tertiary are the ones listed below:

- Primary sources of information are original manuscripts, documents or records used in preparing a published or unpublished papers or studies.
- Secondary sources are published or unpublished papers or studies that rely on primary source(s).
- Tertiary sources are published or unpublished papers or studies that are based on secondary sources.
- It is sometimes difficult to differentiate between primary, secondary and tertiary sources.

1.2.2 Means - Formats of Information Sources.

These are means by which a person is informed about something or knowledge is provided or share with someone, a group of people or an organization (public or private). There are three main producers-creators of information. These are:

1. Government
 - a. Departments
 - b. Agencies
 - c. Ministries
2. Academic-Research Institutions
 - a. colleges
 - b. Universities
 - c. Research institutes
3. Private Sector
 - a. Private Individuals
 - b. Not for profit organizations
 - c. For profit organizations and commercial agencies

- d. International Agencies
- e. Professional Associations or organizations
- f. Private institutions
- g. Corporate bodies and laboratories

There is a great diversity and a variety of information formats. The two main formats are:

1. Print: Books, magazines, journals, bibliographies, maps, indexes and abstracts, photographs, government documents, technical reports, etc.
2. Non-print: audio visual, multimedia, microform and electronic books and journals, images, texts/records from the Internet, Web documents, etc.

1.2.3 Evaluating Information Sources (The Information Cycle).

A practical way of evaluating the information is to consider where information comes from and how it has been produced. The relationship between the different information sources is clearly shown at the below diagram, which called The Information Cycle.

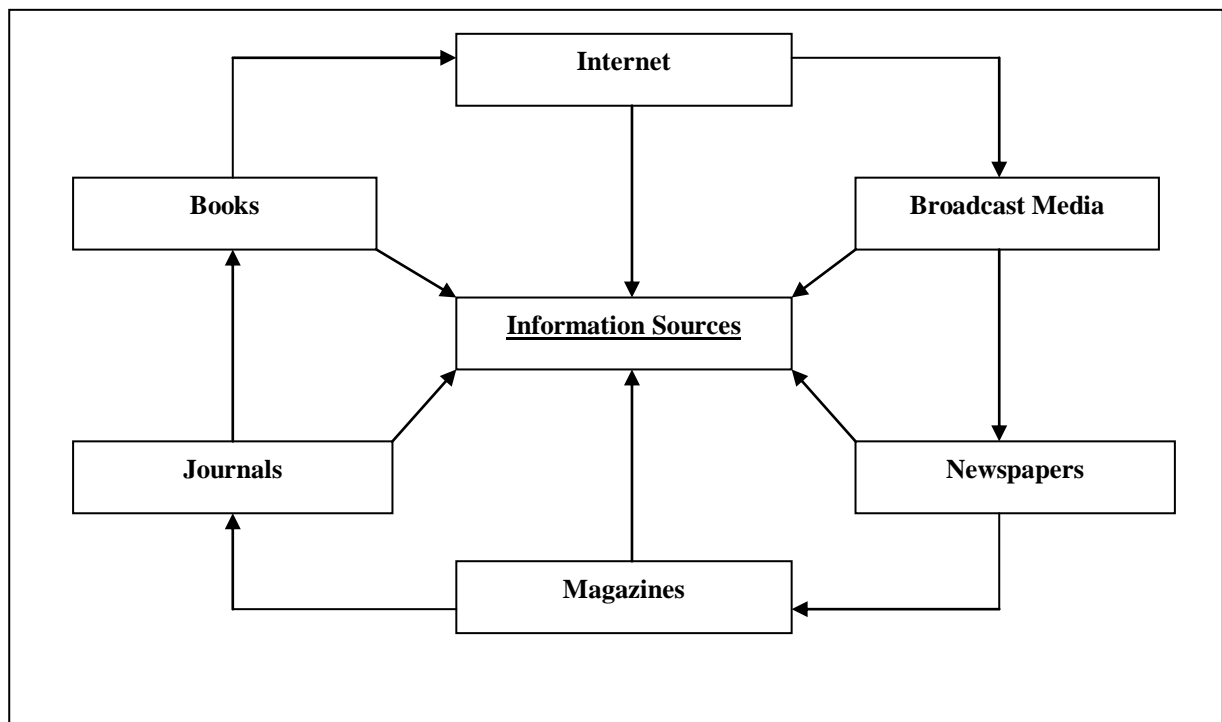


Diagram 1: The Information Cycle .

The Information Cycle illustrates how information is published in set patterns. Information at the beginning of the cycle (Internet) is aimed at an audience wanting quick, up-to-date data or facts. As the information progresses round the “Cycle” it becomes more detailed but also more out of date. When deciding on the quality of the information you may have balance reliability (accurate and proven facts) against currency (the period of time over which the information was written and produced). Information changes as it progresses along the Information Cycle from format to format:

- **Internet:** The Internet is usually the first place information is posted. Information can appear almost instantaneously on the Internet, but this leaves a short period of time for the author to write the information. As a result the information tends to be descriptive, explaining what has

happened and who was involved (it is simply stating facts). There will also be a lack of depth and the information posted will be short.

- **Broadcast Media:** Information is also likely to appear quickly on television and radio. Initially the information will be produced rapidly and is likely to be descriptive, explaining what has happened and who was involved. Professional journalists with expertise in a particular area may be able to provide some relevant background information, and it is likely that expert opinion will also be expressed. As time passes and more information becomes available, larger and more detailed articles and documentary features may be produced.
- **Newspapers:** Newspapers are published frequently; usually daily or weekly. The articles will be written by professional journalists, who often have expertise in a particular area. The emphasis will be on reporting facts, and once the information appears in newspapers the author has had more time to process the information, so there may be greater depth such as statistics, analysis **or** expert opinion. Newspaper articles will not be correctly referenced and they will not provide a bibliography or list of sources, so it will be difficult to identify where the author has found his information.
- **Magazines:** The articles are written by professional journalists with knowledge of a specific **subject** area. There will be emphasis on reporting facts but usually with some analysis as the author has more time to reflect on the information and conduct some research. Although articles in the professional press are likely to be longer than newspaper articles they are unlikely to be correctly referenced with no bibliography or list of sources, so it is difficult to tell what sources the author has used in his research.
- **Journals:** Academic journals contain articles written by scholars and specialist researchers. The authors have had time to conduct their own research and review the available literature. As a result the article will be a detailed examination of the subject with analysis and primary research. Research can take months to conduct, so the article will not be current.
- **Books/e-books:** They may take years to be published, and so are not good sources of up to date information. The strength of books as a resource lies in their authorship, they are usually written by scholars and experts in a certain field. Their content can be variable ranging from a simplified overview of a subject to an in depth piece of research. Books offer a great introduction to a new subject. Books include a list of the sources the author has used to research their book called a reference list. The reference list allows you to review the original sources of information used in the book, which can be used in your assignments to strengthen your own research and arguments.

1.2.4 Open Source Information (OSIF).

Open Source Information is comprised of data that can be put together, generally by an editorial process that provides some filtering and validation as well as presentation management. OSIF is generic information that is usually widely disseminated. Newspapers, books, broadcast, and general daily reports are part of the OSIF world³¹.

1.3 Difference Between data, information and knowledge.

The terms data, information and knowledge (intelligence in our case), are frequently used for overlapping concepts. The main difference is in the level of abstraction being considered. Data is the lowest level of abstraction, information is the next level, and finally, knowledge (intelligence), is the highest level among all three³². Data on its own carries no meaning, for data to become information, it must be interpreted and take on a meaning. Information as a concept bears a diversity of meanings,

³¹ NATO OSINT Handbook .

³² Akash Mitra (2011): "Classifying data for successful modelling", www.en.wikipedia.org

from everyday usage to technical settings. Generally speaking, the concept of information is closely related to notions of constraint, communication, control, data, form, instruction, knowledge, meaning, mental stimulus, pattern, perception, and representation. Beynon-Davies uses the concept of a sign to distinguish between data and information, data are symbols while information occurs when symbols are used to refer to something³³.

Term	Definition	Example
Fact	Verified information: something known to exist or to have happened.	A confirmed inventory of a resource of one's own service.
Direct Information	The content of reports, research, and analytic reflection on an intelligence issue that helps analysts and their consumers evaluate the likelihood that something is factual and thereby reduces uncertainty, Information relating to an intelligence issue under scrutiny the details of which can, as a rule, be considered factual, because of the nature of the source, the source's direct access to the information, and the concrete and readily verifiable character of the contents.	<u>COMINT</u> or <u>OSINT</u> quoting what a foreign official said; <u>IMINT</u> providing a count of the number of ships at a pier. <u>HUMINT</u> from a US diplomatic officer who directly observed an event.
Indirect Information	Information relating to an intelligence issue the details of which may or may not be factual, the doubt reflecting some combination of the source's questionable reliability, the source's lack of direct access, and the complex character of the contents.	<u>HUMINT</u> from a reliable agent, citing secondhand what an informant said that a government official said. <u>OSINT</u> providing a foreign government document that gives the number of ships at a pier. Indirect <u>OSINT</u> from a US embassy officer. <u>COMINT</u> that contains a report by a foreign official to his government, about what something he cannot confirm, but states with a probability.
Direct Data	Organized information that provides context for evaluating the likelihood that a matter under scrutiny is factual.	A chronology of events based on observations by US officers.
Indirect Data	Organized information that provides context for evaluating the likelihood that a matter under scrutiny is factual.	A chronology based on reports from a liaison intelligence service.

Table 3: Definitions of the Kind of Information.³⁴

1.4 Intelligence.

Intelligence is the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations (their policy, their political ideas and thesis etc), hostile or potentially hostile nations, forces or elements, or areas of actual or potential interests. The term is also applied to the activity that results in the product and to the organizations engaged in such activity. The purpose of intelligence is to provide organizations (public or private), and their staff with timely, relevant, accurate, predictive, and tailored intelligence

³³ Beynon P-Davies (2002): Information Systems: An introduction to informatics in organisations. Basingstoke, UK: Palgrave Macmillan. ISBN 0-333-96390-3, and Beynon P-Davies (2009): Business information systems. Basingstoke, UK: Palgrave. ISBN 978-0-230-20368-6.

³⁴ Central Intelligence Agency, Directorate of Intelligence (February 1997), A Compendium of Analytic Tradecraft Notes, retrieved 2007-12-03, en.wikipedia.org .

about a specific question or other aspects of interests. Intelligence supports the planning, preparing, assessment and execution of operations (of any kind)³⁵.

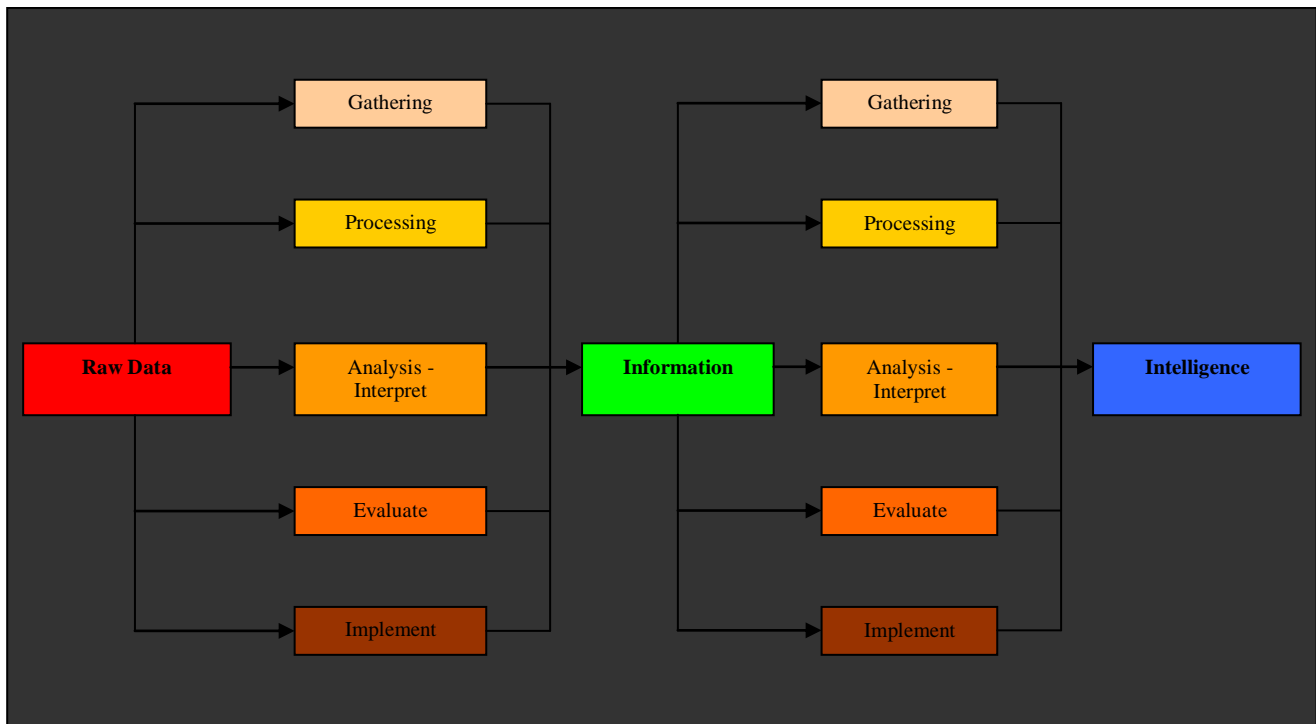


Diagram 2: Generating Intelligence.

1.4.1 The Intelligence Process.

The process of tasking, collecting, processing, analyzing, and disseminating intelligence is called the intelligence cycle. The traditional Intelligence cycle is a concept that describes the fundamental cycle of intelligence processing in a civilian or military intelligence agency or in law enforcement as a closed path consisting of repeating nodes³⁶. It starts with the needs of those who are often referred to within the Intelligence Community as intelligence “consumers” that is, policymakers, military officials, and other decision makers who need intelligence information in conducting their duties and responsibilities. These needs also referred to as intelligence requirements are sorted and prioritized within the Intelligence Community, and are used to drive the collection activities of the members of the Intelligence Community that collect intelligence. The stages of the intelligence cycle include the issuance of requirements by decision makers, collection, processing, analysis, and publication of intelligence. The circuit is completed when decision makers provide feedback and revised requirements³⁷.

³⁵ Intelligence Field Manual FM 2-0 (2010).

³⁶ <https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html>,
www.en.wikipedia.org.

³⁷ <https://courseware.e-education.psu.edu/courses/bootcamp/1o07/09.html>.

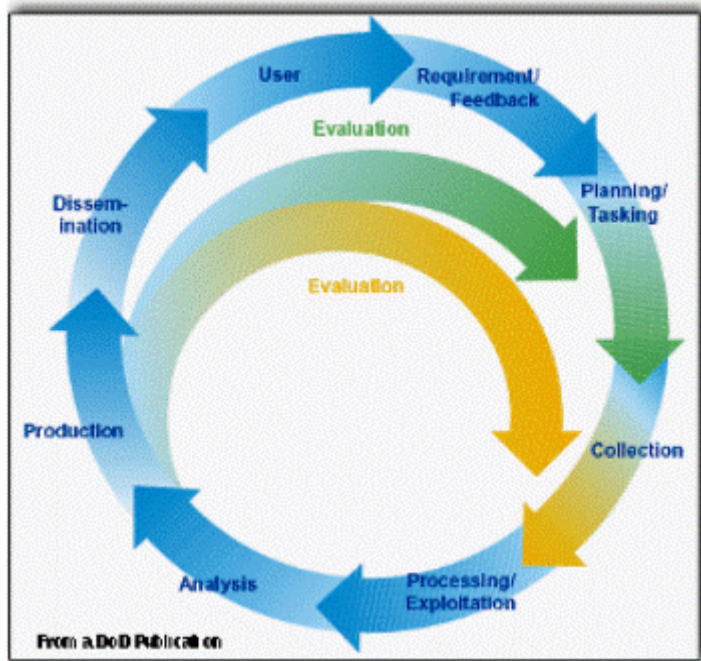


Diagram 3: The Intelligence Cycle.

The term “intelligence process” refers to the steps or stages in intelligence, from policy makers perceiving a need for information, to the community's delivery of an analytical intelligence product to them. Those steps are:

- **Requirements:** Identifying requirements means defining those policy issues or areas to which intelligence is expected to make a contribution, as well as decisions as to which of these issues has priority over the others. It may also mean specifying the collection of certain types of intelligence. The impulse is to say that all policy areas have intelligence requirements, which they do. However, intelligence capabilities are always limited, so priorities must be set, with some requirements getting more attention, some getting less, and some perhaps getting little or none at all. The key questions are: Who sets these requirements and priorities and then conveys them to the intelligence community? What happens, or should happen, if policy makers fail to set these requirements on their own?
- **Collection:** Once requirements and priorities have been established, the necessary intelligence must be collected. Some requirements will be better met by specific types of collection, some may require the use of several types of collection. Making these decisions among always-constrained collection capabilities is a key issue, as is the question of how much can or should be collected to meet each requirement.
- **Processing and Exploitation:** Collection produces information, not intelligence. That information must undergo processing and exploitation before it can be regarded as intelligence and given to analysts. Conversion of large amounts of data to a form suitable for the production of finished intelligence includes translations, decryption, and interpretation of information stored on film and magnetic media through the use of highly refined photographic and electronic processes.
- **Analysis and Production:** Identifying requirements, conducting collection, and processing and exploitation are meaningless unless the intelligence is given to analysts who are experts in their respective fields and can turn the intelligence into reports that respond to the needs of the policy makers. The

types of products chosen, the quality of the analysis and production, and the continuous tension between current intelligence products and longer-range products are major issues. Analysis and production includes the integration, evaluation, and analysis of all available data, and the preparation of a variety of intelligence products, including timely, single-source, event-oriented reports and longer term, all-source, finished intelligence studies.

Significantly most discussions of the intelligence process end here with dissemination, and the intelligence having reached the policy makers whose requirements first set everything in motion. However, Mark Lowenthal (2006), bundles dissemination with consumption and adds feedback:

- **Dissemination and Consumption.**

These two steps are taken together by Lowenthal for seemingly good reasons. The process of dissemination, or the process of moving intelligence from producers to consumers, is largely standardized, with consumption being assumed in the 5-step process. However, Lowenthal points out that policy makers are not pressed into action by the receipt of intelligence, and if and how they consume intelligence is key (Lowenthal, 2006, p. 62).

- **Feedback.**

A dialogue between intelligence consumers and producers should take place after the intelligence has been received. Policy makers should give the intelligence community some sense of how well their intelligence requirements are being met, and discuss any adjustments that need to be made to any parts of the process. Ideally, this should happen while the issue or topic is still relevant, so that improvements and adjustments can be made³⁸.

1.4.2 Intelligence Analysis.

Intelligence analysis is the process of evaluating and transforming raw data and information into descriptions, explanations, and judgments for policy consumers. It involves assessing the reliability and credibility of the data - information and comparing it to the knowledge base available to the analyst, in order to separate fact from error and uncover deception. Each collected item is then examined to determine its nature, proportion, function, relevancy, and interrelationships. Related items will be grouped together and the extent to which they confirm, supplement, or contradict each other will be determined. Once done, the relevant information will be synthesized in order for the analyst to make predictions, gain insight, identify information gaps, or explain a complex set of facts and relationships. Analysts add value to this process by using their substantive knowledge of the issue at hand, and adding, where appropriate, relevant open information. The reverse also holds. Analysis may start from a review and assessment of the relevant open sources, to which would be added “the special knowledge that cannot be obtained without utilizing intelligence sources and methods”. Most intelligence analysis is predictive in nature and follows a simple pattern: it describes what is known, to highlight the interrelationships that form the basis for the judgment, and offers a forecast. Of course, accurate estimates depend at least as much upon the mental model used by the analyst as upon the accuracy and completeness of the information itself³⁹.

An analysis is not a nicely arranged scrapbook of raw data. It should have a summary of the key characteristics of the topic, followed by the key variables and choices. Increasingly deep analysis can explain the internal dynamics of the matter being studied, and eventually to prediction, known as estimation. The purpose of intelligence analysis is to reveal to a specific decision maker the underlying significance of selected target information. Analysts should begin with confirmed facts, apply expert knowledge to produce plausible but less certain findings, and even forecast, when

³⁸ <https://courseware.e-education.psu.edu/courses/bootcamp/1o07/09.html>.

³⁹ [e-education.psu.edu/courses/bootcamp/1o09/04.html](https://courseware.e-education.psu.edu/courses/bootcamp/1o09/04.html).

the forecast is appropriately qualified. Analysts should not, however, engage in fortunetelling that has no basis in fact.

1.4.2.1 Types of Reasoning Apply to Intelligence Analysis.

To produce intelligence objectively, the analyst must employ a process tailored to the nature of the problem. Four basic types of reasoning apply to intelligence analysis⁴⁰:

- **Induction (seeking causality):** The induction process is one of discovering relationships among the phenomena under study. It may come from human pattern recognition ability, looking at a seemingly random set of events, perhaps writing them on cards and shuffling them until a pattern emerges. While induction, for human beings, is usually not at a fully rational level, do not discount the potential role of software that uses statistical or logical techniques for finding patterns. Induction is subtly different from intuition: there usually is a pattern that induction recognizes, and this pattern may be applicable to other situations.
- **Deduction (applying the general):** is the classic process of reasoning from the general to the specific, a process made memorable by the famous Sherlock Holmes: “How often have I said to you that when you have eliminated the impossible, whatever remains, however improbable, must be the truth?” Deduction can be used to validate a hypothesis by working from premises to conclusion.
- **Trained Intuition:** Analysts need to harness trained intuition: the recognition that one has come to a spontaneous insight. The steps leading there may not be apparent, although it is well to validate the intuition with the facts and tools that are available. Experienced analysts, and sometimes less experienced ones, will have an intuition about some improbable event in a target country, and will collect more data, and perhaps send out collection requests within his or her authority. These intuitions are useful just often enough that wise managers of analysts, unless the situation is absolutely critical, allow them a certain amount of freedom to explore.
- **Scientific method:** Astronomers and nuclear physicists, at different ends of the continuum from macroscopic to microscopic, share the method of having to infer behaviour, consistent with hypothesis, not by measuring phenomena to which they have no direct access, but by measuring phenomena that can be measured and that hypothesis suggests will be affected by the mechanism of interest. Other scientists may be able to set up direct experiments, as in chemistry or biology. If the experimental results match the expected outcome, then the hypothesis is validated, if not, then the analyst must develop a new hypothesis and appropriate experimental methods.

In intelligence analysis, the analyst rarely has direct access to the observable subject, but gathers information indirectly. Even when the intelligence subject at hand is a technical one, analysts must remain aware that the other side may be presenting deliberately deceptive information. From these gathered data, the analyst may proceed with the scientific method by generating tentative explanations for a subject event or phenomenon. Next, each hypothesis is examined for plausibility and compared against newly acquired information, in a continual process toward reaching a conclusion. Often the intelligence analyst tests several hypotheses at the same time, whereas the scientist usually focuses on one at a time. Furthermore, intelligence analysts cannot usually experiment directly upon the subject matter as in science, but must generate fictional scenarios and rigorously test them through analysis methods which are presented below.

⁴⁰ Krizan, Lisa (June 1999), [Intelligence Essentials for Everyone](#), Joint Military Intelligence College, retrieved 2009-05-24.

1.4.2.2 Analysis Methods.

The types of reasoning, which are described above, are ways which the analyst uses in order to draft the product, the methods which are described below are ways of validating the analyst's results of reasoning.

Opportunity Analysis: identifies for policy officials opportunities or vulnerabilities that the customer's organization can exploit to advance a policy, as well as dangers that could undermine a policy. To make the best use of opportunity analysis, there needs to be a set of objectives for one's own country, preferably with some flexibility to them. The next step is to examine personalities and groups in that target country to see if there are any with a commonality of interest. Even though the different sides might want the same thing, it is entirely possible that one or the other might have deal-breaking conditions. If that is the case, then ways to smooth that conflict need to be identified, or no more work should be spent on that alternative. Conversely, if there are elements that would be utterly opposed to the objectives of one's side, ways of neutralizing those elements need to be explored. They may have vulnerabilities that could render them impotent, or there may be a reward, not a shared opportunity, that would make them cooperate.

Linchpin Analysis: proceeds from information that is certain, or with a high probability of being certain. By starting from known's (and impossibilities), the analyst has a powerful technique for showing consumers, peers, and managers that a problem has both been thoroughly studied and constrained to reality⁴¹. Linchpin analysis was introduced to CIA by Deputy Director for Intelligence (1993–1996) Doug MacEachin, as one of the "muscular" terms he pressed as an alternative to academic language, which was unpopular with many analysts. He substituted linchpin analysis for the hypotheses driving key variables. MacEachin required the hypotheses - or linchpins - needed to be explicit, so policymakers could be aware of coverage, and also aware of changes in assumptions. This method is an "anchoring tool" that seeks to reduce the hazard of self-inflicted intelligence error as well as policymaker misinterpretation. It forces use of the checkpoints listed below, to be used when drafting reports:

1. Identify the main uncertain factors or key variables judged likely to drive the outcome of the issue, forcing systematic attention to the range of and relationships among factors at play.
2. Determine the linchpin premises or working assumptions about the drivers. This encourages testing of the key subordinate judgments that hold the estimative conclusion together.
3. Marshal findings and reasoning in defence of the linchpins, as the premises that warrant the conclusion are subject to debate as well as error.
4. Address the circumstances under which unexpected developments could occur. What indicators or patterns of development could emerge to signal that the linchpins were unreliable? And what triggers or dramatic internal and external events could reverse the expected momentum?

⁴¹ Davis, Jack (1999), "Improving Intelligence Analysis at CIA: Dick Heuer's Contribution to Intelligence Analysis", *Psychology of Intelligence Analysis*, Center for the Study of Analysis, Central Intelligence Agency, Davis 1999, retrieved 2007-10-27.

Analysis of Competing Hypotheses: Dick Heuer spent years in the CIA Directorate of Operations and worked on methodology of analysis both in his later years and after retirement⁴². Some of his key conclusions, coming from both experience and an academic background in philosophy, include:

1. The mind is poorly “wired” to deal effectively with both inherent uncertainty (the natural fog surrounding complex, indeterminate intelligence issues) and induced uncertainty (the man-made fog fabricated by denial and deception operations).
2. Even increased awareness of cognitive and other “unmotivated” biases, such as the tendency to see information confirming an already-held judgment more vividly than one sees “disconfirming” information, does little by itself to help analysts deal effectively with uncertainty.
3. Tools and techniques that gear the analyst's mind to apply higher levels of critical thinking can substantially improve analysis on complex issues on which information is incomplete, ambiguous, and often deliberately distorted. Key examples of such intellectual devices include techniques for structuring information, challenging assumptions, and exploring alternative interpretations.

In 1980, he wrote an article, “Perception: Why Can't We See What Is There to be Seen?” which suggests to Davis⁴³ that Heuer's ideas were compatible with linchpin analysis.

Given the difficulties inherent in the human processing of complex information, a prudent management system should:

1. Encourage products that (a) clearly delineate their assumptions and chains of inference and (b) specify the degree and source of the uncertainty involved in the conclusions.
2. Emphasize procedures that expose and elaborate alternative points of view—analytic debates, devil's advocates, interdisciplinary brainstorming, competitive analysis, intra-office peer review of production, and elicitation of outside expertise.

According to Heuer, analysts construct a reality based on objective information, filtered through complex mental processes that determine which information is attended to, how it is organized, and the meaning attributed to it. What people perceive, how readily they perceive it, and how they process this information after receiving it are all strongly influenced by past experience, education, cultural values, role requirements, and organizational norms, as well as by the specifics of the information received. To understand how the analysis results, one must use good mental models to create the work, and understand the models when evaluating it. Analysts need to be comfortable with refinement, and challenge. To go back to linchpin analysis, the boundary conditions give places to challenge and test, reducing ambiguity. More challenge, according to Heuer, is more important than more information. He wanted better analysis to be applied to less information, rather than the reverse. Given the immense volumes of information that modern collection systems produce, the mind is the limiting factor. Mirror-imaging is one of Heuer's favourite example of a cognitive trap, in which the analyst substitutes his own mindset for that of the target. “To see the options faced by foreign leaders as these leaders see them”, according to Heuer, “one must understand (the foreign leaders), values and assumptions and even their misperceptions and misunderstandings”.

Dick Heuer created the model of **Analysis of Competing Hypotheses** (ACH). In this model there is competition among competing hypotheses of the foreign leader's assumptions, which will reduce mirror-imaging even if they do not produce the precise answer. The best use of information,

⁴² Heuer & Richards J. Jr. (1999), “Psychology of Intelligence Analysis. Chapter 2. Perception: Why Can't We See What Is There To Be Seen?”, History Staff, Center for the Study of Intelligence, Central Intelligence Agency, retrieved 29-10-2007.

⁴³ Davis, Jack (1999), “Improving Intelligence Analysis at CIA: Dick Heuer's Contribution to Intelligence Analysis”, Psychology of Intelligence Analysis, Center for the Study of Analysis, Central Intelligence Agency, Davis 1999, retrieved 27-10-2007.

in this context, is to challenge the assumption the analyst likes best. One of the key motivations for ACH, according to Heuer, is to avoid rejecting deception out of hand, because the situation looks straightforward. Heuer observed that good deception looks real. “Rejecting a plausible but unproven hypothesis too early tends to bias the subsequent analysis, because one does not then look for the evidence that might support it. The possibility of deception should not be rejected until it is disproved or, at least, until a systematic search for evidence has been made and none has been found”. His ACH model consists of the following steps⁴⁴:

1. Identify the possible hypotheses to be considered. Use a group of analysts with different perspectives to brainstorm the possibilities.
2. Make a list of significant evidence and arguments for and against each hypothesis.
3. Prepare a matrix with hypotheses across the top and evidence down the side. Analyze the “diagnostic” of the evidence and arguments—that is, identify which items are most helpful in judging the relative likelihood of the hypotheses.
4. Refine the matrix. Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value.
5. Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove the hypotheses rather than prove them.
6. Analyze how sensitive your conclusion is to a few critical items of evidence. Consider the consequences for your analysis if that evidence were wrong, misleading, or subject to a different interpretation.
7. Report conclusions. Discuss the relative likelihood of all the hypotheses, not just the most likely one.
8. Identify milestones for future observation that may indicate events are taking a different course than expected.

Analogy: is common in technical analysis, but engineering characteristics seeming alike do not necessarily mean that the other side has the same employment doctrine for an otherwise similar thing.

1.4.2.3 The Analytic Process.

Although it is possible that the exact process used from analyst to analyst may vary, there are a series of steps it is recommended that all analysts use⁴⁵, those steps are:

1. **Define the problem:** Policy makers will have questions based on their intelligence requirements. Sometimes questions are clear and can easily be addressed by the analyst. Sometimes however, clarification is required due to vagueness, multiple layers of bureaucracy between customer and analyst, or due to time constraints. Just as analysts need to try to understand the thinking of the adversary, analysts need to know the thinking of their customers and allies.
2. **Generate hypotheses:** Once the problem is defined, the analyst is able to generate reasonable hypotheses based on the question. For example, a business may want to know whether a competitor will lower their prices in the next quarter. From this problem, two obvious hypotheses are:
 - The competitor will lower prices or
 - The competitor will not lower prices.

⁴⁴ Heuer & Richards J. Jr. (1999), “Psychology of Intelligence Analysis. Chapter 8: Analysis of Competing Hypotheses”, History Staff, Center for the Study of Intelligence, Central Intelligence Agency, retrieved 28-10-2007.

⁴⁵ Heuer & Richards J. Jr. (1999), “Psychology of Intelligence Analysis. Chapter 2. Perception: Why Can't We See What Is There To Be Seen?”, History Staff, Center for the Study of Intelligence, Central Intelligence Agency, retrieved 29-10-2007.

However, with a little brainstorming, additional hypotheses may become apparent. Perhaps the competitor will offer discounts to long term customers, or perhaps they may even raise prices. At this point, no hypothesis should be discarded.

3. **Determine information needs & gather information:** In intelligence, collection usually refers to the step in the formal intelligence cycle process. In many cases, the information needed by the analyst is either already available or is already being sought by collection assets (such as spies, imagery satellites, etc.). If not, the analyst may request collection on the subject, or if this is not possible identify this information gap in their final product. The analyst will generally also research other sources of info, such as open source (public record, press reporting), historical records, and various databases.
4. **Evaluate sources:** Information used for intelligence analysis (whether national, criminal, or business) has been obtained from people or organizations that are actively seeking to keep the information from the analyst, or who are providing misleading information. Adversaries do not want to be analyzed correctly by competitors. This withholding of information is known as counterintelligence, and is very different from similar fields of research, such as science and history where information may be misleading, incomplete or wrong, but rarely does the subject of investigation actively deny the researcher access. So, the analyst must evaluate incoming information for reliability (has the source reported accurate information in the past?), credibility (does the source reasonably have access to the information claimed? Has the source lied in the past?), and for possible denial and deception (even in the source is credible and reliable, they may have been fooled).
5. **Evaluate (test) hypotheses:** This is the step most would consider “actual analysis”. Here the analyst compares the evidence gathered against his or her hypotheses, using various analytic tools and methods such as Analysis of Competing Hypotheses or link charts⁴⁶. Many hypotheses may be quickly discarded, while for others there may simply not be enough information one way or the other to evaluate them.
6. **Production and packaging:** Once hypotheses have been evaluated, the intelligence product must create for the consumer. Three key features of the intelligence product are:
 - Timeliness: includes not only the amount of time required to deliver the product, but also the usefulness of the product to the customer at a given moment.
 - Scope: involves the level of detail or comprehensiveness of the material contained in the product.
 - Periodicity: describes the schedule of product initiation and generation.

Government intelligence products are typically packaged as highly structured written and oral presentations, including electrical messages, hardcopy reports, and briefings. Many organizations also generate video intelligence products, especially in the form of live daily “newscasts,” or canned documentary presentations. Analysts should understand the relationship between the analyst's and the consumer's organization. There may be times that while the ultimate consumer and originating analyst simply want to pass information, a manager in either chain of command may insist on a polished format.

⁴⁶ <http://www.peterlance.com/Peter%20Lance/3.21.00%20Link%20Chart.html>.

7. **Peer review:** Information is disseminated to people who need it within the intelligence agency. “Coordination with peers is necessary. If you think you are right, and the coordinator disagrees, let the assessment reflect that difference of opinion and use a footnote, called a reclama”,⁴⁷ inside the US intelligence community if necessary. But never water down your assessment to a lowest common denominator just to obtain coordination. In large intelligence establishments, analysts have peers at other agencies. The practical amount of coordination, indeed inside one's own agency, will depend on the secure collaboration tools available (wikis, analyst web pages, email), the schedule and availability of the other analysts, any restrictions on dissemination of the material, and the analyst's ability to play nicely with others. Extremely specialized issues might have very few people who could meaningfully look at it.
8. **Customer Feedback and Production Evaluation:** The production phase of the intelligence process does not end with delivering the product to the customer. Rather, it continues in the same manner in which it began: with interaction between producer and customer. For the product to be useful, the analyst and policymaker need to hear feedback from one another, and they refine both analysis and requirements. A feedback procedure between producers and customers includes key questions, such as:
 - Is the product usable?
 - Is it timely?
 - Was it in fact used?
 - Did the product meet expectations?
 - If not, why not?
 - What next?

The answers to these questions lead to refined production, greater use of intelligence by decision makers, and further feedback sessions. Thus, production of intelligence generates more requirements in this iterative process.

1.4.3 Intelligence Assessment.

Intelligence assessment is the development of forecasts of behaviour or recommended courses of action to the leadership of an organization (private or public), based on a wide range of available information sources both overt and covert. Assessments are developed in response to requirements declared by the leadership in order to inform decision making. Assessment may be carried out on behalf of a country-state, military, a company or an organisation (private or public), using information-intelligence from various available sources. An intelligence assessment reviews both available information and previous assessments for relevance and currency, where additional information is required some collection may be directed by the analyst.

Intelligence assessment is based on a customer requirement, which may be a standing requirement or tailored to a specific circumstance or “need”, a Request for Information (RFI). The “requirement” is passed into the assessing agency and worked through the “Intelligence Cycle”.

⁴⁷ US Department of Defense (12 July 2007) (PDF), Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms, retrieved 2007-10-01.

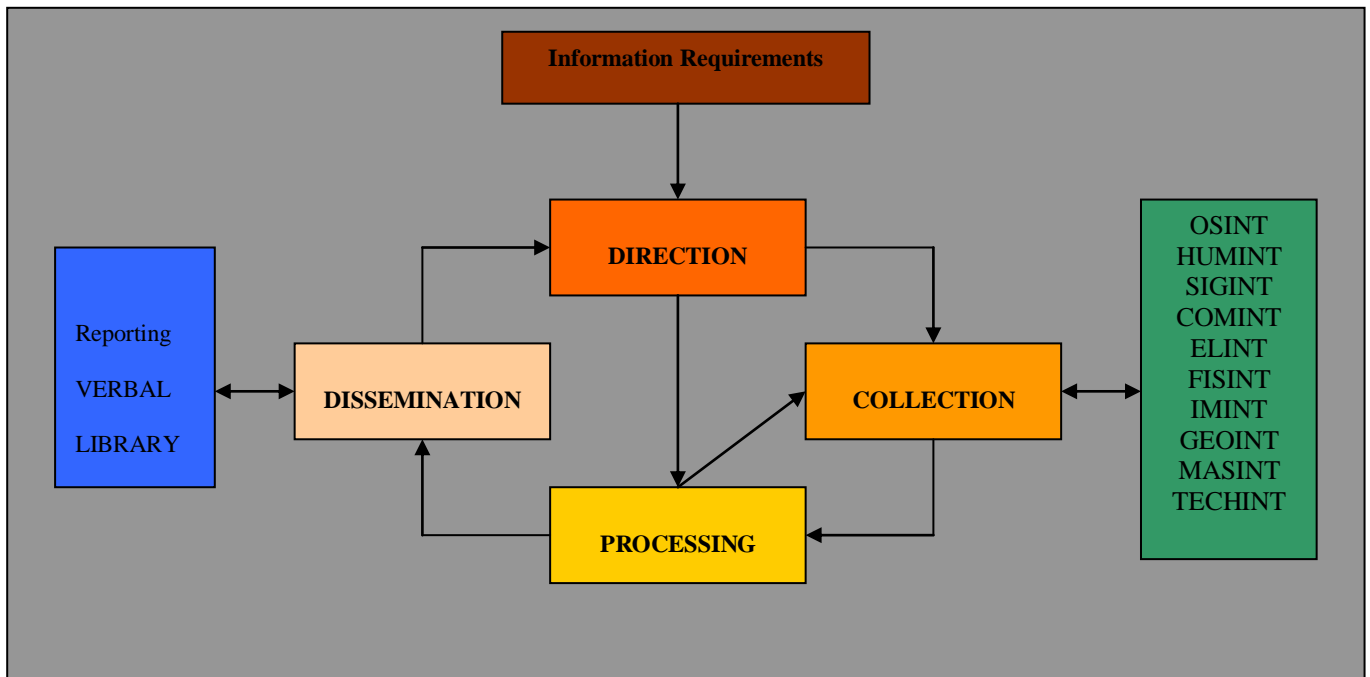


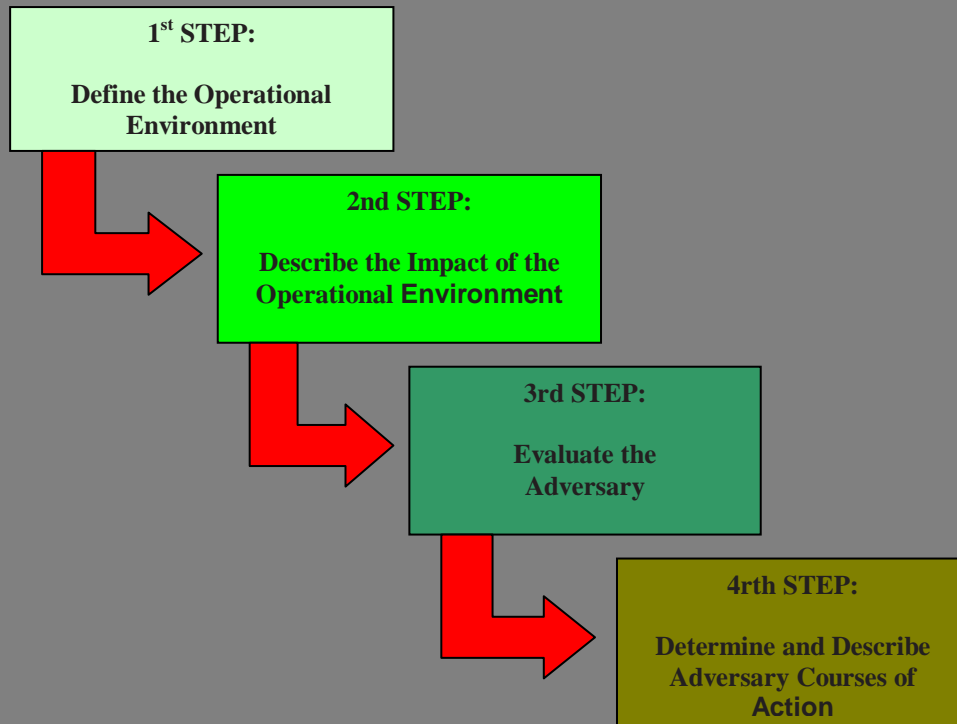
Diagram 4: Intelligence Assessment through The Intelligence Cycle.

The RFI may indicate in what format the requester prefers to consume the product. The RFI is reviewed by the Requirements Manager who will then direct the appropriate tasks to respond to the specific request. This will involve a review of existing material, the tasking of new analytical product or the collection of new information in order to perform an analysis. New information may be collected through one or more of the various collection disciplines, (as shown at the above diagram). The nature of the RFI and the urgency placed on it may indicate that some collection types are unsuitable due to the time taken to collect, or validate the information gathered. Intelligence gathering disciplines and the sources and methods used are often highly classified and compartmentalised with analysts requiring an appropriate high level of security clearance.

The process of taking known information, (about situations and entities), of importance according to the RFI, characterising what is known and then attempting to forecast future events is called “all source” assessment, analysis or processing. The analyst uses multiple sources to mutually corroborate, or exclude, the information collected and then reaching a conclusion along with a measure of confidence around that conclusion.

When the volume of available information is sufficient the analysis may be launched without the need of further information collection or gathering. After the analysis is completed is communicated to the applicant, and should be structured in different levels of classification to which different individuals, (with the appropriate classification level), will have access.

Intelligence Preparation of the Operational Environment



- A systematic methodology used by intelligence personnel.
- Used to analyze information about the physical environment and the adversary.
- A key tool for conducting joint intelligence analysis.
- Can be applied to the full range of military operations.
- Identifies most probable course of action and most dangerous course of action.

Table 4: Intelligence Preparation of the Operational Environment.

1.4.3.1 The Target Centric Assessment Approach.

If the assessment sub topic or subject is already known or clearly identifiable and actions or interventions memoranda are already exist the analyst can make use of The Target Centric Approach.

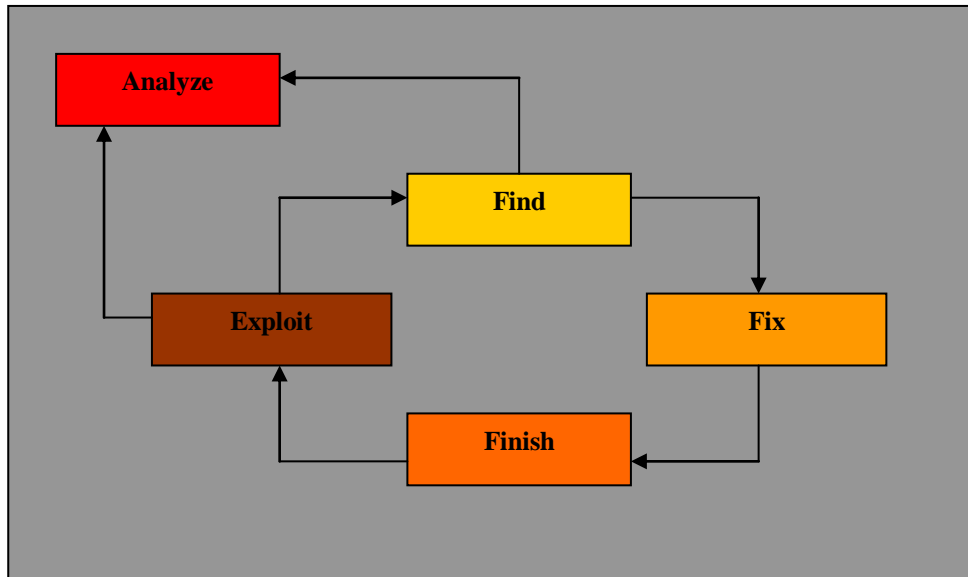


Diagram 5: The Target Centric Assessment Approach.

This approach is known as F3EA⁴⁸, is complementary to the intelligence cycle and focussed on the intervention itself. The matter to be investigated or the “target” is known and has already been identified, efforts focused on gathering (find) additional information. The necessary activities are designed to identify the points (fix), where intervention will have the most beneficial results.

When the decision for intervention is taken, all the measures must be designed in the appropriate way to ensure a high probability of success and reduce the ability of the respective target to react. During the final stage (finish) all the committed actions are performed as decided. Following the intervention, exploitation and analyze is carried out, which may lead to further refinement of the process for related subjects or targets. The output from the exploit-analyze stage will also be passed into other intelligence assessment activities. Completion of the operation followed by debriefing to identify any errors, omissions or gaps in the implementation, to improve the process and creating mnemonic actions to be applied in similar cases.

⁴⁸ F3EA: Find, Fix, Finish, Exploitation and Analyze. (Military example): An aggressive targeting model, features massed, persistent ISR cued to a powerful and decentralized all-source intelligence apparatus in order to *find* a target amidst civilian clutter and fix his exact location. This precision geolocation enables surgical finish operations that emphasize speed to catch a fleeting target. The emphasis on the finish was not only to remove a combatant from the battlefield, but also to take an opportunity to gain more information on the globalized and networked foe. Exploit-analyze is the main effort of F3EA because it provides insight into the enemy network and offers new lines of operations. Exploit-analyze starts the cycle over again by providing leads, or start points, into the network that could be observed and tracked using airborne ISR. A finishing force unified with airborne ISR and an exploit-analyze capability is able to be persistent, surgical, and rapid in operations against the insurgent’s network. Airborne ISR became the pacing item for operations, but it had to be cued by the meticulous work of a robust, allsource, and collaborative intelligence network.

1.4.4 Intelligence Disciplines.

There are seven basic Intelligence Disciplines, those are:

1. **Human Intelligence (HUMINT):** is the collection of foreign information by a trained HUMINT collector. It uses human sources and a variety of collection methods, both passively and actively, to collect information including multimedia on threat characteristics.
2. **Geospatial Intelligence (GEOINT):** is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information.
3. **Imagery Intelligence (IMINT):** is derived from the exploitation of imagery collected by visual photography, infrared sensors, lasers, multispectral sensors, and radar. These sensors produce images of objects optically, electronically, or digitally on film, electronic display devices, or other media.
4. **Measurement and Signature Intelligence (MASINT):** is technically derived intelligence that detects, locates tracks, identifies, or describes the specific characteristics of fixed and dynamic target objects and sources. It also includes the additional advanced processing and exploitation of data derived from IMINT and SIGINT collection. MASINT collection systems include but are not limited to radar, spectroradiometric, electro-optical, acoustic, radio frequency, nuclear detection, and seismic sensors. MASINT collection also includes techniques for collecting CBRN and other materiel samples.
5. **Open Source Intelligence (OSINT):** is produced from publicly available information collected, exploited, and disseminated in a timely manner to an appropriate audience for addressing a specific intelligence requirement.
6. **Signals Intelligence (SIGINT):** is produced by exploiting foreign communications systems and non communications emitters. SIGINT provides unique intelligence and analysis information in a timely manner. This discipline also comprises:

6.1 **Communications Intelligence (COMINT):** is a sub-category of signals intelligence that engages in dealing with messages or voice information derived from the interception of foreign communications. It should be noted that COMINT is commonly referred to as SIGINT, which can cause confusion when talking about the broader intelligence disciplines. The US Joint Chiefs of Staff defines it as "Technical information and intelligence derived from foreign communications by other than the intended recipients⁴⁹". COMINT, which is defined to be communications among people, will reveal some or all of the following:

- Who is transmitting,
- Where they are located, and, if the transmitter is moving, the report may give a plot of the signal against location,
- If known, the organizational function of the transmitter,
- The time and duration of transmission, and the schedule if it is a periodic transmission,

⁴⁹ US Defence Department (12 July 2007). "Joint Publication 1-02 Defence Department, Dictionary of Military and Associated Terms" (PDF). Retrieved 01-10-2007.

- The frequencies and other technical characteristics of their transmission,
- If the transmission is encrypted or not, and if it can be decrypted. If it is possible to intercept either an originally transmitted clear text or obtain it through cryptanalysis, the language of the communication and a translation (when needed),
- The addresses, if the signal is not a general broadcast and if addresses are retrievable from the message. These stations may also be COMINT (e.g., a confirmation of the message or a response message), ELINT (e.g., a navigation beacon being activated) or both. Rather than, or in addition to, an address or other identifier, there may be information on the location and signal characteristics of the responder.

6.2 **Electronic Intelligence (ELINT):** refers to intelligence-gathering by use of electronic sensors. Its primary focus lies on non-communications signals intelligence. The Joint Chiefs of Staff define it as “Technical and geolocation intelligence derived from foreign non communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources”⁵⁰. Signal identification is performed by analyzing the collected parameters of a specific signal, and either matching it to known criteria, or recording it as a possible new emitter. ELINT data are usually highly classified, and are protected as such.

The data gathered are typically pertinent to the electronics of an opponent's defense network, especially the electronic parts such as radars, surface-to-air missile systems, aircraft, etc. ELINT can be used to detect ships and aircraft by their radar and other electromagnetic radiation; commanders have to make choices between not using radar (EMCON), intermittently using it, or using it and expecting to avoid defences'. ELINT can be collected from ground stations near the opponent's territory, ships off their coast, aircraft near or in their airspace, or by satellite.

6.3 **Foreign Instrumentation Signals Intelligence (FISINT):** is a sub-category of SIGINT, monitoring primarily non-human communication. Foreign instrumentation signals include (but not limited to) telemetry (TELINT), tracking systems, and video data links. TELINT is an important part of national means of technical verification for arms control.

7. **Technical Intelligence (TECHINT):** is derived from the collection and analysis of threat and foreign military equipment and associated material for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages.

⁵⁰ US Defence Department (12 July 2007). “Joint Publication 1-02 Defence Department, Dictionary of Military and Associated Terms” (PDF). Retrieved 01-10-2007.

1.4.5 Scope of Intelligence⁵¹.

The following discussion draws on the work of Abram N. Shulsky's 2002 book, *Silent Warfare: Understanding the World of Intelligence*. The concept of intelligence applies not only to governments, but also too many other types of organizations. For example, business corporations treat intelligence as information designed to meet policy-making needs. Similarly, a political party or campaign performs intelligence-like activities in trying to figure out what the opposition is up to. A few of the most common applications of intelligence are:

- **Domestic Intelligence:** Intelligence collected from individuals or groups within the nation's borders is an extremely sensitive issue. This is largely because how a government defines such internal threats depends heavily on the type of government it is. For example, a single political party that has a monopoly of power is likely to regard any domestic political dissent as a security threat, and its intelligence service will focus a great deal of attention on detecting and thwarting that dissent. In the extreme case, a totalitarian government may regard all non members of the ruling party as actual or potential enemies. By contrast, the notion of a “loyal opposition”, as found in democratic systems, implies that the government's domestic political opponents do not pose a security threat and hence are not suitable targets of intelligence.
- **Law Enforcement:** This focuses on threats which are not primarily from a foreign government. Examples are narcotics trafficking or certain types of organized crime. These threats appear to fall within the ambit of law enforcement rather than of intelligence, but intelligence is often involved in the fight against them. Intelligence may be called upon for information about the foreign aspect of these activities, information that would otherwise be unavailable. Also, the law enforcement approach typically waits until a crime has been, (or is about to be), committed, and then attempts to solve that particular crime and arrest the perpetrators. This may not be an acceptable approach toward certain transnational threats. When dealing with entirely domestic organized crime groups, however, law enforcement agencies often use intelligence techniques. For example, with respect to domestic law enforcement, the Federal Bureau of Investigation (FBI) distinguishes between criminal intelligence investigations and ordinary criminal investigations. The dividing line between the law-enforcement and intelligence approaches is whether the focus is on punishment of a given criminal act or on struggle with an organization engaged in criminal activity.
- **Economics:** Intelligence can be used to enhance a nation's economy. Acquiring advanced technology was and is an important goal of Russian and Chinese intelligence. This activity saves both countries the great expense and difficulty of developing technology on their own, whether for military or civilian uses. In a market economy, however, it is much less clear which economic issues have national security dimensions that justify or require the involvement of intelligence agencies. In general, specific economic questions that has a direct impact on military or other foreign policy aspects of national security fall within the purview of intelligence agencies. For example, information concerning a county's access to strategic materials. The broader question is if intelligence should be used to advance the economic well-being of the nation. As Schulsky points out, private economic interests could probably put it to much greater use, but it is not clear that information gathered clandestinely at government expense could be distributed equitably to individuals or corporations to

⁵¹ www.psu.edu - Lesson 7: The Intelligence Process.

further private interests (Shulsky, 2002, p. 6).

- **Other Areas:** Intelligence has been applied to “non traditional” areas such as environmental issues. Environmental security seems to be one of the major non traditional area subjects. It integrates the fields of science, diplomacy, law, finance and education to provide policy-makers with a methodology to tackle environmental security risks in time. The goal is to ensure a scientifically sound response to complex human-environment events such as climate change, West Nile Virus, and Lyme disease. According to Shulsky, “While the argument is made that environmental problems can affect national security, the main motivation seems to be that technical intelligence collection systems developed for other purposes can help track environmental changes over time and across large expanses of territory, and that they can do so at small additional cost” (Shulsky, 2002, p. 7).

1.4.6 The Elements of Intelligence.

According to the type of activity involved, intelligence can be divided into four parts, often referred to as the “elements of intelligence”:

Collection: refers to the gathering of raw data, through espionage, technical means, exploitation of “open sources” (for instance, publications, and radio and television broadcasts), or in any other manner. National Technical Means (NTM) is a euphemism for intelligence collection by reconnaissance satellites. It is normally used in reference to the activities of the United States National Reconnaissance Office (NRO). It may involve imagery intelligence, signals intelligence, electronic intelligence, or other forms, such as space-based radar. There are seven basic intelligence collection disciplines as described above.

Analysis: refers to the process of transforming the pieces of information into something that is usable by policy makers, company managers and military commanders. The result, or “intelligence product”, can take the form of memorandums, elaborate formal reports, briefings, maps, databases, or any other means of presenting information. We use the term “technical analysis” here to refer to analytical methods that transform highly specialized data, totally or virtually incomprehensible to everyone but the specialist, into data that other intelligence analysts can use.

Covert Action: Perhaps the most interesting and sinister field in Intelligence is Covert Action (also referred to as Clandestine Operations, Black Ops, and Black Operations). Some do not consider Covert Action as being part of the traditional Intelligence mission, and they believe that it should be treated independently and even organized within a separate organization. Others believe that, because it often interrelates with Intelligence Operations and Counterintelligence Operations, it should continue to remain within the same ruling organization or apparatus.

There are many types of Covert Action operations, not all of them violent. For example, if a government wishes to influence the politics of another country’s government, the government may secretly fund an opposition party in that country in order to influence that country’s elections. Another method is to employ foreign newspaper reporters to write articles that give their version of events, or publish articles or news stories created by the Intelligence organization for propaganda purposes to be planted in the newspaper or media service. A slant can then be given to influence public perceptions. For example, mercenaries can be referred to as “contractors”, thus making people believe that casualties among the mercenaries are innocent civilian construction workers who were unjustly victimized. The main thing about Covert Action is that it must be deniable. There is a term called “plausible deniability”. When a government authorizes a covert action operation, the operation must be

done in such a way that the government can claim that it knows nothing about it; in other words, the operation must not be attributable to the government that authorized it.

Covert Action operations are often Disinformation Operations, which are conducted in such a way as to discredit the opposition or the enemy. This is done, for example, by doing a violent action, such as a bombing, but making it look like the forces of another country or group did it. Such operations are sometimes called False-Flag Operations, meaning that the operation is conducted to make it look like it was done by people serving under another flag, preferably the enemy's flag. If the operation succeeds as designed, people will blame the action on the wrong party (the enemy). Thus, public opinion will be won over to the side that actually did the killing. Such false-flag, covert action operations are often referred to as Dirty Tricks⁵².

Counterintelligence: refers to efforts made by intelligence organizations to prevent hostile or enemy intelligence organizations from successfully gathering and collecting intelligence against them. National intelligence programs, and, by extension the overall defensive system of a nation, is vulnerable to attack. It is the role of intelligence cycle security to protect the process embodied in the intelligence cycle, and that which it defends.

Many governments organize counterintelligence agencies separate and distinct from their intelligence collection services for specialized purposes. In most countries the counterintelligence mission is spread over multiple organizations, though one usually predominates. There is usually a domestic counterintelligence service, perhaps part of a larger law enforcement organization such as the Federal Bureau of Investigation in the United States.

The United Kingdom has the separate Security Service, also known as MI5, which does not have direct police powers but works closely with law enforcement called the Special Branch that can carry out arrests, do searches with a warrant, etc.

The Russian Federation's major domestic security organization is the FSB, which principally came from the Second Chief Directorate of the USSR KGB and Third Chief Directorate of the KGB USSR.

Canada separates the functions of general defensive counterintelligence, security intelligence (the intelligence preparation necessary to conduct offensive counterintelligence), law enforcement intelligence, and offensive counterintelligence.

Military organizations have their own counterintelligence forces, capable of conducting protective operations both at home and when deployed abroad. Depending on the country, there can be various mixtures of civilian and military operators - contractors in foreign operations. For example, while offensive counterintelligence is a mission of the US CIA's National Clandestine Service, defensive counterintelligence is a mission of the U.S. Diplomatic Security Service (DSS), Department of State, who work on protective security for personnel and information processed abroad at US Embassies and Consulates⁵³.

⁵² <http://www.informationclearinghouse.info/article10356.htm>

⁵³ "Counterintelligence Investigations". Retrieved 08-05-2008, <http://en.wikipedia.org/wiki/Counterintelligence>.

1.4.7 Characteristics of Effective Intelligence.

The effectiveness of the intelligence is measured against the relevant information quality criteria:

- **□Accuracy:** Intelligence must give to decision makers, military or law enforcement commanders etc, an accurate, balanced, complete, and objective picture of one specific subject, matter or target. To the extent possible, intelligence should accurately identify threat intentions, capabilities, limitations, and dispositions. It should be derived from multiple sources and disciplines to minimize the possibility of deception or misinterpretation. Alternative or contradictory assessments should be presented, when necessary, to ensure balance and bias-free intelligence.
- **Timeliness:** Intelligence must be provided early to support decision making, policy or operations, and prevent surprise from competitors (private sector), or enemy action (public sector). It must flow continuously to the manager of a company, or to a military commander, before, during, and after an operation. Intelligence organizations, databases, and products must be available to develop estimates, make decisions, and plan operations.
- **Usability:** Intelligence must be presented in a form that is easily understood or displayed in an appropriate format that immediately conveys the meaning to the consumer.
- **Completeness:** Intelligence briefings and products must convey all the necessary components to be as complete as possible.
- **Precision:** Intelligence briefings and products must provide only the required level of detail and complexity to answer the requirements.
- **Reliability:** Intelligence must be evaluated to determine the extent to which the information that had been collected and is being used in intelligence briefings and products is trustworthy, and undistorted. Any concerns with these must be stated up front.

Effective intelligence must also meet three additional criteria:

- **Relevant:** Intelligence must support the manager's (or commander's), specific needs and preferences (or concept of operations).
- **□Predictive:** Intelligence should inform the manager or the commander about what the competitor or a threat can do (threat capabilities), and is most likely to do. The intelligence staff should anticipate the manager's or the commander's intelligence needs.
- **□Tailored:** Intelligence must be presented - based on the needs of the manager's – commanders and staff, in a specific format that is clear and concise so they can understand it, believe it, and act on it. It should support and satisfy the manager's - commander's and staff priorities.

1.4.8 Causes of Intelligence Failure.

In this section, we are going to present the possible causes of intelligence failure that can reside in an intelligence organization. Those causes are:

- **Surprise Attack:** The most dramatic intelligence failure occurs when an attack happens without warning, one of the most recent example is the 11 September events. Those events proved especially shocking, both because they were so destructive, and because they were so unexpected. Yet, both the fact that the attack occurred and even the form it took should not have taken the United States Intelligence Services completely unaware. The familiarity of terrorist methods (*modus operandi*), the increasing and repeated attacks against U.S. facilities all over the world, combined with indications that the continental United States was one of the top terrorist target should have alerted the US Intelligence Services that the USA were in peril of a significant attack. The 11 September is one of the most typical examples of the consequences that would occur from an intelligence warning breakdown.
- **Rapid and unexpected political changes or disturbances:** This can have dramatic effects on a country's foreign policy. One of the most characteristic examples of such cases was the events that took place in Iran in 1978. The Iranian Revolution (also known as the Islamic Revolution), refers to events which led to the overthrow of the Pahlavi dynasty (under Shah Mohammad Reza Pahlavi), who was supported and installed by the United States and United Kingdom, and its replacement with an Islamic republic under Ayatollah Ruhollah Khomeini, who was the leader of the revolution.

Demonstrations against the Shah commenced in October 1977, developing into a campaign of civil resistance that was partly secular and partly religious⁵⁴ and intensified in January 1978⁵⁵. Between August and December 1978 strikes and demonstrations paralyzed the country. The Shah left Iran for exile on January 16, 1979 as the last Persian monarch and in the resulting power vacuum two weeks later Ayatollah Khomeini returned to Tehran to a greeting by several million Iranians⁵⁶. The royal reign collapsed shortly after (11 February), when guerrillas and rebel troops overwhelmed troops loyal to the Shah in armed street fighting⁵⁷. Iran voted by national referendum to become an Islamic Republic on April 1, 1979⁵⁸, and to approve a new democratic-theocratic hybrid constitution whereby Khomeini became Supreme Leader of the country, in December 1979.

The revolution was unusual for the surprise it created throughout the world⁵⁹ it lacked many of the customary causes of revolution (defeat at war, financial crisis, peasant rebellion, or disgruntled military)⁶⁰, produced profound change at great speed⁶¹, was massively popular⁶², and replaced a westernising monarchy with a theocracy based on Guardianship of the Islamic Jurists (or *velayat-e faqih*). Its outcome - an Islamic Republic "under the guidance of an extraordinary religious scholar from Qom" - was, as one scholar put it, "clearly an occurrence that had to be explained⁶³".

⁵⁴ Ervand Abrahamian, "Mass Protests in the Islamic Revolution", 1977–1979, in Adam Roberts and Timothy Garton Ash (eds.), *Civil Resistance and Power Politics: The Experience of Non-violent Action from Gandhi to the Present*. Oxford & New York: Oxford University Press (2009), pp. 162–78.

⁵⁵ http://en.wikipedia.org/wiki/Iranian_Revolution.

⁵⁶ Ruhollah Khomeini, *Encyclopedia Britannica*, 1979: Exiled Ayatollah Khomeini returns to Iran/ bbc.co.uk

⁵⁷ Graham, Iran (1980) p. 228, Kurzman, Charles, "The Unthinkable Revolution in Iran", Harvard University Press, 2004, p.111.

⁵⁸ Iran Islamic Republic, *Encyclopædia Britannica*.

⁵⁹ Amuzegar Jahangir, "The Dynamics of the Iranian Revolution", SUNY Press, 1991, p.4, 9–12.

⁶⁰ Arjomand, "Turban", 1988, p. 191.

⁶¹ Amuzegar Jahangir, "The Dynamics of the Iranian Revolution", SUNY Press, p.10.

⁶² Kurzman, "The Unthinkable Revolution in Iran", 2004, p.121.

⁶³ Benard, "The Government of God", 1984, p. 18.

The American underestimation in 1978 of the political troubles of the shah of Iran and of the depth of the opposition to his rule is one of the best-known examples of this type of intelligence failure.

Aside from cases like the above ones or cases in which relevant information cannot be obtained at all, intelligence failure refers to a disorder of the analytical process that causes data to be ignored, misinterpreted or misunderstood. In addition, some peculiarities of the intelligence analysis process might cause a variety of different types of errors. Because intelligence analysis is an intellectual activity it is vulnerable to certain pathologies that can be addressed in institutional or bureaucratic terms. At the following section we are going to address some of the causes that can lead to intelligence failure, first at institutional failures and then at those related directly to the intellectual content of the intelligence procedures and disciplines.

- **Subordination of Intelligence to Policy:** This case refers to the possibility that intelligence analysis and results - products will be made in order to produce the results superiors wish or like to hear, instead of what the evidence indicates. This is perhaps the most common source of error or bias in intelligence analysis.
- **Unavailability of Information When and Where Needed:** Due to the size of the departments, agencies and organizations involved in collecting and analyzing intelligence, a possible source of problems or malfunctions might be the unavailability and accessibility of processed and ready to use information that already exist to those who need it and when they need it.
- **Received Opinion:** The success of the intellectual effort can be eroded if the respective analyst makes use of so-called “conventional wisdom”, to assume (without research), as valid and true information and opinions simply treated as such by society.
- **Mirror-Imaging:** The two problems discussed above apply mainly to information analysis that carried out in a purely bureaucratic environment. There is another possible source of error in the information analysis process, which is not related to the environment in which the analysis is conducted. It can be defined as “mirror imaging”, which can be described as the judgment of unfamiliar statements based on known risks. In a situation like this the analyst tries to predict or assess the reaction of a foreign government not based on facts but on how he would react if he was in a similar position. He (or she), decides and estimates using an analogical pattern of what his (or her), actions would be in a similar situation.

1.4.9 Finished Intelligence⁶⁴.

The product of the information analysis is not transferred unchanged to the client (a manager, a military commander, a politician civilian, etc), on the contrary, it must be tailored to the requirements and scope of the individual who will receive it. Developing finished and tailored intelligence involves analytical techniques similar to those used by the social sciences. Thus formed the following types of intelligence forms, (depending on the type of informational analysis and the products that will be produced):

A. Public Sector.

1. **Military Intelligence:** Military intelligence is concerned with the gathering of information about foreign military forces (both allied and enemy), so that we can properly prepare our military forces. The basic military intelligence includes a presentation of information about hostile military forces, information such as the total number of personnel (per branch), the number and types of weapons systems and weaponry means (by sector), organizational structure (by branch-sector) and generally similar data. The next step is trying to anticipate and assess the tactical and strategic techniques and methods that might be followed by the hostile military forces in case of hostilities, in order to develop the appropriate countermeasures to successfully deal with tactical and strategic choices made by the opponent.

1.1 **Military “Scientific Intelligence”:** Collecting and obtaining information about new weaponry systems that the enemy is or had already developed is an important intelligence objective. It is very important for us to get enough detailed information on how a new enemy weapon system is working – operating in order to be able to develop the appropriate response measures and countermeasures. The subcomponents are:

1.1.1 Weapons and weapon systems.

1.1.2 Missile and space program.

1.1.3 Nuclear energy and weapons technology.

1.1.4 NBC developments.

1.2 **Military Geographic Intelligence:** studies all geographic factors (physical and cultural).

1.3 **Military Economic Intelligence:** studies the economic strengths and weaknesses of a country (friendly or hostile). Its subcomponents are:

1.3.1 **Economic warfare:** Information on the diplomatic or financial steps which a country might take to induce neutral countries to cease trading with its enemies.

1.3.2 **Economic vulnerabilities:** The degree to which a country's military power would be tampered by the loss of materials or facilities.

1.3.3 **Manufacturing:** Information on manufacturing processes, facilities, logistics, and so forth.

⁶⁴ Law Enforcement Intelligence Guide,
<http://overwatchreport.com/upload/2038/MANUAL%20of%20INTELLIGENCE.pdf>

1.3.4 **Source of economic capability:** Any means a country has to sustain its economy.

2. **Law Enforcement Intelligence:** Some illegal activities occurring on our soil and abroad could affect our security interests, those primarily are:

- International Threats from Terrorism,
- Drug Smuggling and Trafficking,
- Women Trafficking,
- Illegal Migration, and
- Proliferation of Weapons of Mass Destruction, (WMD).

The law enforcement intelligence function has essentially two broad purposes:

1. Prevention involves gaining or developing information related to threats of terrorism or crime and using it to apprehend offenders, harden targets, and use strategies that will eliminate or mitigate the threat. Two generally accepted types of intelligence are specifically oriented toward prevention:

1.1 **Tactical Intelligence:** Actionable intelligence about imminent or near-term threats that is disseminated to the line functions of a law enforcement agency for purposes of developing and implementing preventive, and/or mitigating, response plans and activities.

1.2 **Operational Intelligence:** Actionable intelligence about long-term threats that is used to develop and implement preventive responses. Most commonly, operational intelligence is used for long-term inquiries into suspected criminal enterprises and complex multijurisdictional criminality.

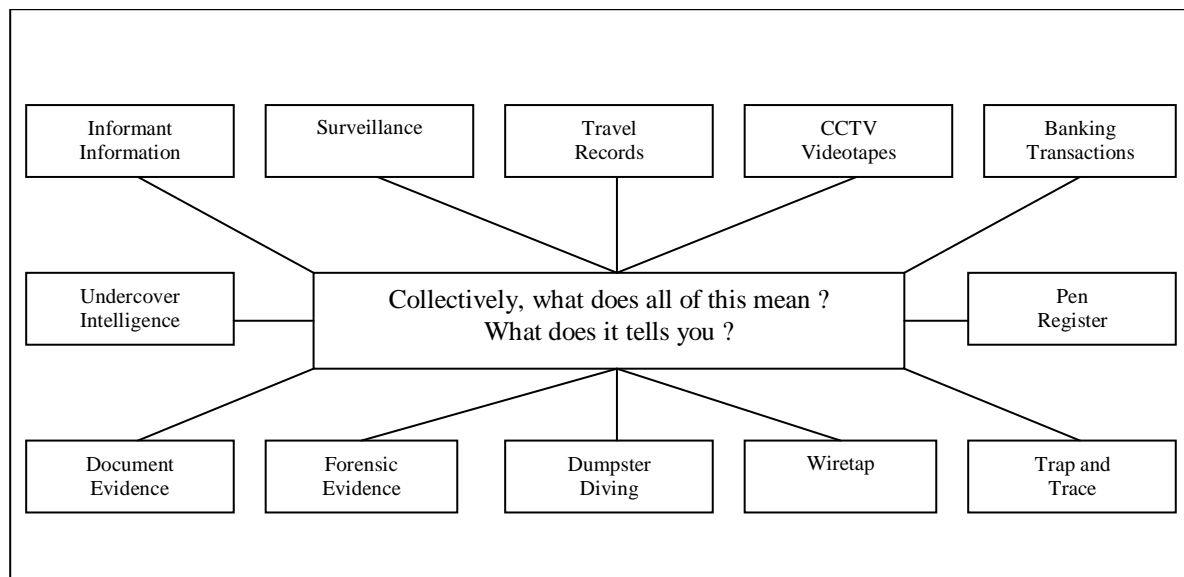


Table 5: Diverse Information Collected for Intelligence Analysis⁶⁵.

⁶⁵ Law Enforcement Intelligence Guide.

2. Planning and resource allocation provides information to decision-makers about the changing nature of threats, the characteristics and methodologies of threats, and emerging threat idiosyncrasies for the purpose of developing response strategies and reallocating resources, as necessary, to accomplish effective prevention.

2.1 Strategic Law Enforcement Intelligence: It provides an assessment of the changing threat picture to the management of a law enforcement agency for purposes of developing plans and allocating resources to meet the demands of emerging threats.

Information	Intelligence
<p>Criminal history and driving records.</p> <p>Offense reporting records.</p> <p>Statements by informants, witnesses, and suspects.</p> <p>Registration information for motor vehicles, watercraft, and aircraft.</p> <p>Licensing details about vehicle operators and professional licenses of all forms.</p> <p>Observations of behaviors and incidents by investigators, surveillance teams, or citizens.</p> <p>Details about banking, investments, credit reports, and other financial matters</p> <p>Descriptions of travel including the traveler(s) names, itinerary, methods of travel, date, time, locations, etc.</p> <p>Statements of ideologies, beliefs, and practices.</p>	<ol style="list-style-type: none"> 1. A report by an analyst that draws conclusions about a person's criminal liability based on an integrated analysis of diverse information collected by investigators and/or researchers. 2. An analysis of crime or terrorism trends with conclusions drawn about characteristics of offenders, probable future crime, and optional methods for preventing future crime/terrorism. 3. A forecast drawn about potential victimization of crime or terrorism based on an assessment of limited information when an analysts uses past experience as context for the conclusion. 4. An estimate of a person's income from a criminal enterprise based on a market and trafficking analysis of illegal commodities.

Table 6: Comparative Illustrations of Information and Intelligence⁶⁶.

⁶⁶ Law Enforcement Intelligence Guide.

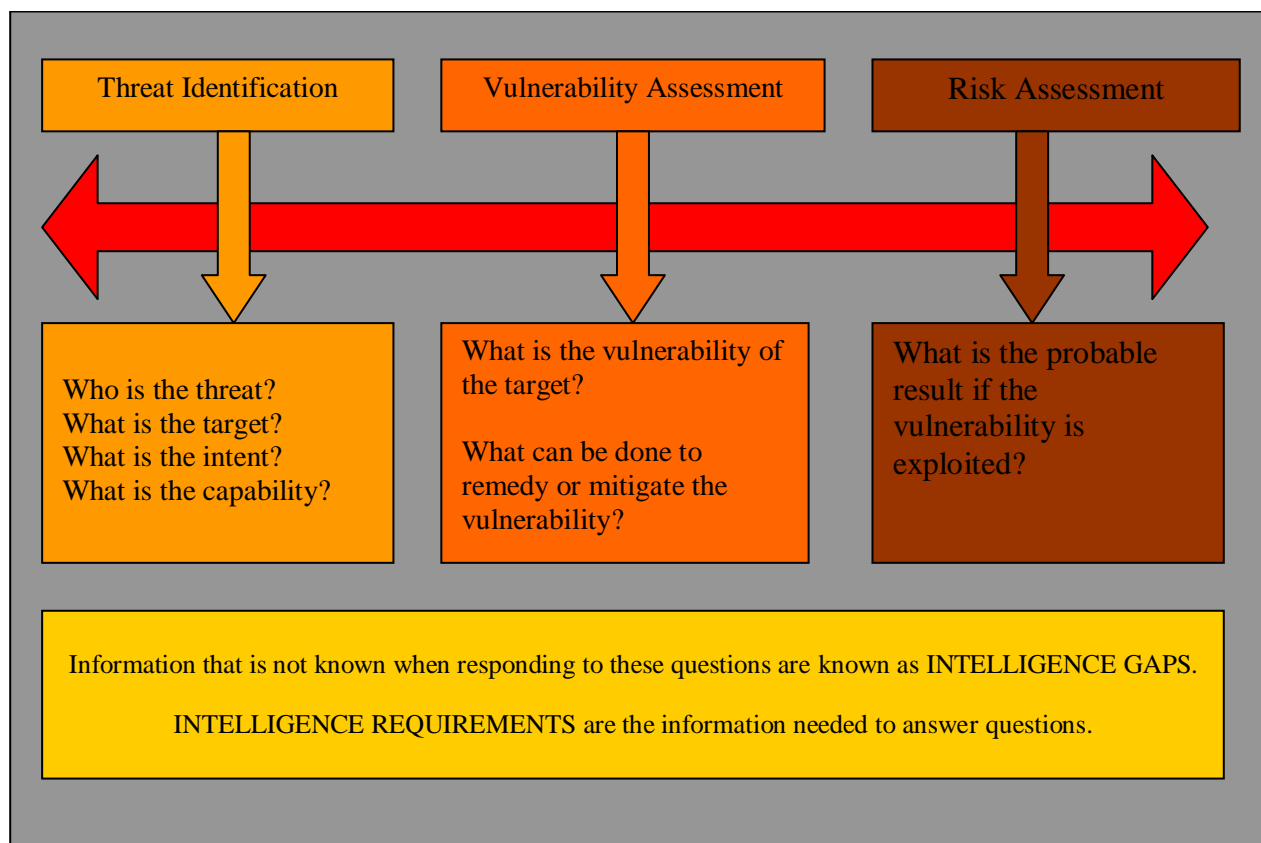


Table 7: Threat Assessment Components for Planning and Direction⁶⁷.

3. **Political Intelligence:** Political intelligence consists of information concerning the political processes, ideas, and intentions of foreign countries, factions, and leaders. The analysis that produces this intelligence is similar to all academic and journalistic research on both international and domestic politics. Its subcomponents are:

3.1 Government structure - organization of departments and ministries.

3.2 National policies - government actions and decisions.

3.3 Political dynamics - government views and reactions to events.

3.4 Propaganda - information and disinformation programs.

3.5 Policy and intelligence services - organizations and functions.

3.6 Subversion - subversive acts sponsored by the government.

⁶⁷ Law Enforcement Intelligence Guide.

B. Private Sector.

In the private sector area, intelligence can find application in many fields, generally speaking, intelligence can help economic policy makers, the opinion leaders, investors, etc. to take the right decisions at critical and specific issues that concern them. Some of the fields are describing below:

1. **Commercial intelligence:** Related to the capabilities and intentions of one's commercial rivals and competitors, often to the acquisition of confidential or proprietary information about their strategies, e.g., bid information, processes, finances or markets.
2. **Economic intelligence:** Studies the economic strengths and weaknesses of a country or a competitor.
3. **Sociological intelligence:** deals with people, customs, behaviors, and institutions.
4. **Transportation and telecommunications intelligence:** studies the role of transportation and telecommunications systems in the new era of globalization.
5. **Biographic intelligence:** is the study of individuals of actual or potential importance through knowledge of their personalities and backgrounds. This component can be divided into a number of subcomponents:
 - 5.1 Educational and occupational history - including civilian and military backgrounds of individuals.
 - 5.2 Individual accomplishment - notable accomplishments of an individual in professional or private life.
 - 5.3 Idiosyncrasies and habits - including mannerisms and unusual life styles.
 - 5.4 Position, influence, and potential present and future positions of power or influence.
 - 5.5 Attitudes and hobbies – significant interests that may affect the individual's accessibility.
6. **Scientific and technical intelligence:** Studies the country's potential and capability to support objectives through development of new processes, equipment, weapons systems, and so forth. The subcomponents are:
 - 6.1 Basic applied science.
 - 6.2 Research and development systems.
 - 6.3 Space program.

Finally, information gathered as strategic intelligence may be categorized into eight components. An easy way to remember these components is through the use of the acronym BEST MAPS⁶⁸:

⁶⁸ According to the US Field Manual 34-52 which details the Components of Strategic Intelligence.

B: Biographic intelligence.

E: Economic intelligence.

S: Sociological intelligence.

T: Transportation and telecommunications intelligence.

M: Military geographical intelligence.

A: Armed forces intelligence.

P: Political intelligence.

S: Scientific and technical intelligence.

Each of these components can further be divided into a number of subcomponents. This approach is merely a mean to enhance familiarization with the types of information included in strategic intelligence. We will not expand further as most of these components have already been analyzed and presented above paragraphs.

LEVELS OF INTELLIGENCE

Strategic:

Senior Military and Civilian Leaders, Combatant Commanders, Executive Managers.

- Assist in developing national strategy and policy (public sector), company strategy and policy (private sector).
- Monitor the international situation, both public and private sector.
- Assist in developing military plans (public sector), and company plans(private sector).
- Assist in determining major weapon systems and force structure requirements (public sector).
- Support the conduct of strategic operations, both public and private sector.

Operational:

Combatant and Subordinate Joint Force Commanders and Component Commanders, Managers and law level managers.

- Focus on military capabilities and intentions of enemies and adversaries (public sector), Focus on capabilities and intentions of competitors (private sector).
- Monitor events in the Joint Force Commander's area of interest.
- Support the planning and conduct of joint campaigns (public sector), support the planning and the execution of a companies "master plan".
- Identify adversary centers of gravity both public and private sector.

Tactical:

Commanders, and managers.

Support planning and conducting battles and engagements (public sector), support planning and conducting with the competitors (private sector).

Provide commanders with information on imminent threats to their forces (public sector), provide managers with information on imminent threats to their companies interests (private sector).

Provide commanders and managers with obstacle intelligence.

Table 8: Levels of Intelligence.

CHAPTER 2.

Intelligence Disciplines.

In this chapter we will proceed to the detailed presentation of Intelligence Disciplines, so that the reader is able to understand better the advantages and disadvantages of each Intelligence Discipline.

2.1 Human Intelligence (HUMINT).

Human Intelligence (HUMINT), is intelligence gathered by means of interpersonal contact, NATO defines HUMINT as:

"A category of intelligence derived from information collected and provided by human sources⁶⁹."

Another definition of HUMINT is the one from US Field Manual 2-0, which is the following :

“Human intelligence is the collection (by a trained human intelligence collector), of foreign Information, from people and multimedia, in order to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities”.

Human intelligence operations are focused on identifying the opportunities for Empowerment hostile power, the characteristics of this threat, the vulnerabilities, and the possible intentions of Empowerment that enemy force, and any other types of threats. Human intelligence collection activities and operations include:

- screening,
- interrogation,
- debriefing,
- liaison, and
- human source operations.

Typical HUMINT activities consist of interrogations and conversations with persons having access to information. Evaluation of HUMINT is essential, because many (of the wide variety), of sources are considered doubtful about their reliability. A standardized system is used to rate the reliability of sources and the accuracy of the information that they provide, an information might be classified as true once it is confirmed by a number of sources.

The way in which HUMINT operations are conducted is dictated by both official protocol and the nature of the information source. Within the context of the U.S. Military, most HUMINT activities does not involve clandestine activities. Both counter intelligence and HUMINT do include clandestine HUMINT and clandestine HUMINT operational techniques.

Sources may be neutral, friendly, or hostile, and may or may not be “witting” of their involvement in the collection of information. “Witting” is a term of the intelligence art which indicates that one is not only aware of a fact or piece of information, but also aware of its connection to intelligence activities. Some examples of HUMINT sources are the following, (but are not limited to):

⁶⁹ AAP-6 (2004) - NATO Glossary of terms and definitions.

- Advisors working with host nation forces or populations,
- Diplomatic reporting by accredited diplomats (e.g., military attaches),
- Espionage clandestine reporting, access agents, couriers, cutouts,
- Military attaches,
- Non-governmental organizations (NGOs),
- Prisoners of war (POWs) or detainees,
- Refugees,
- Routine patrolling (military police, patrols, etc.),
- Special reconnaissance.

HUMINT is both a source of positive intelligence and information of strong counterintelligence value. Interviews should balance any known information requirements of both intelligence collection guidance and counterintelligence requirements.

Once the type of operation has been determined, leaders use the operations process—plan, prepare, execute, and assess—to conduct the operation. The following paragraphs briefly discuss the different types of HUMINT operations.

2.1.2 Human Intelligence Collection Methodologies.

Every Human intelligence questioning session, regardless of the methodology used or the type of operations consists of five phases. Those five phases are:

- Planning and preparation.
- Approach.
- Questioning.
- Termination.
- Reporting.

The phases are generally sequential, however reporting may occur at any point within the process when critical information is obtained and the approach techniques used will be reinforced as required through the questioning and termination phases.

The Human intelligence collection methodologies include five general categories (as we already said):

1. Screening Operations: Screening is the process of evaluating and selecting human sources and documents for the prioritized collection of information based on the collection requirements and mission of the unit conducting the screening or its higher headquarters. Screening categorizes and prioritizes sources based on the probability of a particular source having priority information and the level of cooperation of the source. Screening is also used to determine if a source matches certain criteria that indicate that the source should be referred to another agency. Screening is conducted at all echelons of command and in all operational environments.

There are two general categories of screening:

- Human source screening and
- Document and Media screening.

Media is screened for content, which answers priority intelligence requirements or other information of intelligence interest. Screening operations also help determine which intelligence discipline or agency could best conduct the exploitation of a given source. Screening operations include, (but are not limited to):

- Tactical screening to support combat or contingency operations,
- Checkpoint screening (mobile or static) of local populations as they transit through and within the area of operations or to screen large numbers of individuals, such as refugees or displaced persons as they enter the area of operations,
- Local population screening of personnel within their own neighbourhoods,
- Collection facility screening conducted as a normal part of HUMINT collection operations at collection facilities, such as theater interrogation and debriefing facilities and refugee camps,
- Local employee screening to determine possible security risks or identify sources which can provide information in response to the commander's critical information requirements.

2. Interrogation Operations: Interrogation is the systematic effort to procure information in order to answer specific collection requirements by direct and indirect questioning techniques of a person who is in the custody of the forces conducting the questioning. Interrogation sources range from totally cooperative to highly antagonistic. Interrogations may be conducted at all echelons in all operational environments. Detainee interrogation operations could be conducted at detention facilities, multinational-operated facilities, or other agency-operated collection facilities are more robust and require greater planning, but have greater logistic support. Interrogation operations are specific operations normally conducted at detainee collection facilities directed at the wide-scale collection of information from detainees using interrogation techniques. Although field interrogations are conducted at all echelons and during all operations with detainees, detention facilities where interrogation operations occur are normally located only at theatre or joint task force level.

3. Debriefing Operations: Debriefing is the systematic questioning of cooperating human sources to satisfy intelligence requirements consistent with applicable law. The source is usually not in custody and is usually willing to cooperate. Debriefing may be conducted at all echelons and in all operational environments. The primary categories of sources for debriefing are refugees, displaced persons, local civilians, and friendly forces.

3.1 Friendly Force Debriefing Operations: Every member of the friendly force is a potential source for HUMINT collection. Friendly force personnel frequently have contact with the threat, civilian population, or the environment. Although many individuals report their information in the form of combat information, many do not report the information, do not realize its significance, or do not know how to report key information. Frequently systematic questioning by a trained HUMINT collector will identify key information that can contribute to the intelligence picture and help an individual recall details. It also helps to place this information into a systematic format for the analyst to use.

4. HUMINT collection in Military Source Operations (MSO): HUMINT collection in MSO are directed toward the establishment of human sources who have agreed to meet and cooperate with HUMINT collectors in order to provide information. Within an Army, MSO is conducted by trained personnel under the direction of military commanders. The entire range of HUMINT collection operations can be employed. MSO sources include one-time contacts, continuous contacts, and formal contacts from debriefings, liaison, and contact operations. MSO consists of collection activities that use human sources to identify attitude, intentions, composition, strength, dispositions, tactics, equipment, target development, personnel, and capabilities of those elements that pose a potential or actual threat to a country or multinational forces. MSO is also employed to develop local source or informant networks providing early warning of imminent danger to a country and multinational forces and contribute to mission planning.

Formal contacts are individuals who have agreed to meet and cooperate with HUMINT collectors to provide information. HUMINT collectors who have met with a particular continuous contact three or more times should consider assessing the contact for use as a formal contact. Formal contacts can be tasked, trained, or paid. Formal contacts are employed to develop HUMINT sources which can provide early warning of imminent danger to a country and multinational forces and contribute to mission planning.

HUMINT collection teams (HCTs) must be able to travel in order to meet sources and be trained and able to remain at a “meeting location or point” long enough to conduct their rendezvous or contact. This requirement to remain in one location for several hours or days means that HCTs require dedicated security. Placing an HCT with a combat patrol for movement will not provide them with the support they need for stationary operations, since combat patrols need to keep on the move.

5. Liaison Operations: Liaison with local military, government, or civilian agency officials provides an opportunity to collect information required by the commander. The HUMINT collector meets with these officials to conduct liaison, coordinate certain operations, collect information, and obtain leads to potential sources of information. Elicitation is the primary technique used with liaison contacts, although in many cases there is a more formal exchange of information. Information obtained by these elements through liaison tends to reflect the official positions of their superiors and may not be entirely accurate or complete.

Cooperation level	Cooperation code	Knowledge Ability Level	Knowledge Ability Code
Responds to direct questions	1	Very likely to have pertinent information	A
Responds hesitantly	2	May have pertinent information	B
Does not respond	3	Unlikely to have pertinent information	C

Table 9: System of Prioritizing Interview Subjects⁷⁰.

⁷⁰ http://en.wikipedia.org/wiki/Human_Intelligence (intelligence collection).

2.1.3 Clandestine Human Intelligence⁷¹.

Clandestine Human Intelligence includes a wide range of Espionage sources. This includes the classic spy, (which by “professionals” is called asset or agent), who collects intelligence, but also couriers and other personnel, who handle their secure communications. Other support personnel include access agents, (who may arrange the contact between the potential spy), and the case officer who recruits them. In some cases, the recruiter and the continuing supervision of the agent may be different people. Large espionage networks may be composed of multiple spy levels, support personnel, and supervisors. Espionage networks are usually organized on a cell system, where each clandestine operator knows the people in his own cell, perhaps the external case officer, and an emergency method, (not necessarily a person), to contact higher levels if the case officer or cell leader is captured, but has no knowledge of people in other cells.

Espionage involves a human being obtaining, (i.e., using human intelligence methods), information that is considered secret or confidential without the permission of the holder of the information. Espionage is inherently clandestine, and the legitimate holder of the information may change plans or take other countermeasures once it is known that the information is in unauthorized hands.

Human intelligence is in a constant battle with counterintelligence, and the relationship can become very blurry, as one side tries to “turn” agents of the other into reporting to the other side. Recruiters can run false flag operations, where a citizen of country A believes they are providing intelligence to country B, when they are actually providing it to country C.

Unlike other forms of intelligence collection disciplines, espionage usually involves accessing the place where the desired information is stored, or accessing - approaching the people who know - obtain the information and will divulge it through some kind of subterfuge. There are exceptions to physical meetings, (such as the Oslo Report, or the insistence of Robert Hanssen in never meeting the people to whom he was selling information).

In this section we are not going to cover military units that penetrate deep between enemy lines to conduct special reconnaissance. Such military units can be on the border of the line according to international law, which defines them as spies if they conduct information in civilian clothes. In some circumstances, the uniformed personnel might support the actual agents, providing communications, transportation, financial, or security support. Military or not military units, (uniformed or not), might also conduct what is known as “covert operations”, such as raids, sabotage, assassinations, propaganda (i.e., psychological operations), etc.

⁷¹ http://en.wikipedia.org/wiki/Clandestine_HUMINT.

Country	Human Intelligence Organizations
Australia	Australian Secret Intelligence Service (ASIS)
Brazil	Agência Brasileira de Inteligência (ABIN)
Canada	Canadian Security Intelligence Service (CSIS) or (French: Service canadien du renseignement de sécurité, SCRS)
China	Ministry of State Security of the People's Republic of China
Cuba	Intelligence Directorate, Dirección General de Inteligencia (DGI)
North Korea	Cabinet General Intelligence Bureau
France	Cabinet General Intelligence Bureau
India	Research and Analysis Wing (RAW)
Israel	Mossad, (or Institute for Intelligence and Special Operations)
Germany	Bundesnachrichtendienst (BND) or Federal Intelligence Service
Greece	Εθνική Υπηρεσία Πληροφοριών Ε.Υ.Π or National Intelligence Service
Pakistan	Inter-Services Intelligence (ISI), Intelligence Bureau (IB)
South Korea	National Intelligence Service (South Korea)
Romania	Foreign Intelligence Service
Russia	Foreign Intelligence Service (Russian: Служба Внешней Разведки or SVR), Main Intelligence Directorate (Russian: Главное Разведывательное Управление or GRU).
South Africa	South African Secret Service (SASS)
United Kingdom	Secret Intelligence Service (SIS), commonly known as MI6, MI5 (<u>Military Intelligence, Section 5</u>)
United States	Central Intelligence Agency (CIA), National Clandestine Service (NCS), Defence Intelligence Agency (DIA), Defense Clandestine Service (DCS), National Security Service (NSA),etc.

Table 10: Human Intelligence Organizations⁷²

⁷² http://en.wikipedia.org/wiki/Clandestine_HUMINT.

2.2 Imagery Intelligence (IMINT).

2.2.1 Definitions and Role of IMINT⁷³.

Imagery intelligence is the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. Imagery analysis is the science of converting raw information which had been extracted from imagery into useable and reliable intelligence about a variety of subjects such as: activities, issues, objects, installations, and areas of interest. Imagery exploitation involves the evaluation, manipulation, and analysis of one or more images to extract information related to a list of essential elements of information. There are three phases of imagery exploitation:

1. **First Phase, also known as time-dominant:** The purpose of time-dominant exploitation is to satisfy priority requirements of immediate and/or identify changes or activities of immediate significance.
2. **Second Phase, non time dominant:** The purpose of second phase exploitation is to provide an organized and comprehensive account of the intelligence derived from validated intelligence requirements tasking.
3. **Third Phase, non time dominant:** In the third phase, detailed, authoritative reports on specific installation, objects, and activities are prepared by the agencies participating in the exploitation effort.

The role of Imagery Intelligence (IMINT), in the public sector, for example in Military sector, is to assist commanders in applying and protecting their combat power and support operations. Imagery often enhances the commander's situational understanding of the area of operations. Imagery is also used for military planning, training, and operations that include navigation, mission planning, mission rehearsal modelling, simulation, and precise targeting. Imagery assets, particularly unmanned aircraft systems, military satellites and moving target indicator systems, are useful in cueing other intelligence, surveillance, and reconnaissance systems. Other than direct human observation, IMINT is the only intelligence discipline that allows commanders to visualize the area of operations in near real time as the operation progresses. When maps are not available, hardcopy or softcopy versions of imagery can act as substitutes. Imagery can update maps or produce grid-referenced graphics. Detailed mission planning and intelligence preparation of the battlefield often require imagery, including three-dimensional stereo images, to provide the degree of resolution necessary to support specialized planning.

In the private sector today's technological development is offering a rich variety of uses unforeseen only a decade ago. Some of those uses are:

- Search and Rescue assistance,
- Medical emergency support,
- Images of natural disasters, (volcanic eruptions, high intensity earthquakes, damage from severe weather phenomena, etc).
- Images of technical disasters, (nuclear accidents, such as the Chernobyl nuclear disaster occurred on 26 April 1986, etc).

⁷³ US Field Manual FM 2-0: Intelligence, US Joint Publication 2-03: GEOINT Support to Joint Operations.

As an example we can mention the significant role of Imagery Intelligence in the research field of the Environmental Change. The uses of remotely sensed data in supporting all kinds of environmental investigations, (from oil fires in Kuwait, marine accidents with environmental consequences, to the destruction of the Amazon Rain Forest), are well documented and accepted by the scientific (and not only) community.

2.2.2 Imagery Intelligence Collection Platforms.

There are two general types of imagery collection platforms, those are:

1. **Satellites:** which are comprised and separated into national technical means and Commercial space platforms.
2. **Airborne systems:** Those systems can be divided into sub-categories such as:
 - Specially designed or modified military aircrafts and warplanes,
 - Specially designed or modified military helicopters,
 - Unmanned aerial vehicles (UAV).

All the above airborne systems are also comprised and separated into national and commercial.

National technical means: those systems are developed specifically for supporting the national requirements and specific needs of a country and its military forces.

Commercial space platforms and airborne systems: Commercial companies build, launch, and operate satellite and airborne imagery platforms for profit. Commercial imagery has become increasingly valuable for many reasons:

- □ Due to its unclassified nature, civil and commercial imagery are useful in an open environment, and might be released to different types of a country's government agencies, intergovernmental or nongovernmental organizations, and multinational partners. Civil and commercial imagery can be made available for public release/use.
- The use of civil and commercial imagery allows national technical means systems more time to focus on other intelligence functions.
- Civil and commercial imagery sources and companies offer electro-optical and radar imagery.
- Some offer large area collection useful for broad area coverage purposes, normally at a reduced resolution.

2.2.3 Types of Imagery Intelligence Sensors.

There are two general types of imagery sensors:

1. **Electro-optical sensors** which include:

- Panchromatic (visible),
- Infrared,
- Spectral (multispectral and hyperspectral), and
- Polarimetric.

2. Radar sensors: which are synthetic aperture radar systems that collect and display data either as representations of fixed targets or as moving target indicators. Each sensor and platform has a unique capability, with distinct advantages and disadvantages. The intelligence officer must understand the capability of each sensor and platform to make the best suitable selection for the mission purposes, in order to produce understandable intelligence products for the users. Certain sensors are better suited for military operations than others.

Sensors	Advantages	Disadvantages
Panchromatic (visible) Best tool for: <ul style="list-style-type: none"> • Daytime. • Clear weather. • Detailed analysis. <p>Includes full motion video and electro-optical still frame imagery.</p>	<ul style="list-style-type: none"> ➤ Affords a familiar view of a scene. ➤ Offers system resolution unachievable in other optical systems or in thermal images and radars. ➤ Preferred for detailed analysis and mensuration. ➤ Offers stereoscopic viewing. 	<ul style="list-style-type: none"> ➤ Restricted by terrain and vegetation. ➤ Limited to daytime use only. ➤ Degraded imagery in other than clear weather.
Infrared Best tool for: <ul style="list-style-type: none"> • Nighttime. • Clear weather. • Detection of human activity. <p>Includes Overhead Persistent Infrared (OPIR).</p>	<ul style="list-style-type: none"> ➤ Impossible to jam a passive sensor. ➤ Camouflage penetration. ➤ Night time imaging capability. 	<ul style="list-style-type: none"> ➤ Ineffective during thermal crossover periods. ➤ Not easily interpretable, requires skilled analysis. ➤ Cannot penetrate clouds.
Radar: <p>Useful for detecting the presence of objects at night and in bad weather. Includes synthetic aperture radar still frame imagery, and moving target indicator (MTI) data.</p>	<ul style="list-style-type: none"> ➤ All weather; penetrates fog, haze, clouds, and smoke. ➤ Day or night use. ➤ Active sensor; does not rely on visible light or thermal emissions. ➤ Best sensor for change Detection, good standoff capability. ➤ Large area coverage. ➤ Moving target detection. 	<ul style="list-style-type: none"> ➤ Not easily interpretable, does not produce a literal representation of imaged area. ➤ Requires skilled analysis. ➤ Difficult to obtain positive identification or classification of equipment.
Multispectral imagery Best tool for: <ul style="list-style-type: none"> ➤ Mapping purposes. ➤ Terrain analysis. 	<ul style="list-style-type: none"> ➤ Large database available. ➤ Band combinations can be manipulated to enhance interpretability. ➤ Images can be merged with other digital data for higher resolution. 	<ul style="list-style-type: none"> ➤ Large files slow to ingest. ➤ Not easily interpretable, requires skilled analysis. ➤ Computer manipulation requires large memory and storage capabilities, requires large processing capabilities.

Table 11: Sensors Characteristics Matrix⁷⁴.

⁷⁴ US Field Manual FM 2-0: Intelligence.

2.2.4 Imagery Intelligence in the Intelligence Process.

The Imagery Intelligence discipline has several unique considerations throughout the continuing activities and steps of the intelligence process. At the next paragraphs we will present – analyze the intelligence process tailored to the Imagery Intelligence discipline.

2.2.4.1 Generate Intelligence Knowledge.

The intelligence analyst should research for “targets” or topics using online imagery databases and request those of non perishable imagery products for contingency planning. National (military or governmental agencies or bureaus), and private (commercial companies), imagery databases may contain or obtain recently imaged areas that could meet the commander’s or managers immediate and specific needs, (instead of requesting new imagery collection).

2.2.4.2 Analyze.

Timeliness is critical not only to imagery collection but also to Imagery Intelligence reporting and imagery analysis. It is difficult to separate Imagery Intelligence reporting from imagery analysis in this discussion, as demonstrated below, all the three phases of Imagery Intelligence reporting are depending on timeliness requirements. Each phase represents a different degree of analysis and period available to accomplish imagery exploitation:

- **First phase:** imagery analysis (time-dominant), is the rapid exploitation of newly acquired imagery in order to satisfy an immediate need, based on the commander’s, managers or client requirements. Time-dominant exploitation and reporting are accomplished in accordance with unit standing operating procedures (military), but not later than 24 hours after receipt of imagery. This phase satisfies priority intelligence requirements and/or identifies changes or activity of immediate significance. First phase imagery analysis normally results in an initial phase imagery report.
- **Second phase:** imagery analysis is the detailed exploitation of recently acquired imagery and the reporting of imagery - derived intelligence and information while meeting the production and timeliness requirements. Other intelligence discipline source material may support second phase imagery, as appropriate, and may result in a secondary supplemental imagery report.
- **Third phase:** imagery analysis is the detailed analysis of all available imagery pertinent to a specific information requirement and the subsequent production and reporting resulting from this analysis within a specified time. This phase provides an organized detailed analysis of an imagery target or topic, using imagery as the primary data source but incorporating data from other sources as appropriate.

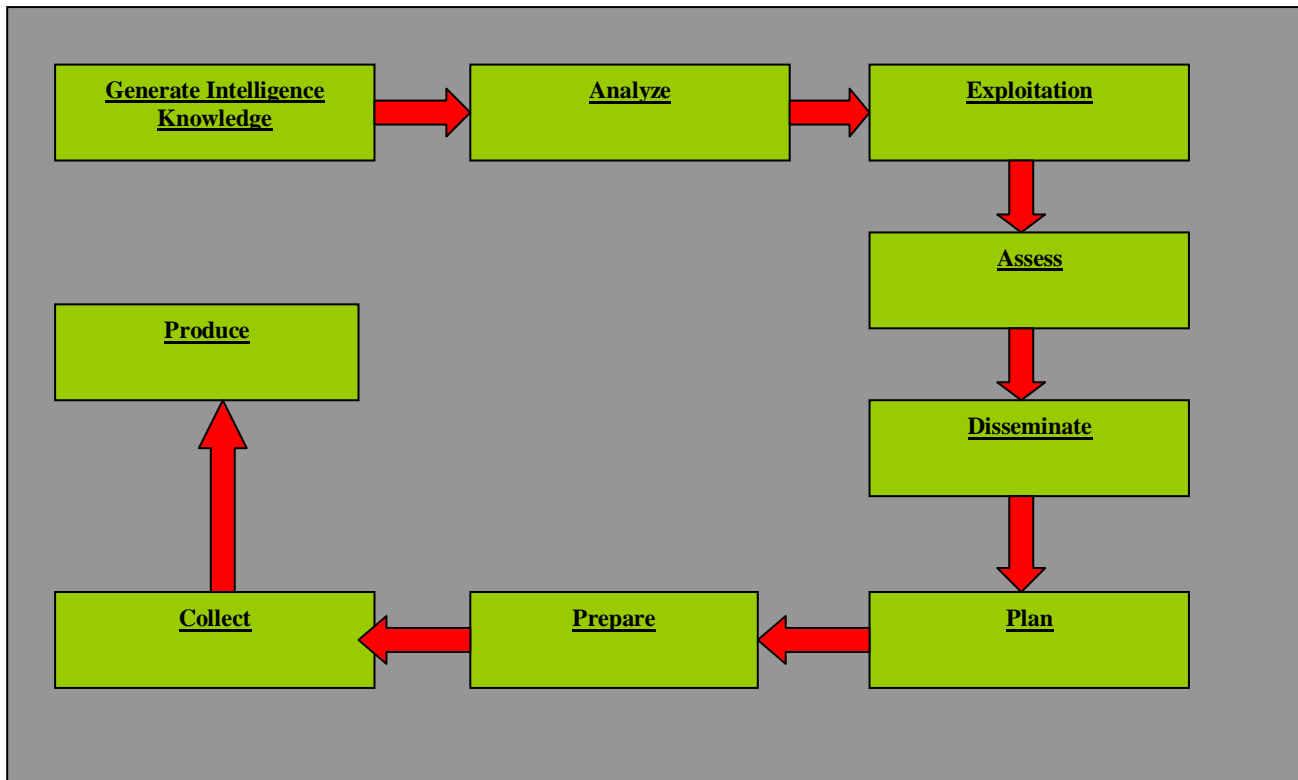


Diagram 6: Imagery Intelligence in the Intelligence Process.

2.2.4.3 Exploitation.

There are two types of imagery exploitation, which are:

- **National exploitation:** is imagery exploitation that supports governmental requirements, national security requirements, or requirements of a common concern to the intelligence community.
- **Departmental exploitation:** is imagery exploitation that supports assigned missions of a single agency, department, or command or company. Imagery analysts complete departmental exploitation to satisfy requirements depending on phase and exploitation and report the results as soon as possible. Timelines for completing exploitation vary depending on the demands and unit capabilities.

2.2.4.4 Assess.

Upon receipt, the requestor should immediately assess the imagery product for accuracy, coherence and relevance to the original request. The requestor then notifies and informs the imagery analyst about the extent to which the product answered – responds to the requirements. Providing feedback, regarding the product, to the producer helps ensure that the producer will provide the required information in the correct format. The following are some of the questions that the requestor should consider when providing feedback to the producer:

- Does the product have the proper classification markings?
- Is the product format acceptable?
- Is additional product or future product information needed?

- Is excess product information included?
- Does the imagery intelligence product satisfy the requirement?

2.2.4.5 Disseminate.

Imagery Intelligence products are disseminated in digital and hardcopy formats. Analysts at the producing organization are responsible for ensuring dissemination. Digital dissemination is the primary means of dissemination. It can be accomplished by posting products to organizational image product libraries and intelligence community Web sites, or even disseminating directly via e-mail (such as in JPEG format). Couriers or other mail systems will distribute the hardcopy products.

2.2.4.6 Plan.

Determining requirement is the first step in planning for Imagery Intelligence. The staff must clearly articulate their intelligence requirements to include communicating, what the mission is and how the requested product will aid in mission/purpose or objective accomplishment. The intelligence analyst should submit the imagery, collection, and production requirements in the Geospatial Intelligence Management System (GIMS) using established procedures, or as established by the client - requestor.

The intelligence analyst must also determine the specific imagery requirements to avoid burdening the system with unnecessary requests. The desire for imagery products often exceeds the capabilities of the imaging system. Therefore, it is imperative that intelligence analysts must consider the type of analysis needed and request only what they require. The specifications of the request for Imagery Intelligence products often affect the timeliness of the response.

2.2.4.7 Prepare.

The Imagery Intelligence analysts or officers - related actions during the prepare step include establishing or verifying the portion of the intelligence communications architecture that supports receipt, processing, displaying, and analysis of imagery. Additionally, the intelligence analyst or officer ensures that required IMINT analytical assets and resources are prepared to provide support or are available through intelligence reach. Lastly, the intelligence analyst or officer also ensures that IMINT reporting and dissemination channels and procedures are in place and rehearsals are conducted with all pertinent IMINT elements in order to ensure interoperability.

2.2.4.8 Collect.

A given target or an area of interest will not necessarily receive continuous coverage, the continuity depends on the priorities and requirements of the requestor and the number and availability of imaging assets and means.

2.2.4.9 Produce.

The imagery analyst ensures that the Imagery Intelligence product satisfies the associated intelligence requirements and the product is in the required format. The quality and resolution of the product highly depends on the type of sensor, the platform, collection geometry, the time of day, and the weather conditions. The quality and resolution directly affect the imagery analyst's ability to identify objects and analyze activity within the images. Imagery Intelligence products include:

A. Public Sector (military, governmental agencies, etc):

- Imagery that detects and/or identifies and locates specific type of units and equipment, obstacles, and field fortifications from which intelligence analysts can assess enemy capabilities and develop possible courses of action.
- Imagery that updates maps and enhances the interpretation of information from maps. Detailed mission planning uses imagery including stereo images for three-dimensional viewing of the terrain.
- Motion Target Indicators and full-motion video displays or products that provide a near real-time picture of an object's movement by indicating its speed, location, and direction of travel. MTI systems do not differentiate friendly from enemy forces.
- Imagery that supports protection of the force by helping commanders visualize how their forces look, including their disposition, composition, and vulnerabilities, as exploited by enemy IMINT systems.
- Target packets with imagery of the high-value targets and high-payoff targets that include critical elements of the targets and potential collateral damage.
- Imagery that supports combat assessment to confirm damage, determine the percentage of damage, or whether the target was unaffected.
- Advanced geospatial intelligence (GEOINT) products that can determine change detection, specific weapon system identifications, chemical compositions and material content, and a threat's ability to employ these weapons.

B. Private Sector (companies, non governmental agencies and organizations, etc):

- Imagery that detects and/or identifies and locates specific type of environmental changes or disasters.
- Imagery that supports assessments to confirm damage, determine the percentage of damage, or whether an area of interest was unaffected by a natural disaster.
- Imagery that updates maps and enhances the interpretation of information from maps. Detailed mission planning (save and rescue and peace keeping operations), uses imagery including stereo images for three-dimensional viewing of the terrain.
- Motion Target Indicators and full-motion video displays or products that provide a near real-time picture of an "object's" movement (such as Tornadoes, hurricanes, etc), by indicating its speed, location, and direction.
- Imagery that supports protection of a specific area of interest (for example a National Park during the summer period in which the chances of a fire are bigger).

2.3 Geospatial Intelligence (GEOINT).

Geospatial Intelligence is a specialized field of practice within the broader profession of intelligence. The Geospatial Intelligence discipline encompasses all activities involved in the planning, collection, processing, analysis, exploitation, and dissemination of spatial information in order to gain intelligence about the national security or operational environment, visually depict this knowledge, and fuse the acquired knowledge with other information through analysis and visualization processes.

At the next paragraphs we are going to present the basic definitions which are related to Geospatial Intelligence, those are the following:

1. **Amplified definition⁷⁵:** “GEOINT encompasses all aspects of imagery (including capabilities formerly referred to as Advanced Geospatial Intelligence and imagery-derived MASINT), and geospatial information and services (GI&S), formerly referred to as mapping, charting, and geodesy). It includes, but is not limited to, data ranging from the ultraviolet through the microwave portions of the electromagnetic spectrum, as well as information derived from the analysis of literal imagery; geospatial data; and information technically derived from the processing, exploitation, literal, and non-literal analysis of spectral, spatial, temporal, radiometric, phase history, polarimetric data, fused products (that is products created out of two or more data sources), and the ancillary data needed for data processing and exploitation, and signature information (to include development, validation, simulation, data archival, and dissemination). These types of data can be collected on stationary and moving targets by electro-optical, and related sensor programs (both active and passive) and non-technical means (to include geospatial information acquired by personnel in the field)⁷⁶”.
2. **De facto definition⁷⁷:** An emerging de facto definition of geospatial intelligence is vastly different than the de jure definition expressed in U.S. Code. This new de facto definition is:

“Geospatial Intelligence is a field of knowledge, a process, and a profession. As knowledge, it is information integrated in a coherent space-time context that supports descriptions, explanations, or forecasts of human activities with which decision makers take action. As a process, it is the means by which data and information are collected, manipulated, geospatially reasoned, and disseminated to decision-makers. The geospatial intelligence professional establishes the scope of activities, interdisciplinary associations, competencies, and standards in academe, government, and the private sectors⁷⁸”.

This has been suggested as an operational definition of Geospatial Intelligence which might use the moniker of GeoIntel so as to distinguish it from the more restrictive definition offered in U.S. Code Title 10, §467.

⁷⁵ http://en.wikipedia.org/wiki/Geospatial_intelligence.

⁷⁶ Memorandum for Principal Director of National Intelligence, Deputy Director of National Intelligence for Collection, from James R. Clapper, Lieutenant General, USAF (Ret.), Director [NGA] 17 October 2005, [gwg.nga.mil](http://www.gwg.nga.mil).

⁷⁷ http://en.wikipedia.org/wiki/Geospatial_intelligence.

⁷⁸ Bacastow, T.S. and Bellafore, D.J. (2009). Redefining geospatial intelligence. American Intelligence Journal. Pp 38-40.

Advanced technology now provides the capability to use and combine geospatial data in different ways to create interactive/dynamic and fully customized visual products. It allows the analysts to quickly make more complex connections between different types of data and information than previously possible. Geospatial products can now leverage a wider variety of data, including other intelligence disciplines (such as SIGINT, HUMINT, and MASINT), through collaborative processes, to provide more accurate, comprehensive, and relevant products. GEOINT can also be combined with other intelligence disciplines, such as SIGINT, to develop custom and tailored products. The result of these advances is a transformation in the analytic and technical processes used to create geospatial products. It is the cumulative effect of all these changes that propelled the evolution of the GEOINT discipline.

The discipline of GEOINT encompasses more than systems, technology, and processes. The discipline is comprised of highly skilled professionals with a wide range of expertise. Collectively, they possess an advanced body of knowledge and operating principles developed over many years of experience. These GEOINT professionals represent and are drawn from a wide range of occupations comprising the GEOINT tradecraft. GEOINT tradecraft is the application of skills, leadership, continuing education, mentoring, special experiences, and knowledge of GEOINT in one or more occupational specialties. However, each professional should be considered a GEOINT analyst first and an expert in a specific occupational specialty second.

2.3.1 Geospatial Intelligence Elements.

Geospatial Intelligence Elements are the ones we are going to present below:

- **Imagery:** A likeness or representation of any natural or manmade feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, including products produced by space-based national intelligence reconnaissance systems, and likenesses and representations produced by satellites, airborne platforms, unmanned aircraft systems, or similar means. This does not include handheld or clandestine photography taken by or on behalf of human intelligence (HUMINT) collection organization.
- **Imagery intelligence (IMINT):** The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials.
- **Geospatial information:** Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies and mapping, charting, geodetic data, and related products.

The term GEOINT encompasses both the standard, and traditional, and the specialized (integrated) capabilities of imagery, IMINT, and geospatial information. The full utility of GEOINT comes from the integration of all three, which results in more comprehensive, tailored GEOINT products for a wider scope of problems and customers across all functional areas. For example, GEOINT can incorporate advanced technology to create dynamic, interactive products such as realistic mission simulations that helps to determine the effects of speed, currents, tide, wind, daylight, etc. on a mission or intelligence problem. These products might be virtual flythrough and walk-through mission scenarios or interactive maps. GEOINT can also create a common operational picture of a specific area by effectively using multiple and advanced sensors, multiple types of data and information (including operations, planning, logistics, etc.), as well as multiple intelligence disciplines to present a comprehensive visual depiction. This capability provides many advantages for the war fighter, national security policymakers, homeland security personnel, and intelligence

community collaborators by precisely locating activities and objects, assessing and discerning the meaning of events, and providing context for decision makers.

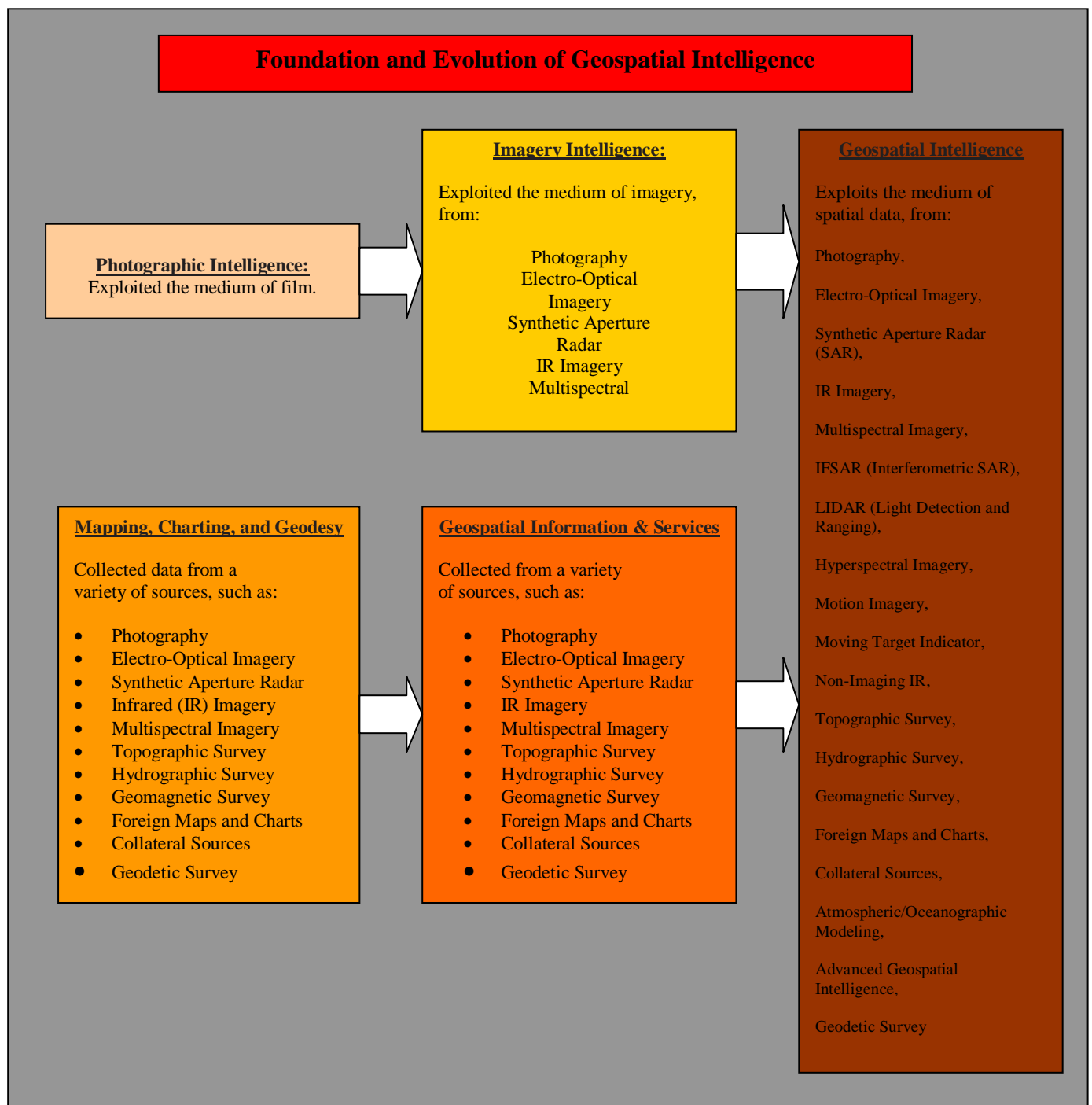


Table 12: Foundation and Evolution of Geospatial Intelligence⁷⁹.

⁷⁹ US Joint Publication 2-03: GEOINT Support to Joint Operations.

2.3.2 The Four Fundamental Components of Geospatial Intelligence.

There are four fundamental components of GEOINT: the discipline of GEOINT, the data that comprise GEOINT, the process used to develop GEOINT products, and the products derived from GEOINT.

- **Discipline:** GEOINT is a specialized field of practice within the broader field of intelligence. The GEOINT discipline encompasses all activities involved in the planning, collection, processing, analysis, exploitation, and dissemination of geospatial information to gain - obtain intelligence about the operational environment, a topic or specific requirement, visually depict of this information, and fuse the visual information with other information through analysis and visualization processes.
- **Data:** GEOINT is developed from the same geospatially - derived data used to create geospatial information, imagery, and IMINT. It also uses intelligence data from other intelligence disciplines to corroborate and provide context to geospatial information. The full capabilities of GEOINT are only realized when two or more types of data are combined and analyzed to create a comprehensive GEOINT product.
- **Process:** Many different analytic processes have been used successfully over the years to create geospatial products. For example the analytic methodology used by US National Geospatial Agency (NGA) is known as GEOINT preparation of the environment (GPE). GPE supports joint intelligence preparation of the operational environment (JIPOE). It is a proven methodology and, of equal importance, it provides a common frame of reference and language between military and civilian personnel.
- **Products:** GEOINT products range from standard geospatial data – derived products, maps, and imagery to specialized products that incorporate data from multiple types of advanced sensors and use four dimensions.

2.3.3 The Five Characteristics of Geospatial Intelligence.

1. Incorporates intelligence analysis into all aspects.
2. Uses multiple types of sensors and advanced sensor technology.
3. Combines multiple types of geospatial data.
4. Uses intelligence data from other intelligence disciplines for corroboration and context.
5. Adds more dimensions to standard geospatial products.
 - 5a. 3rd Dimension: provides the capability to visualize in three dimensions.
 - 5b. 4th Dimension: integrates the elements of time and movement (allowing for realistic motion to create dynamic and interactive visual products).



The use of long endurance, unmanned aerial vehicles, such as the MQ-1 Predator, greatly facilitates real-time, persistent surveillance.

2.3.4 The applications of Geospatial Intelligence.

The use of Geospatial Intelligence can be categorized into five general areas for both public and private sectors:

- I. **General Military Intelligence, Indications and Warning (I&W):** As one component of general military intelligence and I&W, GEOINT supports monitoring scientific and technological developments and capabilities of foreign military forces for long - term planning purposes, detecting and reporting foreign developments that could involve a threat to a country or allied countries, and coalition military, diplomatic, or economic interests or to a country's citizens abroad. Additionally, GEOINT supports I&W situational awareness by providing warning of possible increased threats or significant increased tactical positioning of enemy wartime assets.
- II. **Safety of Navigation:** Using bathymetric, hydrographic, maritime safety, gravimetric, aeronautical, and topographic information for ship, aircraft, and land navigation for both public (military, governmental agencies and organizations), and private (non governmental agencies – organizations, companies, etc), sectors.
- III. **Operational Environment Awareness:** Visualizing the operational environment, by tracking movements of interest, monitoring airfield and port activity.
- IV. **Mission Planning and Command and Control (C2):** Employing foundation data and mission -specific data to plan and execute missions, evaluate mission progress, adjust schedules, and assign and apportion forces as appropriate.
- V. **Target Intelligence:** GPE, target development, which includes precise point generation, with collateral damage estimate, battle damage assessment, and munitions effectiveness assessment functionally integrated into a seamless repeatable standardized end - to end process.

2.3.5 Geospatial Intelligence Tradecrafts.

- **Aeronautical Analysis:** The science of developing specialized representations of mapped natural and man - made features of the Earth and supplemental metadata specifically to aid air navigation, pilotage, or planning air operations.
- **Cartography:** The art and science of making maps and charts.
- **Geodetic Sciences:** The sciences of geodesy and geophysics that deal with information or Earth data pertaining to gravity, point positioning, datum's, etc.
- **Geospatial Analysis:** The science of extracting meaning from geospatial data and using geographic information systems to uncover and investigate relationships and patterns in all forms of geospatial data to answer intelligence or military issues.
- **Imagery Analysis:** The science of converting information, extracted from imagery, into intelligence about activities, issues, objects, installations, and/or areas of interest.
- **Imagery Sciences:** The technical application of remote sensing towards the production of GEOINT products and services.
- **Marine Analysis:** The portrayal of specialized representations of oceanographic, hydrographic, bathymetric data, and supplemental metadata, required for maritime navigation, pilotage, or planning maritime operations.
- **Regional Analysis:** The geographic, geopolitical, or intelligence analysis of a particular country or area of the world.
- **Source Analysis:** Source analysts manage partner relationships, coordinate collection operations with mission partners or other disciplines, perform assessments of collection operations, and support information need brokering activities. Source analysts also proactively develop strategies to identify and deliver sources most helpful to analysts in order to answer specific intelligence problems or requirements.

2.3.6 The Geospatial Intelligence Operations Process.

The GEOINT operations process utilizes the intelligence process, this chapter will provide an overview of each one of the GEOINT operational phases, which are:

- **Planning and Direction:** The GEOINT planning function includes planning for both geospatial information and services and imagery support. Direction refers to the process of shaping and prioritizing the actions identified during planning to create a balanced GEOINT collection requirement strategy. The GEOINT cell conducts both GI&S and imagery-related planning activities for the combatant command. The GEOINT cell supports the intelligence planning process through the development of functional support plans for geospatial intelligence analysis and production.
- **Collection:** Information needs drive collection operations. The GEOINT process requires the tasking and collection of both imagery and geospatial data. Two major categories of collection systems are used, those systems are:

1. Satellite Systems:

- 1a. The national systems are a primary source of collection for imagery used to produce geospatial information. Every country designs, builds, and operates the nation's reconnaissance satellites.
- 1b. Commercial systems collect electro-optical (EO), multispectral, and radar data, but have a more narrow scope of operations than national systems. Commercial systems and commercial producers increasingly contribute geospatial information and products for both governmental and non governmental agencies, services and organizations requirements. These systems can also provide unclassified versions of intelligence that, under certain circumstances, may be shared with allies or coalition partners. Private companies operate commercial systems.

2. Airborne Systems:

- 2a. Government airborne systems at the theater and tactical level provide ISR assets. The full spectrum of airborne ISR sources includes all manned and unmanned platforms that collect still and motion imagery using visible, thermal, multiband, multispectral, hyperspectral, laser-based or radar-based imaging sensors.
- 2b. Commercial airborne systems provide yet another source of GEOINT. Due to their flexibility and resolution capabilities, commercial airborne collectors are increasingly relied upon to augment satellite collection.

- **Processing and Exploitation:** After being processed, geospatial data is distributed, archived, and made accessible for users. The user can manipulate data from available libraries or databases to create tailored products or data sets for specific mission purposes or military. Imagery exploitation involves the evaluation, manipulation, and analysis of one or more images to extract information related to a list of essential elements of information. A report on the results is normally part of exploitation and the way in which the information is disseminated. There are three phases of imagery exploitation: first phase, also known as time-dominant, and second and third phase, which are non-time dominant.
 1. Time-dominant exploitation (also referred to as First-Phase exploitation): The exploitation of newly-acquired imagery within a specified time from receipt of imagery. The purpose of time-dominant exploitation is to satisfy priority requirements of immediate need and/or to identify changes or activity of immediate significance. Time-dominant exploitation and reporting is accomplished as soon as possible according to validated intelligence requirements, but not later than 24 hours after receipt of imagery.
 2. Non-time-dominant exploitation, or Second Phase Exploitation: The detailed non-time dominant exploitation of imagery scheduled within the bounds of analytic requirements and timelines of need (typically within one week after receipt of imagery). The purpose of second phase exploitation is to provide an organized and comprehensive account of the intelligence derived from validated intelligence requirements tasking.

3. **Non-time-dominant exploitation or Third Phase Exploitation:** In depth, long-range analysis that includes all available sources of imagery. It is in this phase that detailed, authoritative reports on specified installations, objects, and activities are prepared by the agencies participating in the exploitation effort. Third phase exploitation timelines are not bounded and typically exceed one week after receipt of imagery.
- **Analysis and Production:** GEOINT products include traditional GI&S and imagery products as well as more advanced products created by combining GI&S and imagery data into a single, multidimensional product. This advanced method provides the battlefield commander or the manager with comprehensive, highly detailed, and precise GEOINT products. Once data has been processed, a variety of users can exploit it and produce either general intelligence or mission-specific products. Data can also be combined in a variety of ways to develop tailored products for specific mission requirements. Users and/or requesters of the intelligence should coordinate with the producers to ensure the products meet mission needs. As an example at the combatant command and Service levels, hydrographic and geospatial engineering units or sections provide the ability to analyze integrated databases for specific applications, add valuable information or update features and attributes within the database, and strengthen the database content to meet the commander's tailored mission requirements.
 - **Dissemination and Integration:** Dissemination is the timely conveyance of GEOINT products in an appropriate form and by any suitable means, whether in hard copy or electronic form. Dissemination is accomplished through both the "pull" and "push" principles. The "pull" principle provides intelligence organizations at all levels with direct reach back capability via electronic access to central databases, intelligence files, or other repositories containing GEOINT data and products. The "push" principle allows the producers to transmit GEOINT to the requestors along with other relevant information. Typically, the intelligence staff element at each echelon manages the dissemination of GEOINT. Current GEOINT-focused processes disseminate GI&S, imagery, and/or imagery-related products. Single dissemination processes are becoming increasingly common as GEOINT evolves.
 - **Evaluation and Feedback:** Many of the GEOINT operations are a combination of individual intelligence products, which are powerful capabilities in and unto themselves that provide a much stronger capability when combined together. It is imperative that intelligence personnel and consumers at all levels provide honest, timely feedback, throughout the intelligence process, on how well the various intelligence operations perform to meet the commander's requirements.

2.3.7 Categories of Geospatial Intelligence Products.

Geospatial Intelligence products range from standard geospatial data - derived products, such as maps and imagery, to specialized products that incorporate data from multiple types of advanced sensors and use four dimensions.

Geospatial Intelligence products usually incorporate intelligence analysis, to ensure that the most comprehensive product is developed. However, customers do not always require or want analyzed products. Almost any type of Geospatial Intelligence product can be produced without using intelligence analysis (e.g. using GEOINT as a base for visualization activities such as a Common Operational Picture). The main categories of Geospatial Intelligence Products and related services and support are the ones which are listed below:

1. **Standard Products:** These include geospatial data-derived products such as maps, charts, imagery and digital raster or vector information. These products may be used alone or with many layers of additional data such as geographic data (vegetation, culture, languages, and weather) and intelligence information. Standard products are primarily derived from electro-optical sensors and existing geospatial data. They can also be derived from radar and multi-spectral sensors, but standard products do not routinely use these sources. The products are normally two-dimensional but can be processed into three-dimensional products, such as anaglyphs. Standard products satisfy a significant portion of GEOINT requirements that would not benefit from the added capabilities of specialized products. Further, geospatial data and standard products are the foundation for development of specialized products. Thus, standard products will continue to comprise a large portion of GEOINT production.

1.1 Examples of Standard products:

1.1.1 **Electro-optical (EO) image:** of an area that has been attacked. It includes factual data on the location and number of vehicles and aircraft in the image.

1.1.2 **Analyzed EO image:** that uses the same factual data as above, but has been interpreted and analyzed, or has incorporated, other intelligence information to provide information on types of vehicles and aircraft activity as well as a battle damage assessment.

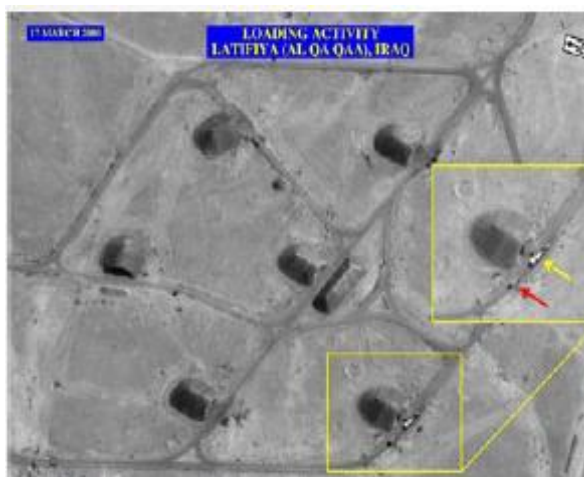


Photo 2: Example of Electro – optical image.

1.2 **Map:** that shows information on the topography, infrastructure, vegetation, and enemy locations in an area of interest.

1.2.1 **Analyzed map:** for which the same map and information above is used; however the map has now been interpreted and analyzed or incorporated other intelligence information to show potential avenues for attack.



Photo 3: Example of a Map.

2. **Specialized Products:** Specialized products can provide additional capabilities to standard products, to customize them for a specific purpose. The products might be developed using sophisticated technology to integrate multiple types of geospatial data as well as data from other intelligence disciplines. The more unique characteristics of specialized products include the incorporation of data from more technically advanced sensors and the use of a fourth dimension – time. The element of time can be used for many purposes, such as introducing motion to create dynamic, interactive products. These advanced features allow analysts to create a more comprehensive geospatial intelligence product. Examples of specialized products include two-color, multi-view (2CMV), change detection, multi/hyper-spectral, and tailored products such as line-of-sight and fly-through scenarios.

2.1 Examples of Specialized Products:

2.1.1 **2CMV image:** shows aircraft parked on an airfield. A simple assessment indicates that two aircraft have departed since the previous day.

2.1.2 **Analyzed 2CMV:** same image and information from above, with the addition of an intelligence assessment on:

- 1) the reason for departure and
- 2) the known or suspected destination of the departed aircraft. The assessment also notes other significant changes in levels of activity at the airfield.

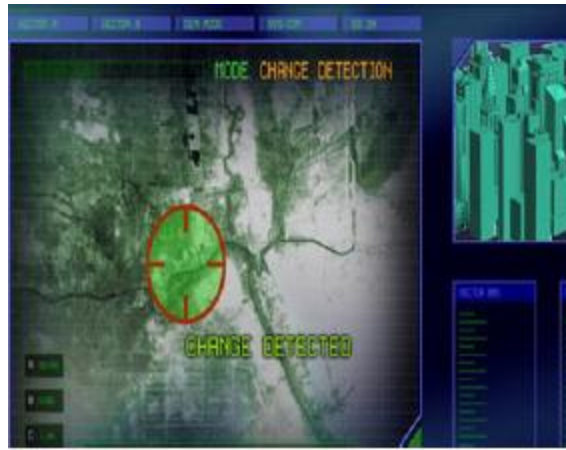


Photo 4: 2Color Multi-View Change Detection.

2.2 Unanalyzed 3D fly-through: shows factual information in three dimensions such as buildings, streets, and topography of an area.

2.2.1 Analyzed 3D fly-through: the same fly-through and information used above that has been interpreted or analyzed and/or combined with intelligence data derived from photos taken by a HUMINT source that show precise details on buildings that might affect collection. It also includes intelligence data from SIGINT, HUMINT, OSINT and MASINT sources that show enemy and threat locations. The simulation allows predictions on where the enemy may be located.

2.3.7.1 Geospatial Intelligence Product Categories and Services.

Geospatial intelligence products are often developed through a process known as “value added,” in which both the producer and the user or requestor of GEOINT updates a database or products with current information. Human collectors are the key component of this process. This newly - identified data is usually referred as “feature data.” New roads, lines of communication, obstacles, changes in terrain, and seismic activity are examples of activities that require updating due to frequent changes in the area of interest. Both standard and specialized GEOINT products fall into seven general categories:

- **Aeronautical:** Examples: Flight Information Publications (FLIP), Aeronautical Charts & Graphs, Digital Aeronautical Flight Information Files (DAFIF), Digital Vertical Obstruction File (DVOF), and mission fly-throughs.
- **Nautical/Hydrographic:** Examples: Bathymetric Navigation Plan Chart (BNPC), Notice to Mariners, Nautical Charts, Digital Nautical Chart (DNC) and Littoral Charts.
- **Topographical /Terrestrial:** Examples: Controlled Image Database (CIB), Image City Maps (ICM), Digital Terrain Elevation Data (DTED), Escape and Evasion Charts, Topographic Line Maps (TLM), and mission walk-through.
- **Precise Positioning & Targeting:** Examples: Precise Point Menstruated Graphics (PPMG) and Digital Point Positioning Database (DPPDB).

- **Geodesy & Geophysics:** Examples: GPS Precise Ephemeris, Earth Gravity Model '96 (EGM96) and World Geodetic System (WGS).
- **Geographic Names:** Examples: Romanization Guide, GEOnet Names Server Reference Source and Gazetteers.
- **GEOINT Analysis:** Examples: Intelligence Briefs, First Looks, Imagery Reports.

This product category list is helpful in understanding the variety of uses for which GEOINT products are developed. However, it is important to note that many standard products do not fall solely into one area, and most specialized products are hybrid products that integrate data and information from more than one of those areas.

2.3.7.2 Geospatial Intelligence Services.

Geospatial intelligence services that support the generation, management, and use of GEOINT data and products are essential to an effective National System for Geospatial Intelligence (NSG). The services include tools that enable both users and producers to access and manipulate data. Examples of GEOINT services are instruction, training, laboratory support, and guidance for the use of geospatial data. Geodetic surveys, software development, tailored geodetic and geophysical products and services to support weapons systems, the calculation of precise locations for targeting of precision guided munitions, training, and on-site technical support are all types of GEOINT services.

2.3.8 An Example of Geospatial Intelligence Analysis Methodology.

2.3.8.1 Geospatial Intelligence Preparation of the Environment (GPE).

Geospatial products become analyzed Geospatial intelligence as a result of the intelligence analysis process. There are many methodologies which can be used to create GEOINT, in this section we are going to present and analyze one of the most common analytic methodology process which is known as Geospatial Intelligence Preparation of the Environment (GPE), we can use it in order to predict intelligence problems during the analytical process. The methodology is based upon the military's Joint Intelligence Preparation of the Battle space (JIPB) process but was modified so that it can be used for non - military intelligence problems.

Given the logic and efficacy of the military analytic methodology the GPE methodology has been widely adapted for applications across many problem sets, including:

- Law enforcement,
- Investigative work, and
- Information operations.

The process has been adapted to include civilian and other non - traditional threat problems, GPE may be used to aid analysis for military operations as well as non - battlefield actions such as:

- **National Security Special Events:** For example, a threat evaluation for the Olympics.
- **Disaster Relief:** Natural disaster relief (a hurricane, a tsunami, etc).

- **Civilian Evacuations:** An evacuation of embassy personnel, recovery from domestic natural disasters (such as hurricanes, earthquakes, etc).
- **Specific National Security Requirements:** Issues relating to the exploitation of the exclusive economic zone.

Geospatial Intelligence Preparation of the Environment is a systematic, four - component process. The components ensure that the analysts will consider all the available information, however, it is not a rigid checklist. GPE provides the analysts with a template for use across the spectrum of intelligence problem sets. The four components of Geospatial Intelligence Preparation of the Environment are described below:

Component 1 - Define the Environment: Gathering of basic facts needed to outline the exact location of the mission or area of interest. Physical, political, and demographic boundaries must be determined. The data might include grid coordinates, latitude and longitude, vectors, altitudes, natural boundaries (mountain ranges, rivers), etc. This data serves as the foundation for the GEOINT product.

Component 2 - Describe the Environment's Influence: Provide descriptive information about the area defined in Component 1. Identify existing natural conditions, infrastructure, and cultural factors. Consider all details that might affect a potential operation in the area:

- ❖ Weather conditions,
- ❖ Vegetation,
- ❖ Roads,
- ❖ Facilities and structures,
- ❖ Population,
- ❖ Language, and
- ❖ Cultural details such as: ethnic, religious, social and political factors.

Component 3 - Evaluate Threats and Hazards: Add intelligence and threat data, drawn from multiple intelligence disciplines, onto the foundation and descriptive information layers (the environment established in the first two steps). This information includes:

- A. Public Sector (military example): order-of-battle, size and strength of enemy or threat, adversary doctrine, the nature, strength, capabilities, and intent of area insurgent groups, and possible chemical/biological effects.
- B. Private Sector: the nature, capabilities, and intent of a competitor, of a country , etc.

Component 3 requires collaboration with national security community counterparts.

Component 4 - Develop Analytic Conclusions: Integrate all information from Components 1 - 3 to develop analytic conclusions. The emphasis is on developing predictive analytic conclusions. For example, the analyst might create models in order to determine likely next courses of action for the adversary, threat, or hazard and then assess the potential impact of those actions. In some cases, Component 4 could include an assessment of potential reactions to friendly operations⁸⁰.

⁸⁰ Of course, friendly operations and courses of action can also be analyzed and visualized by using GEOINT as a foundation base.

2.4 Measurement and Signature Intelligence (MASINT).

Measurement and Signature Intelligence was recognized by the United States Department of Defence as an intelligence discipline in 1986⁸¹. In the Army Intelligence Field Manual we can find the below definition:

“Measurement and signature intelligence is intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic), derived from specific technical sensors for the purpose of identifying any distinctive features associated with the emitter or sender, and to facilitate subsequent identification and/or measurement of the same. The detected feature may be reflected or emitted⁸²”.

Measurement and signature intelligence (MASINT), collection systems include (but are not limited to), radar, spectroradiometric, electro - optical, acoustic, radio frequency, nuclear detection, and seismic sensors, as well as techniques for collecting chemical, biological, radiological, nuclear, and high - yield explosives (CBRNE) signatures and other materiel samples. MASINT requires the translation - modification of technical data into recognizable and useful target features and performance characteristics. Nowadays, technological development in various fields such as: Computing, Communication, Data and Display processing technologies can provide Measurement and Signature Intelligence to support operations (both military and civilian). Measurement and signature intelligence provides intelligence to:

1. Public Sector: governmental agencies, services and organizations, for example:

- 1.1 The commander of a military force in full spectrum operations to facilitate situational understanding.
- 1.2 The commander of a peacekeeping force to facilitate situational understanding.
- 1.3 MASINT systems can provide to the first responders detection of Chemical, Biological, Radiological, and Nuclear agents (CBRNE), both before, during, or after employment.

2. Private Sector: non governmental agencies, services and organizations, for example:

- 2.1 The Commander and staff of the United Nations Forces during peacekeeping operations to facilitate situational understanding.
- 2.2 The staff of non-governmental voluntary organizations during recovery operations from natural disaster incidents, or after nuclear accidents, etc.
- 2.3 Detect natural or manmade environmental disturbances in the earth's surface not discernible through other intelligence means.
- 2.4 Detect and track for safety and security reasons aircrafts, ships, and vehicles.

⁸¹ Interagency OPSEC Support Staff (IOSS) (May 1996), “Section 2, Intelligence Collection Activities and Disciplines”, Operations Security Intelligence Threat Handbook, retrieved 2007-10-03.

US Army (May 2004). “Chapter 9: Measurement and Signals Intelligence”. Field Manual 2-0, Intelligence. Department of the Army. Retrieved 2007-10-03.

⁸² Joint Publication 2-03: Geospatial Intelligence Support to Joint Operations.

Measurement and signature intelligence systems can defeat many of the camouflage, concealment, and deception techniques which are used to deceive intelligence, surveillance, and reconnaissance (ISR) systems. By application of near real-time analysis and dissemination, measurement and signature intelligence systems have a potential ability to provide timely situational awareness and targeting, (not necessarily available to other disciplines). Specifically, MASINT sensors have some “unique” capabilities such as, to:

- ❖ Detect missile launch,
- ❖ Detect and track aircraft, ships, and vehicles,
- ❖ Perform non cooperative target identification and combat assessment, and
- ❖ Detect and Track fallout from nuclear detonations.

Often, the above contributions are the first indicators of potential hostile activities.

The MASINT systems most familiar on today’s battlefield are employed by ground surveillance and chemical, biological, radiological, and nuclear (CBRN) reconnaissance elements. Measurement and signature intelligence systems span the entire electromagnetic spectrum and its capabilities complement the other intelligence disciplines. Measurement and signature intelligence systems provide, to varying degrees, the capability to:

- ❖ Use automatic target recognition and aided target recognition.
- ❖ Penetrate manmade and/or natural camouflage.
- ❖ Penetrate manmade and/or natural cover, including the ability to detect subterranean anomalies or targets.
- ❖ Counter stealth technology.
- ❖ Detect recently placed mines.
- ❖ Detect natural or manmade environmental disturbances in the earth’s surface not discernible through other intelligence means.
- ❖ Provide signatures (target identification), to munitions and sensors.
- ❖ Enhance passive identification of friend or foe.
- ❖ Detect the presence of CBRNE agents including before, during, or after employment.
- ❖ Detect signature anomalies that might affect target - sensing systems.

2.4.1 The Six Sub - categories within MASINT.

There are six sub – categories (based on the technical means), within measurement and signature intelligence and we are going to describe them at the next paragraphs:

1. **Radar:** The active or passive collection of energy reflected from a target or object by line of sight, biostatic, or over – the – horizon radar systems. Radar – derived collection provides information on radar cross – sections, tracking, precise spatial measurements of components, motion and radar reflectance, and absorption characteristics for dynamic targets and objectives. A side - looking airborne radar system, coupled with advanced MASINT processing techniques:

- 1.1 Provides a high resolution, day – and – night collection capability.

- 1.2 Can produce a variety of intelligence products that identify or provide direction change detection, terrain mapping, underwater obstacles, dynamic sensing of targets in clutter, and radar cross - section signature measurements.

2. **Radio frequency:** The collection, processing, and exploitation of electromagnetic emissions from a radio frequency emitter, radio frequency weapon, radio frequency weapon precursor, or a radio frequency weapon simulator, collateral signals from other weapons, weapon precursors, or weapon simulators (for example, electromagnetic pulse signals associated with nuclear bursts), and spurious or unintentional signals.

- 2.1 **Electromagnetic pulses:** Measurable bursts of energy from a rapid change in a material or medium, resulting in an explosive force, produces radio frequency emissions. The radio frequency pulse emissions associated with nuclear testing, advanced technology devices, power and propulsion systems, or other impulsive events can be used to detect, locate, identify, characterize, and target threats or objects in general.

- 2.2 **Unintentional radiation:** The integration and specialized application of MASINT techniques against unintentional radiation sources that are incidental to the radio frequency propagation and operating characteristics of military and civil engines, power sources, weapons systems, electronic systems, machinery, equipment, or instruments. These techniques may be valuable in detecting, tracking, and monitoring a variety of activities of interest.

3. **Electro-optical:** The collection, processing, exploitation, and analysis of emitted or reflected energy across the optical portion (ultraviolet, visible, and infrared), of the electromagnetic spectrum. MASINT electro – optical capabilities provide detailed information on the radiant intensities, dynamic motion, spectral and spatial characteristics, and the material composition of a target. Electro – optical data collection has broad application to a variety of military, civil, economic, and environmental targets. Electro – optical sensor devices include radiometers, spectrometers, non literal imaging systems, lasers, or laser detection and ranging systems such as:

- 3.1 **Infrared:** A subcategory of electro – optical that includes data collection across the infrared portion of the electromagnetic spectrum where spectral and thermal properties are measured.

- 3.2 **LASER:** Integration and specialized application of MASINT electro – optical and other collection to gather data on laser systems. The focus of the collection is on laser detection, laser threat warning, and precise measurement of the frequencies, power levels, wave propagation, determination of power source, and other technical and operating

characteristics associated with laser systems, strategic and tactical weapons, range finders, and illuminators.

3.3 Hyperspectral imagery: A subcategory of intelligence derived from electro - optical sensors resulting from reflected or emitted energy in the visible and infrared spectrum used to improve target detection, discrimination, and recognition. Hyperspectral imagery can detect specific types of foliage (supporting drug - crop identification, disturbed soil), supporting the identification of mass graves, minefields, caches, underground facilities or cut foliage, and variances in soil, foliage, and hydrologic features, often supporting CBRNE contaminant detection.

3.4 Spectroradiometric products: Products that include electro – optical spectral (frequency), and radiometric (energy), measurements. A spectral plot represents radiant intensity versus wavelength at an instant in time. The number of spectral bands in a sensor system determines the amount of detail that can be collected about the source of the object being viewed. Sensor systems range from multispectral, (2 to 100 bands), to hyperspectral, (100 to 1,000 bands), to ultraspectral, (1,000+ bands). More bands provide more discrete information or greater resolution. The characteristic emission and absorption spectra serve to signature or define the makeup of the feature that was observed. A radiometric plot represents the radiant intensity versus time. An example we can use the radiant intensity plot of a missile exhaust plume while the missile is in flight, the intensity or brightness of the object is a function of several conditions including: temperature, surface properties or material, and how fast it is moving. For each point along a time – intensity radiometric plot, a spectral plot can be generated based on the number of spectral bands in the collector.

4. Geophysical: Geophysical measurement and signature intelligence involves detection of phenomena which are transmitted through the earth (ground, water, atmosphere, etc) and manmade structures including emitted or reflected sounds, pressure waves, vibrations, and magnetic field or ionosphere disturbances. Unattended ground sensors (UGS) are an example of geophysical sensors:

4.1 Seismic: The passive collection and measurement of seismic waves or vibrations in the earth's surface.

4.2 Acoustic: The collection of passive or active emitted or reflected sounds, pressure waves, or vibrations in the atmosphere or in the water. Water-based systems detect, identify, and track ships and submersibles operating in the ocean.

4.3 Magnetic: The collection of detectable magnetic field anomalies in the earth's magnetic field (land and sea). Magnetic sensors have the capability to detect – indicate the presence and travel direction of an object which contains iron.

5. Nuclear radiation: The information derived from nuclear radiation and other physical phenomena associated with nuclear weapons, reactors, processes, materials, devices, and facilities. Nuclear monitoring can be done remotely or during onsite inspections of nuclear facilities. Data exploitation results in characterization of nuclear weapons, reactors, and materials. A number of systems detect and monitor the world for nuclear explosions, as well as nuclear materials production.

6. Materials: The collection, processing, and analysis of gas, liquid, or solid samples. Intelligence derived from materials is critical to collection against CBRNE warfare threats. It is also important in analyzing military and civil manufacturing activities, public health concerns, and environmental problems. Samples are both collected by automatic equipment, such as air

samplers or robots, and directly by human operators. Samples, once collected, may be rapidly characterized or undergo extensive forensic laboratory analysis to determine the identity and characteristics of the sources of the samples.

2.4.2 MASINT in the Intelligence Process.

The measurement and signature intelligence discipline has several unique considerations throughout the intelligence process consisting from four continuing activities and four intelligence process steps which are:

1. **Generate Intelligence Knowledge:** The intelligence officer/analyst section must research targets'/topics - subject characteristics and capabilities that may impact the employment and use of MASINT sensors utilizing all available data before conducting operations. Additionally, the intelligence officer/analyst section must collect any existing MASINT products and identify all units, organizations, and systems that may potentially answer the commander's/requestor requirements. National databases, combatant command databases and private companies databases may hold more recent or updated information that can help MASINT planners determine the most effective MASINT means of supporting the commander's/requestor requirements.
2. **Analyze:** The intelligence staff analyzes intelligence and information about the enemy's/competitors equipment, doctrine, tactics, techniques, and procedures. For example in a military service the intelligence officer and staff can develop and refine a collection strategy to maximize the use of their MASINT systems in order to answer - fill intelligence gaps using the above types of information, along with the knowledge of friendly force MASINT capabilities.
3. **Assess:** The primary goal of the MASINT assess continuing activity is to determine whether the results of MASINT collection and production meet the requirements of the unit's intelligence, surveillance, and reconnaissance (ISR) effort. MASINT producers must assess all facets of MASINT operations, (from receipt of the ISR task to the dissemination of MASINT), in an effort to determine the effectiveness of MASINT. An assessment of the friendly force's capabilities must be conducted to ensure the continued effectiveness of, or to improve upon MASINT collection. This assessment is not only directed at each MASINT asset individually but also at the supporting intelligence communications architecture and the unit's entire ISR effort. Additionally, the intelligence officer/analyst immediately assesses MASINT products upon receipt for accuracy and relevance. The intelligence officer/requestor must inform the MASINT producer/analyst of the extent to which the product answered the intelligence requirements. Providing feedback to the MASINT producer/analyst and collector helps to improve the effectiveness and efficiency of MASINT products.
4. **Disseminate:** MASINT of critical importance to the force, including answers to the priority intelligence requirements, is disseminated through the most expeditious means possible. For intelligence reach operations, MASINT products are available and disseminated in a variety of forms and formats. The requestor must ensure that the MASINT product can be transmitted and properly delivered through the available communications systems, satisfying and abiding to the appropriate security and classification level of the communications system.

The four intelligence process steps are the following:

1. **Plan:** Some measurement and signature intelligence sensors can provide extremely specific information about detected targets, objects or topics, whereas other sensors might only be capable of providing an indication that an “entity” or object was detected.

Additionally, there are varying capabilities of detection, identification, and classification among measurement and signature intelligence sensors. These varying capabilities require synchronizing the employment of MASINT sensors both within the MASINT discipline and within the ISR effort as a whole. Depending on the type of sensor employed, a given MASINT collection target or named area of interest might not necessarily receive continuous coverage, the time of coverage depends on the number and the priority of given targets, subjects or topics and the number and availability of measurement and signature intelligence means, sensors and assets. Another consideration when planning measurement and signature intelligence missions or operations is whether to use active, passive, or a combination of sensors, additionally personnel must be detailed to emplace the sensors (and retransmission systems, if necessary) and monitor sensor reports.

2. **Prepare:** The primary responsibilities of the intelligence officer/manager during the prepare step of the intelligence process for measurement and signature intelligence is to support the operations intelligence operators (intelligence staff in general), in identifying the best locations to emplace MASINT assets and also to ensure that the intelligence staff can receive and verify the information transmitted by those assets. Additionally, the intelligence officer/manager must ensure that required MASINT analytical assets and resources are prepared to provide support or are available through intelligence reach. Since MASINT products are not as well known as products from other intelligence disciplines, the intelligence officer/manager must be aware of the types of MASINT products available to support the operation, and then educate the rest of the intelligence unit’s staff on how to use those products. Lastly, the intelligence officer/manager must also ensure MASINT reporting and dissemination channels and procedures are in place and working properly and rehearsals are conducted with all pertinent MASINT elements to ensure interoperability.

3. **Collect:** MASINT provides information required to answer priority intelligence requirements and other intelligence requirements to support the ISR effort. To be effective, MASINT collection must be synchronized within its own discipline, and also synchronized and integrated into the unit’s overall ISR effort. MASINT sensors are employed throughout the full spectrum of operations from a variety of platforms: subsurface, ground, marine, and aerospace.

Measurement and signature intelligence involves huge volumes of data that have to be processed before beginning analysis and production. The process function regarding MASINT involves converting raw data into a form that is suitable for performing analysis and producing intelligence. MASINT processing can include relatively simple actions (such as converting an unattended ground sensors activation into a report), to a complex task (such as processing hyperspectral imagery into a report identifying the composition and concentrations of carcinogenic emissions from a factory).

4. **Produce:** Effective and timely measurement and signature intelligence requires personnel with diverse skill sets. The measurement and signature intelligence producer must ensure the MASINT product satisfies the associated intelligence requirements and the product is in the required format. The quality, fidelity, and timeliness of measurement and signature intelligence products highly depend upon the type of target, the subject or the given topic, the collection system, the system’s position in relation to the target and the weather, as well as the system operator’s ability to identify the appropriate threat activity. The objective of MASINT production is to develop reliable and useable products from all and for all source intelligence.

2.5 Signal Intelligence (SIGINT).

According to US Joint Publication JP 2-0 Joint Intelligence (2007), signals intelligence is:

“Intelligence derived from communications, electronic, and foreign instrumentation signals. Signals intelligence provides unique intelligence information, complements intelligence derived from other sources, and is often used for cueing other sensors to potential targets of interest.”

The discipline is subdivided into three subcategories:

1. **Communications intelligence (COMINT)**⁸³ : is technical information and intelligence derived from foreign communications by other than the intended recipients. COMINT includes cyber operations, which is gathering data from target or adversary automated information systems or networks. COMINT also may include imagery, when pictures or diagrams are encoded by a computer network or radio frequency method for storage and/or transmission. The imagery can be static or streaming.
2. **Electronic intelligence (ELINT)**⁸⁴ : is technical and geolocation intelligence derived from foreign non communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. ELINT consists of two subcategories which are:
 - 2.1 **Operational Electronic Intelligence (OPELINT)**: is concerned with operationally relevant information such as the location, movement, employment, tactics, and activity of foreign non communications emitters and their associated weapon systems.
 - 2.2 **Technical Electronic Intelligence (TECHELINT)**: is concerned with the technical aspects of foreign non communications emitters, such as signal characteristics, modes, functions, associations, capabilities, limitations, vulnerabilities, and technology levels.
3. **Foreign instrumentation signals intelligence (FISINT)**⁸⁵ : is technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non governmental aerospace, surface, and subsurface systems. Foreign instrumentation signals intelligence is a subcategory of signals intelligence and includes telemetry, beaconry, electronic interrogators, and video data links.
 - 3.1 **Telemetry signals intelligence**: is technical and intelligence information derived from the intercept, processing, and analysis of foreign telemetry. Telemetry signals intelligence is a critical source of performance information about foreign (friendly or hostile), missile systems, satellites and space vehicles, (both for/about governmental, non governmental and commercial agencies, services and organizations), during their development, testing and deploying them. TELINT is also an important part of national means of technical verification for arms control.

The role of Signals intelligence is to provide intelligence on threat capabilities, disposition, composition, and intentions. In addition, signals intelligence discipline provides targeting information for the delivery of lethal and nonlethal fires.

⁸³ US Joint Publication JP 2-0 Joint Intelligence (2007).

⁸⁴ US Joint publication JP 3-13.1 Joint Electronic Warfare (2007), US Field Manual FM 2-0 Intelligence, US Joint Publication JP 2-0 Joint Intelligence (2007).

⁸⁵ US Joint Publication JP 2-01, Joint and National Intelligence Support to Military Operations, US Field Manual FM 2-0 Intelligence.



Photo 5: RAF Menwith Hill, a large site in the United Kingdom, part of ECHELON and the UK - USA Agreement. (2005).



Photo 6: Satellite ground station of the Dutch Nationale SIGINT Organisatie (NSO), 2012.

2.5.1 Communication Intelligence (COMINT)⁸⁶.

Communications Intelligence is a sub – category of signals intelligence that engages in dealing with messages or voice information derived from the interception of foreign communications. It should be noted that COMINT is commonly referred to as SIGINT, which can cause confusion when talking about the broader intelligence disciplines. The US Joint Chiefs of Staff defines it as:

“Technical information and intelligence derived from foreign communications by other than the intended recipients⁸⁷”.

Communications Intelligence will reveal some or all of the following:

1. Who is transmitting,
2. Where they are located, and, if the transmitter is moving, the report may give a plot of the signal against location,
3. If known, the organizational function of the transmitter,
4. The time and duration of transmission, and the schedule if it is a periodic transmission,
5. The frequencies and other technical characteristics of their transmission,
6. If the transmission is encrypted or not, and if it can be decrypted. If it is possible to intercept either an originally transmitted clear text or obtain it through cryptanalysis, the language of the communication and a translation (when needed),
7. The addresses, if the signal is not a general broadcast and if addresses are retrievable from the message. These stations may also be COMINT (e.g., a confirmation of the message or a response message), ELINT (e.g., a navigation beacon being activated) or both. Rather than, or in addition to, an address or other identifier, there may be information on the location and signal characteristics of the responder.

2.5.1.1 Communications Intelligence Techniques.

The basic COMINT techniques are the ones described below:

- ❖ **Voice interception⁸⁸**: A basic COMINT technique is to listen for voice communications, usually over radio but possibly “leaking” from telephones or from wiretaps. If the voice communications are encrypted, the encryption first must be solved through a process of introelectric diagram in order to listen to the conversation, although traffic analysis⁸⁹ may give information simply because one station is sending to another in a radial pattern. It is important to check for various cross sections of conversation.

⁸⁶ http://en.wikipedia.org/wiki/Signals_intelligence_COMINT.

⁸⁷ US Department of Defense (12 July 2007): Joint Publication 1-02 Department of Defence Dictionary of Military and Associated Terms (PDF).

⁸⁸ The interceptor must understand the language being spoken. In the Second World War, the United States used volunteer communicators known as code talkers, who used languages such as Navajo, Comanche and Choctaw, which would be understood by few people, even in the U.S., who did not grow up speaking the language. Even within these uncommon languages, the code talkers used specialized codes, so a “butterfly” might be a specific Japanese aircraft. British forces made more limited use of Welsh speakers for the additional protection. (http://en.wikipedia.org/wiki/Signals_intelligence_COMINT.)

⁸⁹ Traffic analysis is the discipline of drawing patterns from information flow among a set of senders and receivers, whether those senders and receivers are designated by location determined through direction finding, by addressee and sender identifications in the message, or even MASINT techniques for “fingerprinting” transmitters or operators. Message content, other than the sender and receiver, is not necessary to do traffic analysis, although more information can be helpful. (http://en.wikipedia.org/wiki/Signals_intelligence_Traffic_Analysis.)

- ❖ **Text interception:** Not all communication is in voice form. At the beginning of the 19th century Morse code interception was very important, the next few years the technological development has made the Morse code telegraphy obsolete and gradually led to the non-use of telegraphy, although it is possible that the Morse code is still used by Special Operations Forces (SOF). However, technological development led those types of forces to develop and use portable cryptographic and encryption equipment. Although Morse code is still in use by military forces of former Soviet Union countries. Nowadays, the transmission of written messages and information is through electronic mail or facsimile, so specially trained staff is scanning radio frequencies for character sequences like the ones described above.
- ❖ **Signalling channel interception:** A simple digital communication link can carry thousands or millions of voice communications, (especially in the more developed western countries). With the appropriate equipment its easy to identify which channel contains which conversation, (when the first thing intercepted is the signalling channel that carries information to set up telephone calls). Many governmental agencies, services, and bureaus can contact Retrospective Analysis of telephone calls through Call Detail Records (CDR), which are used for billing the calls.

2.5.1.2 Communications Security Measures.

Monitoring friendly communications: Within the jurisdiction of Signals intelligence units is the responsibility of monitoring one's own communications or other electronic emissions, for national security reasons (in order to avoid providing intelligence to the enemy). For example, when the operator of a security monitor might take notice of an “individual” transmitting inappropriate information over an unencrypted radio network, or someone who is not authorized for the type of information being given, then the monitor operator will call out one of the BEADWINDOW codes⁹⁰ used by Australia, Canada, New Zealand, the United Kingdom, the United States, and other nations working under their procedures. Standard BEADWINDOW codes (e.g., “BEADWINDOW 2”) include:

1. **Position:** (e.g., disclosing, in an insecure or inappropriate way, “Friendly or enemy position, movement or intended movement, position, course, speed, altitude or destination or any air, sea or ground element, unit or force”.
2. **Capabilities:** “Friendly or enemy capabilities or limitations. Force compositions or significant casualties to special equipment, weapons systems, sensors, units or personnel. Percentages of fuel or ammunition remaining”.
3. **Operations:** “Friendly or enemy operation – intentions progress, or results. Operational or logistic intentions; mission participants flying programmes; mission situation reports; results of friendly or enemy operations; assault objectives”.
4. **Electronic warfare (EW):** “Friendly or enemy electronic warfare (EW) or emanations control (EMCON) intentions, progress, or results. Intention to employ electronic countermeasures (ECM), results of friendly or enemy ECM, ECM objectives, results of friendly or enemy electronic counter – countermeasures (ECCM), results of electronic support measures/tactical SIGINT (ESM), present or intended EMCON policy, equipment affected by EMCON policy”.

⁹⁰ Combined Communications-Electronics Board (CCEB) (January 1987). "ACP 124(D) Communications Instructions: Radio Telegraph Procedure", http://en.wikipedia.org/wiki/Signals_intelligence_References.

5. **Friendly or enemy key personnel:** “Movement or identity of friendly or enemy officers, visitors, commanders; movement of key maintenance personnel indicating equipment limitations”.
6. **Communications security (COMSEC):** “Friendly or enemy COMSEC breaches. Linkage of codes or codeword’s with plain language; compromise of changing frequencies or linkage with line number/circuit designators; linkage of changing call signs with previous call signs or units; compromise of encrypted/classified call signs; incorrect authentication procedure”.
7. **Wrong circuit:** “Inappropriate transmission. Information requested, transmitted or about to be transmitted which should not be passed on the subject circuit because it either requires greater security protection or it is not appropriate to the purpose for which the circuit is provided”.
8. Other codes as appropriate for the situation may be defined by the commander.

For example in World War II the Japanese Navy made possible the interception and death of the Combined Fleet commander, Admiral Isoroku Yamamoto, by BEADWINDOW 5 and 7 violations, they managed to identify a “key person’s” movement over a low – security cryptosystem.

2.5.2 Electronic Signals Intelligence (ELINT).

Electronic signals intelligence (ELINT), refers to intelligence - gathering by use of electronic sensors. Its primary focus lies on non communications signals intelligence. According to USA Joint Chiefs of Staff ELINT is defined as:

“Technical and geolocation intelligence derived from foreign non communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources⁹¹”.

Another definition of ELINT is the one given by Richard L. Bernard⁹² which defines ELINT as:

“ELINT is information derived primarily from electronic signals that do not contain speech or text”.

Signal identification is performed by analyzing the collected parameters of a specific signal, and either matching it to known criteria, or recording it as a possible new emitter. ELINT data are highly classified, and are protected and handled as such.

The data gathered are typically pertinent to the electronics of an opponent's defensive network, especially the electronic parts such as radars, surface-to-air missile systems, aircrafts, etc. ELINT can be used to detect ships and aircraft by their radar emissions or other electromagnetic radiation, electronic signals intelligence can be collected by a variety of platforms such as: ground stations, specially equipped vehicles, ships, aircrafts, or by satellite.

⁹¹ US Department of Defense (12 July 2007). “Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms”.

⁹² Electronic Intelligence (ELINT) At NSA, Center for Cryptology History, National Security Agency, 2009.



Photo 7: “STONEHOUSE”, Deep Space Facility (Now closed)⁹³.

Perhaps the most common area of ELINT techniques application is the one known as “Air Warfare⁹⁴”. Air Warfare consists of techniques designed for unknown radar area detection, radar intercepting (by jamming or destroying), and learning their operating characteristics and procedures. The attacking air forces can avoid over flight of areas covered by radars or knowing the enemy’s radar locations and characteristics, a pack of electronic warfare units might jam⁹⁵ or destroy those radars moments before the impending attack.

Knowing the exact positions of the enemies’ radars, surface-to-air missile and anti-aircraft artillery systems (both types and characteristics, fixed or mobile), air raids can be plotted to avoid the most heavily defended areas or to fly on a flight profile which will give the attacking aircrafts the best chance of evading ground fire and enemy fighter patrols.

⁹³ Electronic Intelligence (ELINT) At NSA, Center for Cryptology History, National Security Agency, 2009.

⁹⁴ Air Warfare is the use of military aircraft and other flying machines in warfare, including military airlift of cargo according to the national interests. Strategic air power is the bombing of enemy resources (by bombers), tactical air power is the battle for control of the air space (by fighters), close air support is the direct support of ground units, naval aviation refers especially to the use of aircraft carriers.

⁹⁵ Confusing radar electronically is called a “soft kill”, but military units will also use specialized missiles in order to destroy radars, or bomb them, to get a “hard kill”. Some modern air to air missiles also have radar homing guidance systems, particularly for use against large airborne radars.



Photo 8: Modified RC-135U advanced ELINT airborne collection platform⁹⁶.

2.5.3 Foreign Instrumentation Signals Intelligence (FISINT).

Foreign Instrumentation Signals Intelligence⁹⁷ is intelligence from the interception of foreign electromagnetic emissions associated with the testing and operational deployment of foreign aerospace, surface, and subsurface systems. Typical examples of such communication include:

- Telemetry data (TELINT): Missiles, satellites, and other remotely – monitored devices often transmit streams of data concerning their location, speed, engine status and other metrics.
- Video data links: These may be from UAVs or from satellites used for reconnaissance.

Another definition of FISINT is the following one⁹⁸:

“A subcategory of signals intelligence, consisting of technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of a foreign countries aerospace, surface, and subsurface systems. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links”.

It should be noted at this point that the use of techniques, procedures and technical means that described in this chapter is very specialized and in more extensive use by governmental agencies, services, and organizations. At the private sector, those techniques, procedures and technical means are used by non – governmental services, organizations and commercial companies with a very specialized research, development and implementation, and if they have acquired specific

⁹⁶ Electronic Intelligence (ELINT) At NSA, Center for Cryptology History, National Security Agency, 2009.

⁹⁷ <http://en.wikipedia.org/wiki/FISINT>.

⁹⁸ USA Joint Publication 1-02 Department of Defense: Dictionary of Military and Associated Terms.

prerequisites and licensing. Their use by individuals liable to be considered as espionage with all this implies.



Photo 9: Cold War ELINT signals analysis equipment set operated at NSA⁹⁹.

2.6 Legal Aspects.

Inadequate and inconsistent with the legislative framework (both national and international), usage of the above disciplines and their techniques by both governmental and non governmental organizations, agencies, services and commercial companies or even by individuals can lead both to legal complexities and ethical issues and completely change the topic we are examining.

Espionage is a crime under the legislative framework of many nations, the risks taken by a spy vary:

- ❖ A spy breaking the host country's laws may be deported, imprisoned, or even executed (especially during a war or a military conflict), a summary execution may well be the penalty.
- ❖ A spy breaking his/her own country's laws can be imprisoned for espionage or/and treason, or even executed.

At the United States legislative framework¹⁰⁰, treason, espionage, and spying are separate crimes, the former two of which have graduated punishment levels, the latter for which death is a mandatory sentence.

At the following paragraphs we are going to examine Espionage and Propaganda which are two subjects directly connected with our main topic.

⁹⁹ Electronic Intelligence (ELINT) At NSA, Center for Cryptology History, National Security Agency, 2009.

¹⁰⁰ The United States in World War I passed the Espionage Act of 1917. Over the years many spies, such as the Soble spy ring, Robert Lee Johnson, the Rosenberg ring, Aldrich Hazen Ames, Robert Philip Hanssen,[†] Jonathan Pollard, John Anthony Walker, James Hall III, and others have been prosecuted under this law.

2.6.1 Espionage a Historical Approach.

Espionage or spying involves a government or individual obtaining information considered secret or confidential without the permission of the holder (of the information), using clandestine or covert action techniques. Espionage is inherently clandestine, as it is taken for granted that it is unwelcome and, in many cases illegal and punishable by law. It is a subset of intelligence gathering which otherwise may be conducted from public sources and using perfectly legal and ethical means. It is crucial to distinguish espionage from intelligence gathering, as the latter does not necessarily involve espionage, but often collates open – source information. However we can mention that “successful” espionage always produces intelligence.

There is a variety of documented events involving espionage throughout the history of men kind. At the ancient Chinese and Indian military archives, writings from strategists such as Sun-Tzu and Chanakya contain information on deception and subversion. Chanakya's student Chandragupta Maurya, founder of the Maurya Empire in India, made use of assassinations, spies and secret agents, which are described in Chanakya's “Arthasastra”. The ancient Egyptians had a thoroughly developed system for the acquisition of intelligence, and the Hebrews used spies as well, as in the story of Rahab, spies were also prevalent in the Greek and Roman empires¹⁰¹. During the 13th and 14th centuries, the Mongols relied heavily on espionage in their conquests in Asia and Europe. Aztecs used Pochtecas, people in charge of commerce, as spies and diplomats, and had diplomatic immunity. The Cold War involved intense espionage activity between two poles, the first was the United States and its allies and the second one was the Soviet Union - China and their allies, particularly related to nuclear weapons secrets. Different intelligence services value certain intelligence collection techniques over others. For instance the former Soviet Union services and organizations preferred human sources (HUMINT), over research in open sources, while the United States has tended to emphasize in technological methods such as SIGINT and IMINT.

2.6.2 Defining the Term.

Black's Law Dictionary (1990) defines espionage as:

“Gathering, transmitting, or losing...information related to national defense”.

In the UK, (under the 1911 Act), a person commits the offence of “spying” if he for any purpose prejudicial to the safety or interests of the State:

- approaches, inspects, passes over or is in the neighbourhood of, or enters any prohibited place,
- makes any sketch, plan, model, or note which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy, or
- obtains, collects, records, or publishes, or communicates to any other person any secret official word code, or password, or any sketch, plan, model, article, or note, or other document which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy¹⁰².

The offence of spying covers all such acts committed by any person within Her Majesty's dominions, and such acts committed elsewhere by British Officers or subjects. It is not necessary for the person concerned to have been warned beforehand that they were subject to the Official Secrets Act. The

¹⁰¹ “Espionage in Ancient Rome”, <http://en.wikipedia.org/wiki/Espionage>.

¹⁰² Note: “an enemy” apparently means a potential enemy, so could theoretically include all foreign governments.

1920 Act creates further offences of doing any “act preparatory” to spying, or of soliciting, inciting, seeking to persuade, or aiding and abetting any other person to commit spying¹⁰³.

The USA defines espionage towards itself as:

“The act of obtaining, delivering, transmitting, communicating, or receiving information relevant to national defence, with an intent, (or reason to believe), that the information may be used to harm (in any way), the United States or to the advantage of any foreign country - nation. Espionage is a violation of 18 United States Code 792-798 and Article 106, Uniform Code of Military Justice¹⁰⁴”.

Espionage is usually part of an institutional effort (i.e., governmental or corporate espionage), and the term is most readily associated with state spying on potential or actual enemies, primarily for military purposes, but this has been extended to spying involving corporations, known specifically as “Industrial Espionage”. Many nations routinely spy on both their enemies and allies, although they maintain a policy of not making comment on this. In addition to utilizing government agencies within the state many governments hire private intelligence companies to collect information on their behalf.

2.6.3 Potential “Targets” of Espionage.

There is a variety in the classification of espionage targets:

- ❖ **Natural resources:** strategic production identification and assessment (food, energy, materials, etc). Agents are usually found among bureaucrats who administer these resources in their own countries.
- ❖ **Popular sentiment:** towards domestic and foreign policies (popular, middle class, elites, etc). Agents often recruited from field journalistic crews, exchange postgraduate students and sociologists.
- ❖ **Strategical and economical strengths:** production, research, manufacture, infrastructure, technological aspects, etc. Agents recruited from scientific and technological academia, commercial enterprises, and more rarely from among military technologists.
- ❖ **Military capabilities:**
 - Intelligence field: offensive, defensive, manoeuvre, naval, air, space, etc.
 - Organizational, tactical and strategical field.

Agents are trained by special military – espionage agencies and services, and posted to an area of operation – interest with covert identities.

- ❖ **Counterintelligence:** Operations specifically targeting opponents' intelligence services themselves, such as breaching confidentiality of communications, and recruiting defectors or moles.

¹⁰³ UK Security Service (MI5): “Espionage and the Law”.

¹⁰⁴ US Department of Defense (12-07-2007): “Joint Publication 1-02, Department of Defense: Dictionary of Military and Associated Terms”.

2.6.4 Organization and Types of Espionage Agents.

One of the main purpose of intelligence organizations is to “penetrate” a “target” with an agent or a network of agents (within the United States Intelligence Community, the term “asset” is in more common use). By definition, an “agent” acts on behalf of someone else, (whether someone else is an individual, an organization, or a foreign government). The agent can be a citizen of one country who is recruited by a second country to spy or in general work against his own country or a third country. Agents can be considered either witting or unwitting, and in some cases, willing or unwilling. Agents typically work under the direction of a principal agent or a case officer. When agents work alone, and are not members of an agent network, they are known as “singletons”. Such agents/assets can either infiltrate the target, or be recruited “in place”. The “managers” of those agents are known as Intelligence Officers, Intelligence Operatives or Case Officers¹⁰⁵ and they are specially trained employees of an intelligence organization, service or agency (and might have diplomatic status, for example official cover or non-official cover), the CO is also capable of managing principal agents and intelligence agents network¹⁰⁶. Within the CO responsibilities are also:

- ❖ Spotting of potential - capable agents,
- ❖ Recruiting prospective – potential agents, (which is considered an art form, and it is the Raison d'être¹⁰⁷ of the intelligence case officer), and
- ❖ Train agents in the appropriate procedures and tradecrafts¹⁰⁸ (intelligence gathering methods, communications, avoiding detection methods from host nation counter – intelligence organizations and agents.

The management procedure in the intelligence community is known as Agent Handling. An agent's network is organized in a Clandestine Cell system or structure, which is an organizational method for organizing a group of people in such a way that it can more effectively resist penetration by an opposing organization, service or agency. Depending on the group's philosophy, its operational area, available communication technologies (and in use), and the nature of their mission, it can range from a strict hierarchy to an extremely distributed organization.

¹⁰⁵ For our study we are going to use the third term.

¹⁰⁶ Thefreedictionary.com

¹⁰⁷ The claimed reason for the existence of something or someone, the sole or ultimate purpose of something or someone, (literally “reason to be”). [http://en.wiktionary.org/wiki/raison d'être](http://en.wiktionary.org/wiki/raison_d'être).

¹⁰⁸ Agent training often includes techniques of tradecraft such as clandestine communications, including cryptography, the use of one-time pads, the construction and deployment of concealment devices, and the employment of dead drops. Other elements of tradecraft include elicitation, surveillance and counter surveillance, photography and the emplacement of audio devices, sensors, or other type of transmitting and receiving devices. Case officers generally train agents one at a time, in isolation, including only those elements of tradecraft needed to penetrate a specific target. Case officers will also teach agents how to develop cover for status, and cover for action, meaning how to establish credible pretexts for their presence and behaviour while engaged in intelligence collection activities. A well-trained and competent agent can conduct his or her clandestine tasks while under close surveillance, and still evade detection. More advanced agent training can include resistance to interrogation.

There are several types of agents, those are the following:

1. **A Penetration Agent**¹⁰⁹ also called **Deep Covert Agent**, or **Mole**¹¹⁰: is a long-term spy who is recruited before he has access to secret intelligence, and subsequently works his way into the target organization¹¹¹. However it is popularly used to mean any long-term clandestine spy or informant within an organization, (governmental or private). Perhaps the most famous example of moles was the “Cambridge Five”, five upper-class British men recruited by the KGB as left-wing students at Cambridge University in the 1930s who later rose to high levels in various parts of the British government¹¹². By contrast, most espionage agents, such as CIA Director of Counterintelligence Aldrich Ames and FBI agent Robert Hanssen who spied on the US government for the KGB, are either recruited or offer their services as spies after they are positioned at the targeted organization. Because their recruitment occurred in the remote past, moles are difficult for a nation's security services to detect¹¹³. The possibility that a top politician, corporate executive, government minister, or officer in an intelligence service could be a mole working for a foreign government is the worst nightmare of counterintelligence services.
2. **A Defector Agent**: who is recruited after he/she gets access to intelligence/secrets and then left his/her country.

2.1 **A Defector in Place Agent**: who is recruited after he/she gets access to intelligence/secrets but don't leave his/her country.

3. **Double agent**: is a person engaged in clandestine activities for two intelligence or security services (or more in joint operations), who provides information about one or about each to the other, and who wittingly withholds significant information from one on the instructions of the other or is unwittingly manipulated by one so that significant facts are withheld from the adversary. Peddlers, fabricators, and others who work for themselves rather than a service are not double agents because they are not agents. The fact that doubles have an agent relationship with both sides distinguishes them from penetrations, which normally are placed with the target service in a staff or officer capacity. The double agent usually has knowledge of both

¹⁰⁹ Smith, W. Thomas (2003): “Encyclopedia of the Central Intelligence Agency”, New York City, USA, Infobase Publishing.

¹¹⁰ The term was introduced to the public by British spy novelist John Le Carré in his 1974 novel “Tinker, Tailor, Soldier, Spy” and has since entered general usage, but its origin is unclear, as well as to what extent it was used by intelligence services before it became popularized.

¹¹¹ US Military Intelligence Handbook, Vol. 1, International Business Publications, 7 February 2007, Washington, USA,

¹¹² Carlisle, Rodney P. (2003): “Complete Idiot's Guide to Spies and Espionage”, Indianapolis – Indiana, USA, Alpha Books.

¹¹³ The most common procedure used by intelligence services to recruit agents is to find the location within the foreign government or organization of the information they want (the target), find out which people have access to it, and attempt to recruit one of them as a spy (*agent*) to obtain the information. However, the people with access to top secret government information, government employees with high security clearances, are carefully monitored by the government's security apparatus for just this sort of espionage approach, so it is difficult for a representative of the foreign intelligence service to meet with them clandestinely to recruit them. Private organizations such as large corporations or terrorist groups have similar security monitors. In addition, the security clearance process weeds out employees who are openly disgruntled, ideologically disaffected, or otherwise have motives for betraying their country, so persons in these positions are likely to reject recruitment as spies. For these reasons, some intelligence services have tried to reverse the above process, and recruit potential agents first, and have them conceal their allegiance, and pursue careers in the target government agency in hopes that they can reach positions of access to desired information. Because the spy career of a mole is such a long-term one, sometimes occupying a majority of a lifetime, persons who become moles must be highly motivated. One common motivation is ideology (political convictions). During the Cold War a major source of moles in Western countries was so-called “fellow travellers”, Western citizens who in their youth in the 1920s to 1940s became disaffected with their own governments and sympathetic to world Communism without actually joining the Communist party.

intelligence services and can identify operational techniques of both, thus making third party recruitment difficult or impossible.

3.1 **Re-doubled agent:** an agent who gets caught as a double agent and is forced to mislead the foreign intelligence service.

3.2 **Unwitting double agent:** an agent who offers or is forced to recruit as a double or re-doubled agent and in the process is recruited by either a third party intelligence service or his own government without the knowledge of the intended target intelligence service or the agent. This can be useful in capturing important information from an agent that is attempting to seek allegiance with another country.

3.3 **Triple agent:** an agent who works for three intelligence services.

4. **Intelligence agent:** provides access to sensitive information through the use of special privileges. If used in corporate intelligence gathering, this may include gathering information of a corporate business venture or stock portfolio. In economic intelligence, “Economic Analysts may use their specialized skills to analyze and interpret economic trends and developments, assess and track foreign financial activities, and develop new econometric and modelling methodologies”. This may also include information on trade or tariff.
5. **Access agent:** provides access to other potential agents by providing profiling information that can lead to recruitment into an intelligence service.
6. **Agent of influence:** someone who might provide political influence in an area of interest or might even provide publications needed to further an intelligence service agenda. I.e. The use of the media to print a story to mislead a foreign service into action, exposing their operations while under surveillance.
7. **Agent provocateur:** this type of agent instigates trouble, or may provide information to gather as many people as possible into one location for an arrest.
8. **Facilities agent:** a facilities agent may provide access to buildings such as garages or offices used for staging operations, resupply, etc.
9. **Principal agent:** this type of agent functions as a handler for an established agent’s network.
10. **Confusion agent:** may provide misleading information to an enemy intelligence service or attempt to discredit the operations of the target in an operation.
11. **Sleeper agent:** is a person who is recruited to an intelligence service to wake up and perform a specific set of tasks or functions while living under cover in an area of interest. This type of agent is not the same as a deep cover operative, who continually contacts a case officer to file intelligence reports. A sleeper agent is not in contact with anyone until he has been activated.
12. **Illegal agent:** This is a person who is living in another country under false credentials that does not report to a local station. A non official cover operative is a type of cover used by an intelligence operative and can be dubbed an “Illegal”¹¹⁴ when working in another country without diplomatic protection.

¹¹⁴ Mi5.gov -How spies operate.

Spies could easily be used to spread disinformation in the organization in which they are planted, such as giving false reports about their country's military movements, or about a competing company's ability to bring a product to market. They can also be used in other ways which also require infiltration, such as sabotage.

It is an open secret that all Countries are spying on both their enemies and their allies, but it is common practice and policy to deny it categorically. Governments and all types of organizations (both national and non-national), also employ private companies to collect information on their behalf.

2.6.5 Industrial Espionage.

Industrial espionage, (also known as economic espionage or corporate espionage), has a long history through ages, as an example we can refer to the work of Father Francois Xavier d'Entrecolles¹¹⁵ (1712-1722), when he was in Jingdezhen, China, to reveal the manufacturing methods of making the famous Chinese porcelain¹¹⁶. The Federal Bureau of Investigation estimates that U.S. Corporations lose \$100 Billion annually due to industrial espionage¹¹⁷.

Industrial espionage is a form or a subcategory of espionage conducted for commercial purposes. Economic espionage is conducted by governments and it has a widely international scope, while industrial or corporate espionage is more often national and occurs between competitive companies or corporations¹¹⁸. Economic or industrial espionage is a threat to any business whose livelihood depends on information. In our days, economic or industrial espionage has taken an expanded definition:

“The theft of trade secrets by the removal, copying or recording of confidential or valuable information from a company for use by a competitor¹¹⁹”.

“The stealing of technological or commercial research data, blueprints, plans, etc., by a person in the hire of a competing company or corporation¹²⁰”.

“The attempt of obtaining trade secrets or any type of classified information by dishonest or illegal means and methods such as: telephone or computer-tapping, infiltration of a competitor's workforce, etc¹²¹”.

The purpose of espionage is to gather information which with the proper elaboration (intelligence cycle), can be converted into knowledge, about a company, a group of companies, or an organization(s). It might include the acquisition of intellectual property, such as information on industrial manufacture, ideas, techniques and processes, recipes, formulas and new innovative products. It could also include sequestration of proprietary or operational information, such as, customer datasets, pricing, sales, marketing, research and development, policies, prospective bids, planning or marketing strategies or the changing compositions and locations of production¹²². It might

¹¹⁵ Francois Xavier d'Entrecolles (1664 Lyon–1741 Beijing): D'Entrecolles entered the Society of Jesus in 1682, he arrived in China in 1698 to become a member of the Jesuit China missions. Initially proselytizing in Jiangxi, he then became Superior General of the French Jesuits in China from 1706 to 1719. D'Entrecolles was then Superior of the French Residence in Beijing from 1722 to 1732.

¹¹⁶ Rowe, William & Brook, Timothy (2009): “China's Last Empire: The Great Qing”, The Belknap Press of Harvard University Press, Cambridge.

¹¹⁷ <http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper040/WINKLER.PDF>

¹¹⁸ Naseri, Hedieh (2005): “Economic Espionage and Industrial Spying”, Cambridge: Cambridge University Press, page: 10.

¹¹⁹ <http://www.investopedia.com/terms/i/industrial-espionage>.

¹²⁰ <http://dictionary.reference.com/browse/industrial+espionage>.

¹²¹ <http://dictionary.reference.com/browse/industrial+espionage>.

¹²² Naseri, Hedieh (2005): “Economic Espionage and Industrial Spying”, Cambridge: Cambridge University Press, page: 72.

describe as well activities such as theft of trade secrets, bribery, blackmail and technological surveillance. Industrial espionage (with the “form” of economic espionage), could also target

governmental organizations or companies (for instance: to determine the terms of a tender for a government contract so that another tendered can underbid). The types of companies that can be targeted and be subjected to corporate espionage are truly inexhaustible, but not limited to the following:

- ❖ Computer software and hardware development companies or corporations.
- ❖ Biotechnology companies or corporations.
- ❖ Nanotechnology companies or corporations.
- ❖ Pharmaceutical companies or corporations.
- ❖ Aerospace and naval development products companies or corporations.
- ❖ Telecommunications companies or corporations.
- ❖ Companies or corporations whom are operating in the energy sector – field and so on.

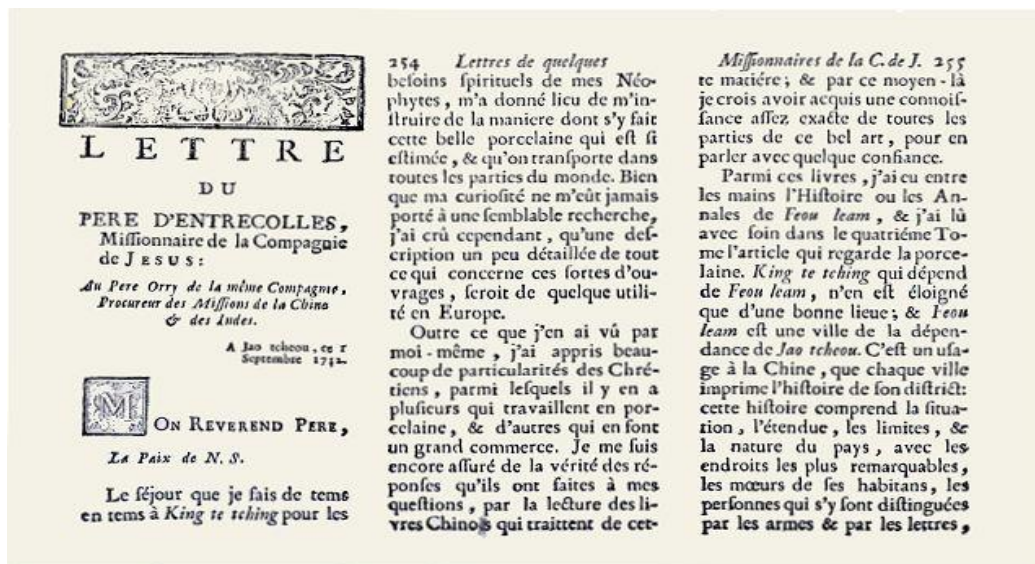


Photo 10: Section of the letter from Entrecolles, 1712, re-published by Jean-Baptiste du Halde in 1735.

Industrial espionage commonly occurs in one of the following described ways (depends and based on the type of the corporate spies, infiltrators or hackers):

- If the corporate spy, infiltrator or hacker is an insider¹²³: Insiders are usually employees such as: executives, managers, IT personnel, contractors (programmers, network penetrator or computer auditors), engineers, or janitors who have legitimate reasons to access facilities, data, computers or networks. Insiders have immediate access to enormous amounts of valuable or even classified company information and can misuse their privileges or impersonate someone else with higher privileges to do the job for them. The basic reasons or motives for insiders to “sell out” their company to a competition are: lack of loyalty, disgruntled,

¹²³ A frequently quoted statistic states that employees commit 85% of corporate espionage crimes.

boredom, mischievousness, blackmail, and most importantly, money. Trusted insiders are generally considered the best sources to contact industrial and economical espionage¹²⁴, historically are known as “patsy”. A very characteristically example of an “insider” is one dissatisfied employee who appropriates information to advance his/her own interests or in order to revenge the company he/she tries to damage the company by “selling” classified information to a competitor or a foreign government which seeks information to advance its own technological or financial interest¹²⁵. An also frequently occurring practice is when individuals leave their company to take up employment with another and take sensitive or classified information with them. Such apparent behaviour has been the focus of numerous industrial espionage cases that have resulted in legal battles.

- If the corporate spy, infiltrator or hacker is an outsider: Outsiders are those who entered the company from outside (physical brake in), they can also infiltrate a company by using the Internet, dial-up lines or to use a companies partner, (vendor, customer, or reseller), network that is linked to the targeted company’s network¹²⁶. A very characteristically example of an “outsider” is the one known as “kite”¹²⁷. Kite is a special type of an outsider, he/she is an expendable contractor. A kite provides his/her clients with actionable intelligence that they either don’t know how to get or they don’t want to get caught collecting it themselves. A kite also provides plausible deniability to his/her clients. If a covert operation is discovered and there is litigation or a criminal charge, the hiring company can deny all responsibility by denying all knowledge of the kite’s actions¹²⁸, the company can claim ignorance by demonstrating in court that the “consultant” had signed a contract saying that he would abide by all ethical rules, and that the company had no idea what the “consultant” was doing¹²⁹.
- Another commonly used method by some countries is to hire individuals to do the “dirty work” rather than make use of their own intelligence agencies, services or organizations¹³⁰. Academics, business delegates and students are often thought to be utilized by governments in gathering information¹³¹.

As a conclusion we can state that a potential spy could be anyone, an engineer, a maintenance man, a cleaner, an insurance salesman or an inspector - basically anyone who has legitimate access to the premises of a company or a corporation.

The legal process of collecting and gathering business intelligence is known as “Competitive Intelligence” and it describes the legal and ethical activities of systematically collecting, gathering, analyzing and managing information on industrial competitors¹³². This process includes activities such as examining newspaper articles, corporate publications, websites, patent filings, specialised databases, information at trade shows and exhibitions to determine information about a corporation¹³³.

¹²⁴ Nasheri, Hedieh (2005): “Economic Espionage and Industrial Spying”, Cambridge: Cambridge University Press, pages: 80 - 81.

¹²⁵ Nasheri, Hedieh (2005): “Economic Espionage and Industrial Spying”, Cambridge: Cambridge University Press, page: 07.

¹²⁶ <http://www.commondreams.org/views01/0306-03.htm>.

¹²⁷ Kitesurfing or kiteboarding (or abbreviated as kite): is a surface water sport combining aspects of wakeboarding, windsurfing, surfing, paragliding, and gymnastics into one extreme sport. A kitesurfer or kiteboarder harnesses the power of the wind with a large controllable power kite to be propelled across the water on a kiteboard similar to a wakeboard or a small surfboard, with or without foot-straps or bindings. The terms kiteboarding and kitesurfing are interchangeable.

¹²⁸ Like cutting the string to a kite and letting it fly away by itself.

¹²⁹ <http://www.commondreams.org/views01/0306-03.htm>.

¹³⁰ Nasheri, Hedieh (2005): “Economic Espionage and Industrial Spying”, Cambridge: Cambridge University Press, page: 80.

¹³¹ Nasheri, Hedieh (2005): “Economic Espionage and Industrial Spying”, Cambridge: Cambridge University Press, page: 88.

¹³² Nasheri, Hedieh (2005): “Economic Espionage and Industrial Spying”, Cambridge: Cambridge University Press, page: 73.

¹³³ Nasheri, Hedieh (2005): “Economic Espionage and Industrial Spying”, Cambridge: Cambridge University Press, page: 74.

The compilation of these crucial elements is sometimes termed as Competitive Intelligence Solution (CIS) or as Competitive Response Solution (CRS). Competitive Intelligence has its roots in market research and it has been described as the:

“Application of principles and practices from military and national intelligence to the domain of global business¹³⁴”.

It is also known as the business equivalent of open-source intelligence. The difference between Competitive Intelligence and industrial espionage is not clear. To be able to understand those differences we must first understand the legislative frameworks governing CI and IE in order to recognize how and where to draw the line between those two¹³⁵.

2.6.5.1 Industrial Espionage Tools and Methods.

In our days it is a global phenomenon that more and more companies (regardless of the industry in which they operate), are trying to create a more “relaxed” work environment for their employees. In their effort to do so, they succumb ostensibly and according to statistical studies to a fatal mistake, to relax (or in the worst cases to abstain), the minimum necessary security measures, both physical presence (security officers and personnel), and technical means (such as cameras, access control systems, IT security systems, etc). The lack of skilled personnel, technical means and safety procedures and unnecessary training and education of the other corporate personnel in security issues (such as: management and protection of important documents and information), allows an attacker to use a variety of techniques to gain access to vital information concerning the company.

Some of those methods include: physically removing the hard disk drive and copying the information to another machine, hacking, dumpster diving, social engineering, bribery, hiring away key employees, and the list is virtually limitless. In the following sections we will try to describe some of those tools and methods.

2.6.5.2 Hacking.

Rapid technological development and the increasing use of computers, computer networks and the Internet has expanded enormously the range and detail of information available and the ease of access for the purpose of industrial espionage. Worldwide, around 50,000 companies per day are thought to become victims of cyber attacks, with the rate estimated as doubling each year.

So the first method we are going to talk about is Hacking, which is considered one of the top three methods for obtaining trade secrets, and it is continually increasing in popularity. There are two main reasons why hacking is on the rise:

1. The wide availability of hacking tools. Currently, there are over 100,000 websites that offer free hacking tools.
2. Hacking is relatively easy to do. There are tools available that aren't require special knowledge or skills (such as: protocols or IP addressing), they are almost as easy as simply point and click.

¹³⁴ Walker Nick (1996): “Marketing: Know your enemy”. The Independent, http://en.wikipedia.org/wiki/Industrial_espionage.

¹³⁵ “The Economic Espionage Act: The Rules Have Not Changed, Competitive Intelligence Review”, July/August 1998, “Competitive Intelligence, Law, and Ethics: The Economic Espionage Act Revisited Again”, July/September 2011.

Hacking method can be broken up into three subcategories which are:

1. **System hacking:** assumes that the attacker has already access to a low level or to a privilege user account on the system. If the system does not have the latest security patches and the appropriate security settings, there is a big chance that the attacker will be able to use a known exploit to gain administrative privileges.
2. **Remote hacking:** involves an attacker who attempts to penetrate a system remotely across the network or Internet. The attacker usually begins with no special privileges, and tries to obtain higher level or administrative access. There are several forms of this type of hacking:

2.1 Unexpected input,

2.2 Buffer overflows,

2.3 Default configurations, and

2.4 Poor system administrator practices.

3. **Physical hacking:** requires that the attacker is going to penetrate a facility. Once inside, the intruder can easily:

- Roam the building searching for a vacant office or unsecured workstation with an employee's login name and password lying around,
- Search for memos or unused letterhead, and then insert the fake documents into the corporate mail system,
- Attempt to gain physical access to a server or telephone room in order to gain more information on the systems in use,
- Look for remote access equipment and note any telephone numbers written on the wall jacks,
- Place a protocol analyzer in a wiring closet to capture data, user names, and Passwords,
- Steal targeted information or hardware containing targeted information,
- Attach a hardware keystroke logger between the keyboard cable and the keyboard port on a user's workstation. Hardware keystroke loggers do not require drivers, uses no system resources, works on all PC operating systems, installs in seconds, and they do not send alerts to administrators. However, they do record a user's keystrokes character by character until the logger is disabled. When a password is entered, the logger allows access to the recorded keystrokes.⁷ Keystroke loggers have recording capabilities ranging in sizes from 8k (8,000 keystrokes) to 64k (more than 65,000 keystrokes). A keystroke logger can be used to record:

1. E-mail compositions,

2. Instant Messaging,

3. Chat room activity,

4. Web URL's,
5. User names and passwords and
6. Anything else a user types.

2.6.5.3 Social Engineering – Social Media.

Social engineering is another popular method of obtaining valuable corporate information. Social Engineering is the attempt of tricking a person (a company employee in our case), into revealing his/her password or other valuable or even classified corporate information. In general the basic goals of social engineering are the same as hacking, to gain unauthorized access to:

- Corporate computer network or systems in general,
- Classified or valuable corporate information,

In order to commit:

- Fraud,
- Network intrusion,
- Industrial or economical espionage,
- Identity theft, or
- Simply to disrupt the company's computer system or network.

Even conversations with unsuspecting relatives of company's employees have become an conventional tool in corporate espionage.

Some of the techniques which are used in social engineering are:

1. A potential hacker is sending an email claiming to be a system administrator. The hacker will claim to need user's password for some important system administration work, and ask the user to email it to him/her. A hacker will usually send this email to all the users of a system, with the hope that one or two users will fall for the trick.
2. Another common social engineering technique is "shoulder surfing", someone looking over an employee's shoulder while he or she types in a password.
3. Password guessing is an additional easy social engineering technique. If a person (a potential attacker/hacker), can find out personal type of information things about someone, (an employee), he/she can usually take advantage and use that information to guess a password.

Such passwords can be the names of his/her children, wife or husband, their birthdays and anniversaries or the social security number.

2.6.5.4 Dumpster Diving.

Dumpster diving is a messy, but a very successful technique for acquiring corporate or company information (such as: trade secrets or other valuable information). No matter how disgusting it may be dumpster diving is legal. Once trash is discarded onto a public street or alley, it is considered fair game. According to the law if trashes are left to be accessed by commercial carters, then it is no longer private property. It is only private property if there is a “no trespassing” sign and you have to trespass to get into the dumpster¹³⁶.

According to LAN Times the following items are listed as potential security leaks in corporate trash:

- Company phone books: can give to a hacker names and numbers of people to target and impersonate.
- Organizational charts: contain information about people who hold positions of authority within the organization.
- All type of memos: provide small amounts of useful information for creating authentic looking fake memos.
- Company policy manuals: can reveal to potential hackers how secure or insecure a company really is.
- Calendars of meetings, events and vacations: can inform an attacker which employees are out of town at a certain time.
- System manuals, sensitive data or other sources of technical information: might give to a hacker the exact information he/she needs to access the corporate network.
- Print outs of sensitive data or login names and passwords,
- Printouts of source code, disks and tapes,
- Company letterhead and memo forms, and last but not least
- Out dated hardware: Discarded hardware, particularly computers with hard drives, can be restored to provide all sorts of useful information¹³⁷.

2.6.5.5 Whacking.

Basically, whacking is another term which is used instead of wireless hacking. To eavesdrop on a wireless networks, all an intruder needs is the right kind of radio, and to be within range of a wireless transmission. With the wide usage of 802.11b devices, it is possible to pick up signals from outside an office building. Once tapped into a wireless network, an intruder can easily access anything on both the wired and wireless networks, because the data sent over networks is usually unencrypted.

If a company is not using wireless networking, an attacker can pose as a janitor and insert a rogue wireless access node into a supposedly secure hard – wired network. Once the wireless access point is installed, an intruder can safely sit outside an office building with a laptop and a wireless network interface controller and leisurely sniff and explore a company’s network looking for weaknesses and information to exploit. If the wireless access point is discovered, it will most likely be mistaken for a hub or Jet direct box.

¹³⁶ <http://www.commondreams.org/views01/0306-03.htm>.

¹³⁷ http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html.

2.6.5.6 Phone Eavesdropping .

Eavesdropping on phone transmissions is another used method to commit corporate or company espionage. A person with a digital recording device can monitor a FAX line and record a FAX transmission or reception. By playing the recording back into a modified Group III¹³⁸ or Group IV¹³⁹ FAX machine, an intruder can reproduce an exact copy of a message without anyone's knowledge. Even without monitoring a FAX line, a FAX sent to a "communal" FAX machine can easily be read or copied before it is picked up from the incoming FAX basket for delivery to the intended recipient.

Another way is by picking up an extension or by tapping a telephone, it is possible to record the tones that represent someone's account number and password using a tape recorder. The tape recording could be replayed over the telephone to gain access to someone else's account.

2.6.6 Industrial Espionage Intelligence Objectives.

Perhaps the major question that should worry those who, (generally), deal with information security and combat corporate espionage, (particular), is "What types of information do corporate spies seek". Basically any digital or hardcopy data can be valuable to competitors. Gathering as much information as possible provides to the competitor the ability to form a complete point of view about a firm's actions, plans, operations and strategies. Ultimately, the goal is to out manoeuvre a company and gain a competitive advantage. At the following paragraph we will describe some of those potential information targets competitor seeks:

- Marketing used techniques, methods and plans.
- Marketing, advertising and packaging expenditures.
- Product research and development, plans and budgets¹⁴⁰.
- New product or a service cost of employment.
- Pricing issues, strategies, and lists.
- Source codes¹⁴¹.
- Company Websites.
- Corporate strategies.
- Manufacturing and technological techniques, methods and operations.

¹³⁸ Group 2 faxes conform to the ITU-T Recommendations T.30 and T.3. Group 2 faxes take three minutes to transmit a single page, with a vertical resolution of 96 scan lines per inch. Group 2 fax machines are almost obsolete, and are no longer manufactured. Group 2 fax machines can interoperate with Group 3 fax machines.

¹³⁹ Group 4 faxes conform to the ITU-T Recommendations T.563, T.503, T.521, T.6, T.62, T.70, T.72, T.411 to T.417. They are designed to operate over 64 kbit/s digital ISDN circuits. Their resolution is determined by the T.6 recommendation, which is a superset of the T.4 recommendation.

¹⁴⁰ Real example: On 14 June 1997, Hsu Kai-Lo and Chester H. Ho (naturalized US citizens) were arrested by the FBI for attempting to steal the formula for Taxol, a cancer drug patented and licensed by the Bristol-Myers Squibb (BMS) Company presumably on behalf of their employer, the Yuen Foong Paper Manufacturing Company of Taiwan. In July 1997 the two accused along with Jessica Chou (a Taiwan citizen actively involved in the attempted theft) were indicted on 11 counts including violations of 18 USC Section 1832. Chou remained in Taiwan and that nation refused to extradite Chou, http://www.mekabay.com/overviews/industrial_espionage.htm#_Toc187674946.

¹⁴¹ Real example: In July 2004, an Indian software engineer employed by a US company's software development center in India was accused of "zipping up" proprietary software source code for printing identification cards and uploading it to her personal e-mail account, http://www.mekabay.com/overviews/industrial_espionage.htm#_Toc187674946.

- Target markets and prospect information.
- Plant closures and development.
- Alliance and contract arrangements: delivery, pricing, terms.
- Customer and supplier information.
- Merger and acquisition plans.
- Financial information, revenues and budgets.
- Staffing, operations, org charts, wage/salary.

Besides proprietary company information, personnel records are also what we call “hot targets” for pilfering. Any of the following described information could be valuable to a potential competitor or to a hired (or individual working), spy:

- An employee’s home phone number and addresses.
- The names of an employee’s husband/wife or children.
- Employee’s salary.
- Social security number.
- Medical records.
- Credit records or credit union account information.
- Performance reviews.

2.6.7 Preventing Industrial Espionage Techniques and Methods.

As we have already sown the techniques and methods which are been used by industrial spies are the same as those used by traditional spies, so the measures that a company can take are equivalent to those which are used to prevent traditional espionage.

The basic idea is that companies should adopt the appropriate countermeasures that are justified by the potential losses that the company can suffer. According to conducted studies and statistical data, the survival rate of companies which have been victims of espionage (industrial or economical), is very small, this is due the percentage of losses (for most of them), might reach the amount of billions of dollars.

Therefore, each company should proceed in a coordinated effort to achieve information security, it should arrange for the design and adoption of an appropriate information security plan. This plan should include memoranda of actions (which will be followed by the employees), and the appropriate counter-measures which will have to deal with espionage. A comprehensive safety plan should make use of all the existing available means of protection, those means are: Technical, Operational, Physical, and Personnel Security, and we are going to present them at the following paragraphs.

2.6.7.1 Technical Security.

This term is used to identify all the technical means that are used for security reasons in general. In this paragraph (and for the main purpose of this paper), we are going to emphasize on the technical security systems and countermeasures which are used in order to reduce the vulnerabilities present in electronic systems. Those countermeasures should ensure the confidentiality, integrity, and availability of a company's computer systems and networks. A good technical security plan could also protect all the electronic systems of a company.

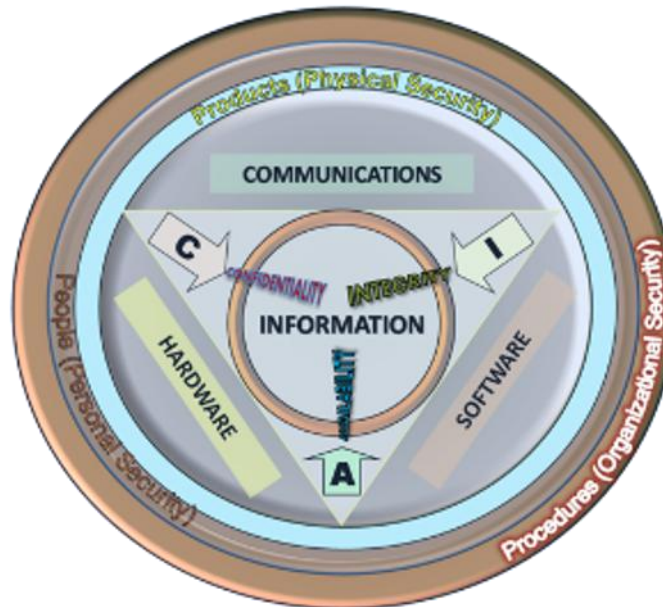


Table 13: Information Security Attributes: or qualities, i.e., Confidentiality, Integrity and Availability (CIA)¹⁴².

Those technical means are also known as Logical Controls, use software and data to monitor and control access to information, computing and network systems. For example: passwords, network and host based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls. An important logical control that is frequently overlooked is the principle of least privilege. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read Email and surf the Web. Violations of this principle can also occur when an individual collects additional access privileges over time. This happens when employees' job duties change, or they are promoted to a new position, or they transfer to another department. The access privileges required by their new duties are frequently added onto their already existing access privileges which may no longer be necessary or appropriate. It is also recommended that companies should also educate travelling executives who carry company's laptops about using those laptops after taking the appropriate precautions in order to prevent theft or possible communications interception.

¹⁴² Information Systems: are composed in three main portions, hardware, software and communications with the purpose to help identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational. Essentially, procedures or policies are implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organizations, http://en.wikipedia.org/wiki/Information_security.

Another recommended way to protect information is to use cryptographic means (both hardware and software). Information that has been encrypted (rendered unusable), can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage, encrypted information is unusable to someone who doesn't know the encryption key.

2.6.7.2 Operational Security.

Operational security examines the business processes and procedures used by a company and how those procedures are aligned with the need to protect migrant information and if not, how those processes and procedures could compromise information through non-technical means.

Those processes and procedures are known as Administrative controls, they are consisting of tested, proven and approved written policies, procedures, standards and guidelines that should be followed by all company's staff. These administrative procedures act as a framework for the proper operation of the business, the staff management and also the associates of the company. Administrative controls consists the base of the selection and implementation of logical and physical means and measures. Logical and physical means and measures are manifestations of administrative controls. Administrative controls are of paramount importance. Some of those Administrative controls are the ones, (and not limited to), described below:

- ❖ The known as "Need to know" policy¹⁴³: which is used to classify information and then provide access to them based on specific classification levels or ratings. Its based on the perception that all types of information are not equal and so different types of information requires different degree of protection, that's why, is necessary to assign a security classification. The first step in information classification is to develop and adapt a "classification policy". This policy should describe:
 - The different classification levels,
 - To define the criteria by which information is going to be assigned to a particular level,
 - List the required security controls for each classification,
 - To define (based on the classification levels), who is/are going to have access to the different levels of classification.

Some of the factors that define the classification levels and which type of information should be assigned – attached to those include factors such as: how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. The current legislative framework and other regulatory requirements are also important considerations when classifying information. The type and designation of the information classification levels is selected and used based on the nature of each organization, service or agency. Some examples of the classification levels that can be used are the following:

¹⁴³ This policy has been used by the US Department of Defense and familiar organizations, services and agencies.

- In the business sector (public or private), labels such as: Public, Sensitive, Private and Confidential.
- In the government sector, labels such as: Unclassified, Sensitive But Unclassified, Restricted, Confidential, Secret, Top Secret and their non-English equivalents.
- In cross sectoral formations, it can be used the Traffic Light Protocol, which consists of: White, Green, Amber, and Red.

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification levels should be reviewed periodically to ensure that the classification level is still appropriate for the information and to ensure the security controls required by the classification are in place. This policy helps the avoidance of unnecessary proliferation of information.

- ❖ The application of similar, (to that described above), policies tailored appropriately to contribute in some way to impose the restriction of using, (by employees), hotlines, such as Internet and other telephone systems, with the objective of reducing the chances of compromising information.
- ❖ The company's effort to convince (or enforcing, if necessary), vendors, external partners, suppliers and customers to adopt strict and if it is possible similar, (to the companies), measures and security policies. It would make no sense to perform background checks on your own computer systems, networks and employees, while contractor employees, who have free access to your facilities, go unchecked, or do not follow the prescribed procedures of the company.

Operational security is considered as a complex issue, therefore requires in-depth study of how a company is structured and organized. In this context, the respective company should examine all procedures which are used in each department and at every stage of the production process, depending on whether these procedures can be potential risks related to the protection of information.

Every company should invest in an appropriate educational program to raise awareness of employees in security issues, which will be the foundation for a strong and effective operational security program. This educational program should be structured in a way that makes company personnel capable of knowing both the ways and means which has at his disposal in order to protect corporate information. It is also considered self-evident that companies should encourage their staff to report any suspicious situations or conditions, and also know how and to whom they should report such things¹⁴⁴.

¹⁴⁴ Security administrators can not assume that all staff has the necessary knowledge to properly handle information security.

2.6.7.3 Physical Security.

As we have already told, a large number of industrial espionage incidents have been occurred due to simple breaking in a company and theft. Physical access to facilities (in general), and in the individual sections and general premises (in particular), of each company should be carefully regulated and controlled. It's considered crucial (for security reasons), that nobody should have a free roam in all corporate facilities.

This can be achieved through the adoption and installation of an access control system or by the adoption of a corporate policy that includes limiting the access both to visitors and contractors, as well as the companies' employees, the optimal security method is the combination of the above. Another issue that could be included in the category of physical security is the garbage control. There have been numerous of serious industrial espionage incidents that have occurred solely from the content of an organization's garbage¹⁴⁵.

In this category we can also integrate technical means such as: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc, which are used in order to monitor and control the access to and from the companies facilities.

Another important physical security procedure is the one known as "Separation of Duties". Separation of duties ensures that an individual can not perform and complete a critical task on his own. For example:

- ❖ An employee who works in the supply department of a company should not be able to order materials, to receive them, and also and record the expenses.
- ❖ An applications programmer should not also be the server administrator or the database administrator – these roles and responsibilities must be separated and performed by different employees of the companies IT department.

For the successful implementation of all the above described techniques and methods the key role will be the followed by the company policy and whether the company will be able to instill this policy to its staff.

2.6.7.4 Personnel Security.

Each and every organization and company should adopt a policy known as "Knowing the Employees". This policy consists of establishing procedures and processes with the use of which the company will be able to verify the backgrounds of current employees', new employee applicants or employees assigned to work on sensitive departments or projects. The term employee is used broadly and includes anyone (from executive and general managers to janitors, clerical workers, security guards and even cleaning staff), who has physical access to company facilities, departments, technical means or information. Unfortunately, many organizations and companies overlook the accessibility that the lowest, (in hierarchy), staff has in all company facilities and departments (and by extension to any type of information), in contrast to criminal elements which understand the potentials of low level positions. So, it is crucial for security managers to understand the risks associated with these perspectives and to take the appropriate respond countermeasures.

Responsible for cross-checking the backgrounds of employees (current, new employee applicants or external contractors), should be the companies "Information Office", (which administratively belongs to the companies "Security Office" and work in close cooperation with the

¹⁴⁵ U.S. Military organizations, services and agencies have several units devoted to "trash intelligence", and invest millions of dollars in the proper disposal of "classified waste". Private companies operating in sensitive sectors (such as: energy, aerospace technology, etc), have also invested significant amounts of money in the safe management of their wastes.

Human Resources department). By using the term background we are referring to any personal data that may relate to an employee such as name and surname, address, degrees, qualifications, expertise in a particular field, previous work experience, his/her habits, hobbies, etc.

The Human Resources department must also establish a close cooperation with the companies IT department, which should be informed about staff that will or has already left the company so that IT's system administrators could lock the accounts of departed employees on the day that they leave the company.

The measures that can be proposed and adopted are really unlimited, summarizing, we can claim that the most important role regarding whether the proposed security plans will prove successful or not mainly depends on two key factors:

- ❖ Security policy that will be decided and being adopted by the company or organization (and whether the company managed to keep this policy), and
- ❖ Continuing staff training and education in matters relating to the safety of information (and security and safety matters in general).

2.7 Propaganda.

We can trace primitive forms of propaganda as far back as reliable recorded evidence exists. The Behistun Inscription, (c. 515 BC), detailing the rise of Darius I to the Persian throne is viewed by most historians as one of the earliest examples of propaganda¹⁴⁶. As a term it started to gain currency in 1622, when a new branch of the Catholic Church was created, called the Congregatio de Propaganda Fide (Congregation for Propagating the Faith), or informally simply Propaganda¹⁴⁷. Its activity consisted in a group of cardinals pitching Catholicism in non Catholic countries. From the 1790s, the term began being used also for propaganda in secular activities. The term began taking a pejorative connotation in mid 19th century, when it was appropriated from religion to the political sphere. Its political use became particularly significant during World War I and culminated in the wars that followed, (World War II, Korean War, Vietnam, etc), gaining more and more importance to the attempt of manipulating public opinion (both the attacker and the defender).

When the term propaganda is literally translated from the Latin gerundive it means: "things that must be disseminated", although in some cultures the term is neutral or even positive, while in others the term has acquired a strong negative connotation. For instance, in Portuguese and generally Spanish language speaking countries, (particularly in the Southern Cone), the term "propaganda" is synonymous to "advertising" (as the most common manipulative technique used by the media). In English language, the term "propaganda" had originally a neutral denotation, considering the dissemination of information in favour of any given cause. However this changed during the 20th century, (because of the WW I and WW II¹⁴⁸), the term acquired a thoroughly negative meaning, mostly in western countries, representing the intentional dissemination of often false, but certainly "compelling" claims to support or justify political actions or ideologies. This redefinition arose because both the governments of the Soviet Union and Germany used propaganda both as a term and a process to justify and promote their ideologies (Communism and Nazism), in all forms of public expression. As these ideologies were repugnant to liberal western societies, the negative feelings towards those ideologies came to be projected to the word "propaganda" itself.

¹⁴⁶ Nagle D. Brendan and Stanley M Burstein: "The Ancient World: Readings in Social and Cultural History", Pearson Education, 2009, page: 133.

¹⁴⁷ Diggs-Brown, Barbara (2011): Strategic Public Relations: Audience Focused Practice, page: 48, <http://www.etymonline.com/index.php?term=propaganda>, <http://en.wikipedia.org/wiki/Propaganda>.

¹⁴⁸ This redefinition arose because both the Soviet Union's and Germany's government admitted explicitly to using the term propaganda favouring, respectively, communism and Nazism, in all forms of public expression. As these ideologies were repugnant to liberal western societies, the negative feelings toward them came to be projected into the word "propaganda" itself.

Defining the term “propaganda” has always been a problem, this is due the wide usage and applicability in many levels of social life (communicative, political, commercial, military, etc.). The main difficulties had to do with differentiating propaganda from other types of “persuasion methods”. Two of the most authoritative definitions of the term “propaganda” are those presented below:

“Propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behaviour to achieve a response that furthers the desired intent of the propagandist¹⁴⁹”.

Although more comprehensive is the definition given by Richard Alan Nelson:

“Propaganda is a systematic form of purposeful persuasion that attempts to influence the emotions, attitudes, opinions, and actions of specified target audiences for ideological, political or commercial purposes through the controlled transmission of one-sided messages (which may or may not be factual), via mass and direct media channels. A propaganda organization employs propagandists who engage in propagandism (which defined as the applied creation and distribution of such forms of persuasion)¹⁵⁰”.

Both of the above definitions are focused on the communicative process of propaganda and to be more precise, on the purpose of the communicative process, allowing propaganda to be considered objectively and then interpreted as positive or negative depending on the perspective of the viewer or the listener (a good example is Ernesto Che Guevara, who was presented both as a rebel and a freedom fighter and also as a bad communist and a terrorist¹⁵¹). For the purposes of this paper we will complement that propaganda has to do with the handling and presentation of information in a way that serves our purposes.

2.7.1 Types or Forms of Propaganda.

As we have already told propaganda could be found in various types and forms, although it is always in some form of “activated” ideology. Considering the source (which is transmitting the message), and also the nature of the message we can categorise propaganda at the following forms and types:

1. **White Propaganda**¹⁵²: comes from a source that can be easily – openly identified and the information contained in the message is considered as accurate. The techniques which are used in white propaganda are the milder methods of persuasion, such as standard public relations techniques and one – sided presentation of an argument. This is the type of propaganda that has been always used by the Radio Moscow during the Cold War era. Although what listeners hear is reasonably close or almost true, the message has been transmitted and presented in a way that attempts to convince the audience that the sender is the “good guy”, with the best ideas and political ideology. The purpose of white propaganda is to achieve – build credibility between the “sender” and the “receiver” (which is the audience), that’s the main reason that white propaganda could be useful at some point of time in the near future (for the sender).

¹⁴⁹ Garth Jowett and Victoria O'Donnell: “Propaganda and Persuasion”, 5th edition, Sage Publications, page: 7.

¹⁵⁰ Richard Alan Nelson: “A Chronology and Glossary of Propaganda in the United States”, 1996, pages: 232-233.

¹⁵¹ Ernesto “Che” Guevara (14 June 1928 – 9 October 1967): he was commonly known as el Che or simply Che, he was an Argentine Marxist revolutionary, physician, author, guerrilla leader, diplomat, and military theorist. A major figure of the Cuban Revolution, his stylized visage has become a ubiquitous countercultural symbol of rebellion and global insignia within popular culture. Time magazine named him one of the 100 most influential people of the 20th century, and also an Alberto Korda photograph of him entitled Guerrillero Heroico, was cited by the Maryland Institute College of Art as “the most famous photograph in the world”, while USA considered him responsible for the Cuban Missile Crisis.

¹⁵² <http://en.wikipedia.org/wiki/Propaganda>, Garth S. Jowett & Victoria O'Donnell: Propaganda & Persuasion, 4th edition.

2. **Black Propaganda**¹⁵³: when the source – sender is concealed or credited to a false – fake authority and spreads lies, fabrications and deceptions. Black propaganda is the “purest” form of “creative deceit”. The success or failure of black propaganda depends on the receivers’ willingness to accept both the credibility (of the source – sender), and the content of the transmitted message as true. Requires careful and expert handling on the part of the sender to succeed in harmonizing and placing the transmitted messages within the targeted audiences’ social culture, political beliefs and framework.

Prominent examples of black propaganda are incidents that occurred during the Second World War (from all the warring sides). The Germans considered as “Pioneers¹⁵⁴” in use of black propaganda, a known successful usage of black propaganda was during WWII and prior to Hitler’s planned invasion to Britain, the operation of a radio station known as “The New English Broadcasting Station”, whose program consisted of “war news”, and was run by discontented British. The station was broadcasting half hour programs throughout the day, opening with the song “Loch Lomond¹⁵⁵”, and closing with the “God save the King”. It turned out that the operation of the radio station was a German elaborate – undercover propaganda operation determined to reduce the morale of the British people during the Battle of Britain. The same technique was used to influence the French soldiers who were served at the Maginot Line (from autumn 1939 to spring 1940).

Black propaganda techniques are also used from allies in order to “target” friendly nations, a very characteristic example was the British intelligence propaganda operations, (during WW II), that aimed to manipulate USA in order to declare war at Germany two years before the Pearl Harbor Japanese attack. British Security Coordination settled in New York to contact covert black propaganda operations. The British activities were discovered after the Pearl Harbor attack and forced the US State Department to declare that: “British intelligence operations in America were out of control and demanded that offensive covert operations against the USA should end”.

2.1. **Disinformation**: A very commonly used synonym of the term propaganda is the word disinformation, the word disinformation is a cognate for the Russian word “dezinformatsia”, which in fact was the name of a KGB’s division devoted to covert black propaganda operations. A definition about disinformation is the following one (which has been given by Shults & Godson):

“False, incomplete or misleading information, that is passed, fed or confirmed to a targeted individual, group or country”.

Disinformation is always covert and includes false information, it consists of “made up” news stories deliberately designed to weaken adversaries and moved through newspapers and other media by journalists who are actually agents of a foreign country (friendly or hostile). One of the most characteristic examples of Russian disinformation campaigns was the one which targeted the USA as responsible for the production of the virus known as Acquired Immune Deficiency Syndrome (AIDS), in order to use it for Biological Warfare. The Russian “dezinformatsia”, division was able to channel the information and replicated by the news media of more than sixty countries all over the world.

Disinformation is based on the following communication process models:

¹⁵³ <http://en.wikipedia.org/wiki/Propaganda>, Garth S. Jowett & Victoria O’Donnell: Propaganda & Persuasion, 4th edition.

¹⁵⁴ Joseph Goebbels, who was Hitler’s Propaganda Minister proved a “Master” in that specific field of expertise.

¹⁵⁵ The original author of the song is unknown. One story is that the song was written by a Scottish soldier who awaited death in enemy captivity; in his final letter home, he wrote this song, portraying his home and how much he would miss it. Another tale is that during the 1745 Rebellion a soldier on his way back to Scotland during the 1745-1746 retreat from England wrote this song. The “low road” is a reference to the Celtic belief that if someone died away from his homeland, then the fairies would provide a route of this name for his soul to return home. Within this theory, it is possible that the soldier awaiting death may have been writing either to a friend who was allowed to live and return home, or to a lover back in Scotland.

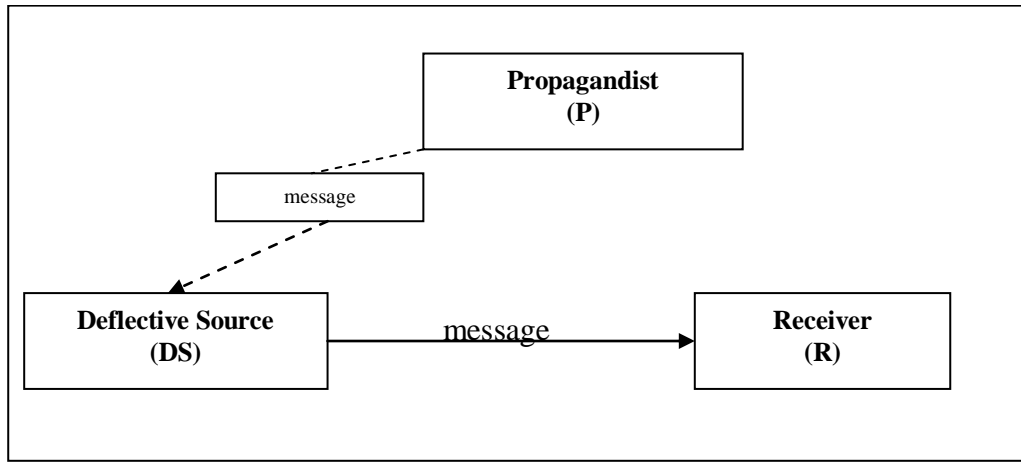


Diagram 7: Deflective Source Model¹⁵⁶.

As the above figure shown, the Propagandist (P), creates a Deflective Source (DS), and transmits the emitted message through this source, in this way the propagandist managed to present the Deflective Source as the apparent source of the transmitted message. The Receiver (R), perceives the information as a direct transmission of the DS and he can not (in any way), associate the message with the original transmitter which is the propagandist.

The second model is known as “Legitimizing Source Model” and is presented at the following figure:

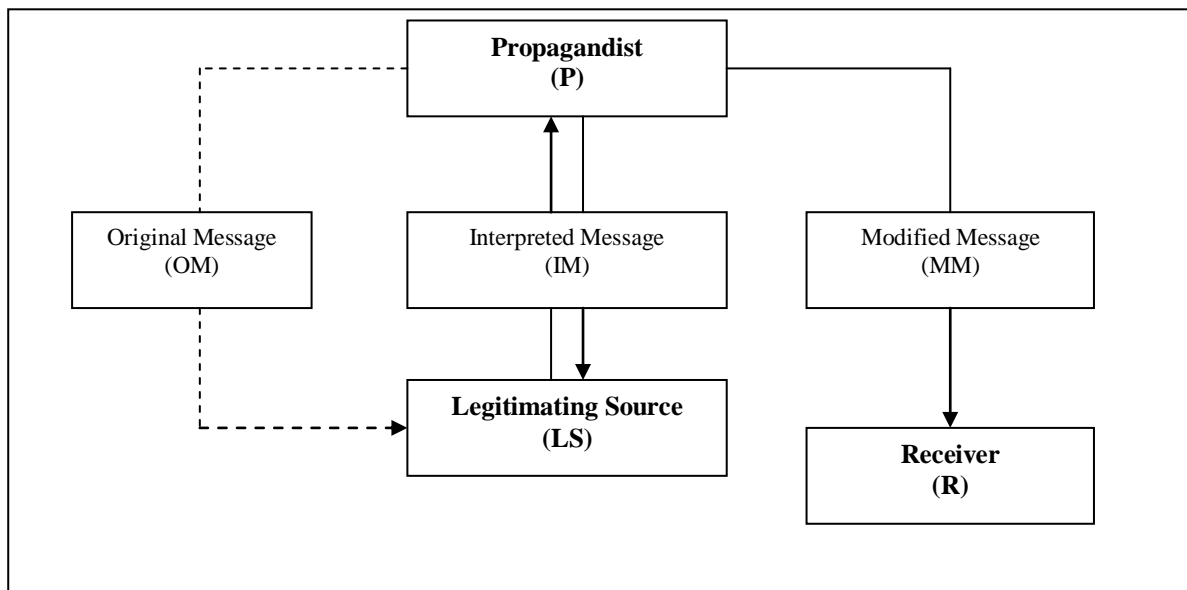


Diagram 8: Legitimizing Source Model¹⁵⁷.

Again as the above figure is shown The Legitimizing Source Model can be separated in three phases, those phases are:

1. The Propagandist (P), secretly channels – places the original message (OM), to a recognized and established Legitimizing Source (LS).
2. Then the Propagandist picks up the Interpreted, (by the LS), Message and
3. Transmits – communicates the Modified Message (MM) to the receiver (R) as a message - information that came from the LS.

¹⁵⁶ Garth Jowett and Victoria O'Donnell: “Propaganda and Persuasion”, 5th edition, Sage Publications.

¹⁵⁷ Garth Jowett and Victoria O'Donnell: “Propaganda and Persuasion”, 5th edition, Sage Publications.

Through the above process the propagandist manages to legitimate the transmitted message and at the same time dissociates him/her self from the message origination.

Considering the above two communication models we can conclude that in both models the propagandist's intention is to obscure the identity of the original message transmitter, thus creating a high degree of credibility for both the message and the apparent source.

Despite continuous denials of most major world powers increasing evidence indicates that disinformation is widely practiced and this reflects the reality of international politics.

In any case we must not confuse Disinformation with Misinformation. Misinformation is false or inaccurate information that is spread unintentionally. It is distinguished from disinformation by motive. Misinformation is simply erroneous, while disinformation, in contrast, is intended to mislead¹⁵⁸. When comparing misinformation to disinformation, Jurgen Habermas¹⁵⁹ says that the motives play an active role in the effect the information has. Misinformation may have a less devastating effect because readers can criticize what they have read and evaluate it as truth or fiction. Authors will also have to give reasoning for their beliefs and support their statements with facts¹⁶⁰.

3. **Gray propaganda:** this type of propaganda lays somewhere between white and black propaganda, the source may or may not be easily identified and the reliability of the message and the information contained in this is uncertain. A typical example of gray propaganda was the reaction attitude of the "VOA"¹⁶¹ in 1961, during the Gulf of Pigs invasion in Cuba. The "VOA" moved to the gray propaganda when preceded in denying any U.S. involvement in the CIA covert operations.

This type of propaganda is also used in order to embarrass a competitor or even an enemy, a typical example of this type of usage was when the Radio Moscow took advantage of John F. Kennedy¹⁶² and Martin Luther King Jr¹⁶³ assassinations to derogate the USA, VOA seized the opportunity and offer similar commentaries about the Russian invasion in Afghanistan and also the prosecutions and arrests of Jewish dissidents.

¹⁵⁸ Nel Francois: "Writing for the Media in Southern Africa", 2005, Oxford University Press. Page: 57.

¹⁵⁹ Jürgen Habermas: is a German (born 18 June of 1929), sociologist and a philosopher in the tradition of critical theory and pragmatism. He is perhaps best known for his theory on the concepts of communicative rationality and the public sphere. His work focuses on the foundations of social theory and epistemology, the analysis of advanced capitalistic societies and democracy, the rule of law in a critical social-evolutionary context, and contemporary politics, particularly German politics.

¹⁶⁰ Stahl Bernd: "On the Difference of Equality of Information, Misinformation, and Disinformation: A Critical Research Perspective", Informing Science 2006 pages: 83-96.

¹⁶¹ Voice of America (VOA): is the official external broadcast institution of the United States federal government. It is one of five civilian U.S. international broadcasters working under the umbrella of the Broadcasting Board of Governors (BBG). VOA provides a wide range of programming for broadcast on radio and TV and the Internet outside of the U.S. in 43 languages. VOA produces about 1,500 hours of news and feature programming each week for an estimated global audience of 123 million people. Its day-to-day operations are supported by the International Broadcasting Bureau (IBB).

¹⁶² John Fitzgerald "Jack" Kennedy (29 May 1917 – 22 November 1963): was the 35th President of the United States, serving from 1961 until his death in 1963. After military service as commander of the Motor Torpedo Boats PT-109 and PT-59 during World War II in the South Pacific, Kennedy represented Massachusetts' 11th congressional district in the U.S. House of Representatives from 1947 to 1953 as a Democrat. Thereafter, he served in the U.S. Senate from 1953 until 1960. Kennedy defeated Vice President and Republican candidate Richard Nixon in the 1960 U.S. presidential election. At 43 years of age, he is the youngest to have been elected to the office, the second-youngest President (after Theodore Roosevelt), and the first person born in the 20th century to serve as president.^[3] A Catholic, Kennedy is the only non-Protestant president, and is the only president to have won a Pulitzer Prize. Events during his presidency included the Bay of Pigs Invasion, the Cuban Missile Crisis, the building of the Berlin Wall, the Space Race, the African-American Civil Rights Movement, and early stages of the Vietnam War. Kennedy was assassinated on November 22, 1963 in Dallas, Texas.

¹⁶³ Martin Luther King, Jr. (15 January 1929 – 4 April 1968): was an American clergyman, activist, and leader in the African-American Civil Rights Movement. He is best known for his role in the advancement of civil rights using nonviolent civil disobedience. King has become a national icon in the history of American progressivism. On the 14 of October 1964, King received the Nobel Peace Prize for combating racial inequality through nonviolence. King was assassinated on the 4 April 1968, in Memphis, Tennessee. His death was followed by riots in many U.S. cities. King was posthumously awarded the Presidential Medal of Freedom and the Congressional Gold Medal. Martin Luther King, Jr. Day was established as a U.S. federal holiday in 1986. Hundreds of streets in the U.S. have been renamed in his honor. A memorial statue on the National Mall was opened to the public in 2011.

Planting stories in foreign newspapers (and media in general), has always been practiced by governmental organizations and services, since 1980 the phenomenon of planted stories appears to apply in the private sector too. The phenomenon consists of a growing usage of Video News Releases which were technically inserted in television news programs. This is categorized as gray propaganda because the original source of the envoy video was hidden and the video's credibility have been legitimized by the prestige of the news station (radio or television station), as a legitimating source.

In our days the usage and application of gray propaganda techniques has spread in a wide range of private sector aspects, such as:

- ❖ Companies that use gray propaganda techniques in order to distort statistics on annual reports,
- ❖ Advertisements which are used to promote specific products, highlighting only the advantages and concealing the possible disadvantages,
- ❖ Annual reports which are suggesting that a product will achieve results that it cannot achieve, and so on.

4. **Subpropaganda or Facilitative propaganda:** Leonard William Doob¹⁶⁴ suggested in 1948 that there is another dimension of propaganda and named this dimension "Subpropaganda". According to Doob in this form of propaganda the intention and propagandist's task is to spread an unknown doctrine, which to achieve, requires considerable time to build an adequate intellectual framework in the minds of the audience towards the acceptance of the unknown doctrine. At this form of propaganda in order to gain the attention and favor of the targeted audience the propagandist uses various stimuli, which are used to excite the attention of the public and the relevant codes and factors that mediate communication. To accomplish his/her task the propagandist might use "facilitative communication" techniques, those techniques most frequently take the form of financial aid, radio newscasts, books, magazines, etc. The above described techniques are designed and arranged in a way that is going to create a friendly atmosphere and attitude towards the potential propagandist and his/her interests. According to W. Phillips Davison¹⁶⁵ facilitative communication might not be propaganda but for sure is a communication strategy designed especially to render a positive and friendly attitude towards a potential propagandist. Davidson claimed that in 1969 there were 450 active registrations of agencies distributing propaganda and as he pointed out the most of them were occupied in fields such as tourism, investments and trade. A more modern example is the creation, (under the president's Clinton administration), of the Bureau of International Information Programs (BIIP). President Clinton himself claimed that "The BIIP is the most effective foreign policy tool we have". The Bureau's mission statement was to "inform, engage and influencing the international audiences in favor and advance of the U.S. global interests.

¹⁶⁴ Leonard William Doob (3 March 1909 – 29 March 2000): was the Sterling Professor Emeritus of Psychology at Yale University, he was also a pioneering figure in the fields of cognitive and social psychology, propaganda and communication studies, as well as in conflict resolution. He served as Director of Overseas Intelligence for the Office of War Information in World War II and also wrote several interesting works intersecting cognition, psychology and philosophy.

¹⁶⁵ W. Phillips Davison: was the sociologist who first articulated the third-person effect hypothesis in 1983, he explains that the phenomenon first piqued his interest in 1949 or 1950 upon learning of a Japanese attempt during World War II to dissuade black U.S. soldiers from fighting at Iwo Jima using propaganda. His third-person effect hypothesis predicts that people tend to perceive that mass communicated messages have a differential influence on themselves and others; additionally, because of this perception, people tend to take action to counteract the messages' influence. Specifically, the original hypothesis predicts that people tend to perceive that mass communicated messages have a greater influence on others than on themselves.

5. **Agitatsia**¹⁶⁶: the word comes from the Latin word *agitatio* (which means encouragement), so it is the mobilization of the masses, (many people with unitary behavior), using the appropriate cues, in order to achieve certain objectives of an organization or a party. The term was used primarily by parties with Marxist ideology and orientation. The agitation manifests itself in many ways, such as: rallies, gatherings, celebrations, etc. It must not be confused with the propaganda with which organizations or parties do not attempt to mobilize the masses, but merely seek to convince the correctness of their views. The propaganda is the first stage of the attempt to affect many people – an audience (in a massive way), followed by agitation, which is mainly mobilization through verbal and emotional stimuli.

As a conclusion we can claim that: “The use of propaganda is prevalent more than ever in our days, we can detect signs of its use in countries at war, differences between ethnic and religious groups and generally speaking at the struggle of the power conquest (in all its forms). This has been contributed by the rapid technological development, (communication networks have evolved and expanded greatly), making all kinds of information easily accessible and traded. The institutions of modern society, (governmental organizations - services and agencies, profit and non profit organizations, private organizations, business organizations and companies, religion, etc.), are still maintaining the need to manipulate human feelings and shape - affect minds and opinions.



Photo¹⁶⁷ & Posters¹⁶⁸: Which have been used for propagandistic reasons.

¹⁶⁶ The Greek word written with Latin characters, the English word is agitation.

¹⁶⁷ Northern propaganda in the American Civil War. A former slave showing keloid scars from whipping. This famous photo was distributed by abolitionists, <http://en.wikipedia.org/wiki/Propaganda>.

¹⁶⁸ World War I poster by Winsor McCay, urging Americans to buy Liberty Bonds, Propaganda poster (1876), to urge immigrants to move to California, <http://en.wikipedia.org/wiki/Propaganda>.

2.7.2 Propaganda Techniques and Methods¹⁶⁹.

Propaganda campaigns are organized based on a specific strategic communication plan, using the appropriate techniques, (of information transferring, communication and persuasion), in order to influence the targeted audience. A propaganda campaign can begin with a simple transmission, such as leaflets dropped from a plane or an advertisement poster or spot. Generally the initial broadcast messages will contain instructions - directions considering the way in which the message recipient will be able to obtain more information (this can be done via a web site, a hot line, radio, etc.). The communication plan of the propaganda campaign is divided into two phases:

- I. The first phase aims to alter the message recipient, from the contained in the message information recipient to information seeker.
- II. At the second phase, as the recipient has accepted the information as true, valid and reliable, (and consequently has also accepted the transmitted message as true), to become an opinion leader through indoctrination.

Some of the techniques which are used to generate propaganda are based on techniques that have been developed and tested through the research of social psychology (and other social sciences). Many of these used techniques can be characterized as “Logical Fallacies”, as the arguments used by propagandists might be persuasive but not necessarily true or valid. Trough out the years many studies - researches have been conducted in order to analyze the means and methods which have been used to transmit - spread propaganda messages, generally speaking we can claim that the transmission and dissemination information strategies alter to propaganda strategies only when coupled with propagandistic messages. The ability to detect these messages is a necessary prerequisite for anyone who wants to study the methods by which these types of messages are being transmitted or disseminated. At the following paragraph we are going to present the main techniques which are being used for generating propaganda:

Ad hominem : (it’s a Latin phrase which means “to the man” or “to the person¹⁷⁰”), the full phrase is “argumentum ad hominem”, and it means an argument made personally against an opponent instead of against their argument¹⁷¹. Ad hominem reasoning is normally described as an informal fallacy¹⁷², more precisely an irrelevance.

Ad nauseam¹⁷³ : is also known as argument from repetition or argumentum ad infinitum, its about an argument made repeatedly, (possibly by different people), until nobody cares to discuss it any more. This may sometimes, but not always, be a form of proof by assertion¹⁷⁴. We can also say that this argument approach uses tireless repetition of an idea. An idea, especially a simple slogan, that is repeated enough times, may begin to be taken as the truth. This approach works best when media sources are limited or controlled by the propagator.

¹⁶⁹ <http://en.wikipedia.org/wiki/Propaganda>.

¹⁷⁰ The Free Merriam - Webster Dictionary. Merriam-Webster, Incorporated.

¹⁷¹ www.answers.com. 02/04/2013.

¹⁷² Walton, Douglas: Informal Logic: A Pragmatic Approach, Cambridge University Press, 2008, page: 190.

Bowell Tracy & Kemp Gary: Critical Thinking: A Concise Guide, Abingdon, Oxon: Routledge, 2010, pages: 210–213.

¹⁷³ Definition by The American Heritage Dictionary.

¹⁷⁴ Proof by assertion: sometimes informally referred to as proof by repeated assertion, is an informal fallacy in which a proposition is repeatedly restated regardless of contradiction. Sometimes, this may be repeated until challenges dry up, at which point it is asserted as fact due to its not being contradicted (argumentum ad nauseam). In other cases, its repetition may be cited as evidence of its truth, in a variant of the appeal to authority or appeal to belief fallacies.

Appeal to authority: also known as: Argument from authority, (the Latin phrase is argumentum ad verecundiam), or authoritative argument, is an inductive-reasoning argument that often takes the form of a statistical syllogism¹⁷⁵. Although certain classes of argument from authority can constitute strong inductive arguments, the appeal to authority is often applied fallaciously: either the authority is not a subject-matter expert, or there is no consensus among experts in the subject matter, or both¹⁷⁶.

Appeal to fear: the Latin phrases are argumentum ad metum or argumentum in terrorem, is a fallacy in which a person attempts to create support for an idea by using deception and propaganda in attempts to increase fear and prejudice toward a competitor. The appeal to fear is common in marketing and politics.

Appeal to prejudice: Using loaded or emotive terms to attach value or moral goodness to believing the proposition. Used in biased or misleading ways.

Argumentum ad populum: its again a Latin phrase which means “appeal to the people”, it is a fallacious argument that concludes a proposition to be true because many or most people believe it. In other words, the basic idea of the argument is: “If many believe so, it is so”.

This type of argument is also known by several names, some of those are: appeal to the masses, appeal to belief, appeal to the majority, appeal to democracy, argument by consensus, consensus fallacy, authority of the many, and bandwagon fallacy, and in Latin as argumentum ad numerum (appeal to the number), and consensus gentium (agreement of the clans). It is also the basis of a number of social phenomena, including communal reinforcement and the bandwagon effect¹⁷⁷. The Chinese proverb “three men make a tiger” concerns the same idea.

Inevitable victory: Invites those not already on the bandwagon to join those already on the road to certain victory. Those already or at least partially on the bandwagon are reassured that staying aboard is their best course of action.

Join the crowd: This technique reinforces people's natural desire to be on the winning side. This technique is used to convince the audience that a program is an expression of an irresistible mass movement and that it is in their best interest to join.

The Lie: The repeated articulation of a complex of events that justify subsequent action. The descriptions of these events have elements of truth, and the "big lie" generalizations merge and eventually supplant the public's accurate perception of the underlying events. After World War I the German Stab in the back explanation of the cause of their defeat became a justification for Nazi re-militarization and revanchist aggression.

¹⁷⁵ http://en.wikipedia.org/wiki/Appeal_to_authority.

¹⁷⁶ http://en.wikipedia.org/wiki/Appeal_to_authority.

¹⁷⁷ The bandwagon effect is a well documented form of groupthink in behavioural science and has many applications. The general rule is that conduct or beliefs spread among people, as fads and trends clearly do, with “the probability of any individual adopting it increasing with the proportion that have already done so”. As more people come to believe in something, others also “hop on the bandwagon” regardless of the underlying evidence. The tendency to follow the actions or beliefs of others can occur because individuals directly prefer to conform, or because individuals derive information from others. Both explanations have been used for evidence of conformity in psychological experiments.

False dilemma: also called the fallacy of the false alternative, false dichotomy, **fallacy of false choice**, black-and/or-white thinking, or the fallacy of exhaustive hypotheses. It is a type of informal fallacy that involves a situation in which limited alternatives are considered, when in fact there is at least one additional option. The options may be a position that is between two extremes, (such as when there are shades of grey), or may be completely different alternatives. False dilemma can arise intentionally, when fallacy is used in an attempt to force a choice (such as, in some contexts, the assertion that “if you are not with us, you are against us”). But the fallacy can also arise simply by accidental omission of additional options rather than by deliberate deception. The opposite of this fallacy is argument to moderation.

Argument to moderation: the Latin phrase is: *argumentum ad temperantiam*, and it is also known as false compromise, gray fallacy and the golden mean fallacy, it is an informal fallacy which asserts that the truth can be found as a compromise between two opposite positions.

Classical conditioning, (also Pavlovian conditioning or respondent conditioning): All vertebrates, including humans, respond to classical conditioning. That is, if object A is always present when object B is present and object B causes a negative physical reaction (e.g., disgust, pleasure) then we will when presented with object A when object B is not present, we will experience the same feelings.

Cognitive dissonance: is the feeling of discomfort when simultaneously holding two or more conflicting cognitions: ideas, beliefs, values or emotional reactions. In a state of dissonance, people may sometimes feel “Disequilibrium”, which means: frustration, hunger, dread, guilt, anger, embarrassment, anxiety, etc. The phrase was coined by Leon Festinger in his 1956 book “When Prophecy Fails”. The theory of cognitive dissonance in social psychology proposes that people have a motivational drive to reduce dissonance by altering existing cognitions, adding new ones to create a consistent belief system, or alternatively by reducing the importance of any one of the dissonant elements. It is the distressing mental state that people feel when they “find themselves doing things that don't fit with what they know, or having opinions that do not fit with other opinions they hold”.

A key assumption is that people want their expectations to meet reality, creating a sense of equilibrium. Likewise, another assumption is that a person will avoid situations or information sources that give rise to feelings of uneasiness, or dissonance. Cognitive dissonance theory explains human behaviour by positing that people have a bias to seek consonance between their expectations and reality. According to Festinger, people engage in a process he termed “dissonance reduction”, which can be achieved in one of three ways: lowering the importance of one of the discordant factors, adding consonant elements, or changing one of the dissonant factors. Cognitive dissonance is one of the most influential and extensively studied theories in social psychology. An example: suppose a pollster finds that a certain group of people hates his candidate for senator but loves actor A. They use actor A's endorsement of their candidate to change people's minds because people cannot tolerate inconsistency. They are forced to either to dislike the actor or like the candidate.

Common man: also known as “The plain folks”, it's an approach that attempts to convince an audience that the propagandist's positions reflect the common sense of the people. It is designed to win the confidence of the audience by communicating in the common manner and style of the targeted audience. Propagandists use ordinary language and mannerisms, (and “clothe” their message in face-to-face and audiovisual communications), in attempting to identify their point of view with that of the average person. With the plain folk's device, the propagandist can win the confidence of persons who resent or distrust foreign sounding, intellectual speech, words, or mannerisms.

Cult of personality: As a term appeared in English around 1800-1850, along with the French and German usage. At first it had no political connotations but was instead closely related to the Romantic “cult of genius”. The political use of the phrase came first in 1877 by Karl Marx.¹⁷⁸ The term became more popular when used by Khrushchev's Secret Speech at 1956.

A cult of personality arises when an individual uses mass media, propaganda, or other methods, to create an idealized, heroic, and, at times god-like public image, often through unquestioning flattery and praise. Sociologist Max Weber developed a tripartite classification of authority, the cult of personality holds parallels with what Weber defined as “charismatic authority”. A cult of personality is similar to hero worship, except that it is established by mass media and propaganda. For example, modern propagandists hire popular personalities to promote their ideas and/or products.

Demonization¹⁷⁹ (of the opponent or the enemy): is sometimes used against what are arguably political opponents rather than religious ones¹⁸⁰. In colloquial usage, the term demonization is used metaphorically to refer to propaganda or moral panic directed against any individual or group. In other words, making individuals from the opposing nation, from a different ethnic group, or those who support the opposing viewpoint appear to be subhuman, (e.g., the Vietnam War-era term “Gooks” which had been used for National Front for the Liberation of South Vietnam soldiers), worthless, or immoral, through suggestion or false accusations.

Dictat: This technique hopes to simplify the decision making process by using images and words to tell the audience exactly what actions to take, eliminating any other possible choices. Authority figures can be used to give the order, overlapping it with the “Appeal to authority” technique, but not necessarily. A characteristic example of the above technique is The Uncle Sam “I want you” image.



Photo 11: Poster of The Uncle Sam “I want you”.

¹⁷⁸ Karl Marx, A letter to German political worker, Wilhelm Blos, 10 November 1877, http://en.wikipedia.org/wiki/Cult_of_personality

¹⁷⁹ Demonization is the reinterpretation of polytheistic deities as evil, lying demons by other religions, generally monotheistic and henotheistic ones. The term has since been expanded to refer to any characterization of individuals, groups, or political bodies as evil.

¹⁸⁰ The Templar Knights were destroyed by accusations that they worshipped Baphomet from King Philip the Fair. Baphomet, often thought to be Beelzebub, may have been used because of the likeness of this horned deity with the Christian images of Satan.

Door-in-the-face technique: is a compliance method commonly used to increase a person's latitude of acceptance. The persuader attempts to convince the respondent to comply by making a larger request that the respondent will most likely turn down, much like a metaphorical slamming of a door in the persuader's face. The respondent is then more likely to agree to a second, more reasonable request, compared to the same reasonable request made in isolation. For example, if a salesperson wants to sell an item for \$100 but the public is only willing to pay \$50, the salesperson first offers the item at a higher price (e.g., \$200) and subsequently reduces the price to \$100 to make it seem like a good deal.

Foot-in-the-door technique: (is the opposite of the above technique), in which a persuader begins with a small request and gradually increases the demands of each request.

Euphoria: The use of an event that generates euphoria or happiness, or using an appealing event to boost morale. Euphoria can be created by declaring a holiday, making luxury items available, or mounting a military parade with marching bands and patriotic messages.

Fear, uncertainty, and doubt: the term appeared for the first time back in the 1920s, a similar formulation "doubts fears and uncertainties" reaches back to 1965 and by 1975 the term was already appearing abbreviated as FUD in marketing and sales contexts. FUD is generally a strategic attempt to influence perception by disseminating negative and dubious or false information. An individual firm, for example, might use FUD to invite unfavourable opinions and speculation about a competitor's product, to increase the general estimation of switching costs among current customers, or to maintain leverage over a current business partner who could potentially become a rival.

Glittering generalities: also called glowing generality, is an emotionally appealing word so closely associated with highly-valued concepts and beliefs that it carries conviction without supporting information or reason. Such highly-valued concepts attract general approval and acclaim. Their appeal is to emotions such as love of country and home, and desire for peace, freedom, glory, and honour. They ask for approval without examination of the reason. They are typically used by politicians and propagandists.

Half-truth: A half-truth is a deceptive statement, which may come in several forms and includes some element of truth. The statement might be partly true, the statement may be totally true but only part of the whole truth, or it may utilize some deceptive element, such as improper punctuation, or double meaning, especially if the intent is to deceive, evade, blame or misrepresent the truth. The purpose and the consequence of a half-truth is to make something that is only a belief to appear as knowledge, or a truthful statement to represent the whole truth, or possibly lead to a false conclusion. According to the justified true belief theory of knowledge, in order to know that a given proposition is true, one must not only believe in the relevant true proposition, but one must also have a good reason for doing so. A half-truth deceives the recipient by presenting something believable and using those aspects of the statement that can be shown to be true as good reason to believe the statement is true in its entirety, or that the statement represents the whole truth. A person deceived by a half-truth considers the proposition to be knowledge and acts accordingly.

Labelling or labelling: is describing someone or something in a word or short phrase. For example, describing someone who has broken a law as a criminal. Labelling theory is a sociology theory which ascribes labelling of people to control and identification of deviant behaviour. It has been argued that labelling is necessary for communication. However, the use of the term labelling is often intended to highlight the fact that the label is a description applied from the outside, rather than something intrinsic to the labelled thing. This can be done for several reasons:

- To provoke a discussion about what the best description is,
- To reject a particular label,

- To reject the whole idea that the labelled thing can be described in a short phrase.

A euphemism is used when the propagandist attempts to increase the perceived quality, credibility, or credence of a particular ideal. A Dysphemism is used when the intent of the propagandist is to discredit, diminish the perceived quality, or hurt the perceived righteousness mark. Instead of creating a "label", a "category" or "faction" of a population, it is much easier to make an example of these larger bodies, because they can uplift or defame the Mark without actually incurring legal-defamation. Example: "Liberal" is a dysphemism intended to diminish the perceived credibility of a particular Mark. By taking a displeasing argument presented by a Mark, the propagandist can quote that person, and then attack "liberals" in an attempt to:

- I. create a political battle-ax of unaccountable aggression and
- II. diminish the quality of the Mark.

If the propagandist uses the label on too-many perceivably credible individuals, muddying up the word can be done by broadcasting bad-examples of "liberals" into the media. Labelling can be thought of as a sub-set of Guilt by association, another logical fallacy.

Latitudes of acceptance: If a person's message is outside the bounds of acceptance for an individual and group, most techniques will engender psychological reactance (simply hearing the argument will make the message even less acceptable). There are two techniques for increasing the bounds of acceptance. First, one can take a more even extreme position that will make more moderate positions seem more acceptable. This is similar to the Door-in-the-Face technique. Alternatively, one can moderate one's own position to the edge of the latitude of acceptance and then over time slowly move to the position that was previously.

Love bombing: is an attempt to influence a person by lavish demonstrations of attention and affection. The phrase can be used in different ways. Members of the Unification Church (who reportedly coined the expression) use or have used it themselves to mean a genuine expression of friendship, fellowship, interest, or concern. Critics of cults use the phrase with the implication that the "love" is feigned and the practice is manipulative. It has also been used to refer to abusers in romantic relationships showering their victims with praise, gifts, and affection in the early stages of a relationship.

Lying and deception: can be the basis of many propaganda techniques including Ad Homimen arguments, Big-Lie, Defamation, Door-in-the-Face, Half-truth, Name-calling or any other technique that is based on dishonesty or deception. For example, many politicians have been found to frequently stretch or break the truth.

Managing the news: refers to acts that are intended to influence the presentation of information within the news media. The expression managing the news is often used in a negative sense. According to Adolf Hitler "The most brilliant propagandist technique will yield no success unless one fundamental principle is borne in mind constantly - it must confine itself to a few points and repeat them over and over. This idea is consistent with the principle of classical conditioning as well as the idea of "Staying on Message" (which is a technique intended to limit questions and attention to a narrow scope favourable to the subject).

Milieu control: is a term popularized by psychiatrist Robert Jay Lifton to describe tactics that control environment and human communication through the use of social pressure and group language. Such tactics may include dogma, protocols, innuendo, slang, and pronunciation, which enables group members to identify other members, or to promote cognitive changes in individuals. Lifton originally used “milieu control” to describe brainwashing and mind control, but the term has since been applied to other contexts.

Name-calling: Propagandists use this technique to incite fears and arouse prejudices in their hearers in the intent that the bad names will cause hearers to construct a negative opinion about a group or set of beliefs or ideas that the propagandist wants hearers to denounce. The method is intended to provoke conclusions about a matter apart from impartial examinations of facts. Name-calling is thus a substitute for rational, fact-based arguments against an idea or belief on its own merits.

Obfuscation, intentional vagueness and confusion: Generalities are deliberately vague so that the audience may supply its own interpretations. The intention is to move the audience by use of undefined phrases, without analyzing their validity or attempting to determine their reasonableness or application. The intent is to cause people to draw their own interpretations rather than simply being presented with an explicit idea. In trying to “figure out” the propaganda, the audience forgoes judgment of the ideas presented. Their validity, reasonableness and application may still be considered.

Obtain disapproval or Reductio ad Hitlerum: This technique is used to persuade a target audience to disapprove of an action or idea by suggesting that the idea is popular with groups hated, feared, or held in contempt by the target audience. Thus if a group that supports a certain policy is led to believe that undesirable, subversive, or contemptible people support the same policy, then the members of the group may decide to change their original position. This is a form of bad logic, where A is said to include X, and B is said to include X, therefore, A = B.

Operant conditioning or instrumental conditioning: is a type of learning in which an individual's behaviour is modified by its consequences; the behaviour may change in form, frequency, or strength. The word operant can be described as, “an item of behaviour that is initially spontaneous, rather than a response to a prior stimulus, but whose consequences may reinforce or inhibit recurrence of that behaviour”. In other words operant conditioning involves learning through imitation. For example, watching an appealing person buy products or endorse positions teaches a person to buy the product or endorse the position. Operant conditioning is the underlying principle behind the Ad Nauseam, Slogan and other repetition public relations campaigns.

The fallacy of the single cause: also known as complex cause, causal oversimplification, causal reductionism, and reduction fallacy, is a fallacy of questionable cause that occurs when it is assumed that there is a single, simple cause of an outcome when in reality it may have been caused by a number of only jointly sufficient causes.

Pensée unique: Enforced reduction of discussion by use of overly simplistic phrases or arguments, for example: “There is no alternative to war”.

Quotes out of context: it's a practice that sometimes also referred as “contextomy”¹⁸¹ or “quote mining”, is a logical fallacy and a type of false attribution in which a passage is removed from its surrounding matter in such a way as to distort its intended meaning. Arguments based on this fallacy typically take two forms:

¹⁸¹ Contextomy: refers to the selective excerpting of words from their original linguistic context in a way that distorts the source's intended meaning, a practice commonly referred to as “quoting out of context”. The problem here is not the removal of a quote from its original context, (as all quotes are), per se, but to the quote's decision to exclude from the excerpt certain nearby phrases or sentences, (which become “context” by virtue of the exclusion), that serve to clarify the intentions behind the selected words.

- I. As a **straw man argument**: which is frequently found in politics, it involves quoting an opponent out of context in order to misrepresent their position, (typically to make it seem more simplistic or extreme), in order to make it easier to refute.
- II. As an **appeal to authority**: it involves quoting an authority on the subject out of context, in order to misrepresent that authority as supporting some position.

Selectively editing quotes to change meanings—political documentaries designed to discredit an opponent or an opposing political viewpoint often make use of this technique.

Rationalization, (making excuses): It is an informal fallacy of reasoning. It is an unconscious defence mechanism in which perceived controversial behaviours or feelings are logically justified and explained in a rational or logical manner in order to avoid any true explanation, and are made consciously tolerable – or even admirable and superior – by plausible means. Rationalization encourages irrational or unacceptable behaviour, motives, or feelings and often involves ad hoc hypothesizing. This process ranges from fully conscious (e.g. to present an external defence against ridicule from others) to mostly subconscious (e.g. to create a block against internal feelings of guilt).

Red herring¹⁸²: Presenting data or issues that, while compelling, are irrelevant to the argument at hand, and then claiming that it validates the argument.

Repetition¹⁸³: This is the repeating of a certain symbol or slogan so that the audience remembers it. This could be in the form of a jingle or an image placed on nearly everything in the picture/scene.

Scapegoating: Assigning blame to an individual or group, thus alleviating feelings of guilt from responsible parties and/or distracting attention from the need to fix the problem for which blame is being assigned.

Slogan: is a memorable motto or phrase used in a political, commercial, religious, and other context as a repetitive expression of an idea or purpose. The word slogan is derived from slogorn which was an Anglicisation of the Scottish Gaelic sluagh-ghairm tanmay (sluagh “army”, “host” + gairm “cry”). Slogans vary from the written and the visual to the chanted and the vulgar. Their simple rhetorical nature usually leaves little room for detail, and a chanted slogan may serve more as social expression of unified purpose, than as communication to an intended audience. Although slogans may be enlisted to support reasoned ideas, in practice they tend to act only as emotional appeals. Opponents of the US's invasion and occupation of Iraq use the slogan “blood for oil” to suggest that the invasion and its human losses was done to access Iraq's oil riches. On the other hand, supporters who argue that the US should continue to fight in Iraq use the slogan “cut and run” to suggest withdrawal is cowardly or weak.

¹⁸² Ignoratio elenchi, (also known as irrelevant conclusion): is the informal fallacy of presenting an argument that may or may not be logically valid, but fails nonetheless to address the issue in question. Ignoratio elenchi falls into the broad class of relevance fallacies. It is one of the fallacies identified by Aristotle in his Organon. In a broader sense he asserted that all fallacies are a form of ignoratio elenchi. The phrase ignoratio elenchi is Latin meaning “ignorance of refutation”. Here elenchi is the genitive singular of the Latin noun elenchus, which is from the Greek word “ἐλεγχος”, meaning an argument of disproof or refutation.

¹⁸³ Repetition is the simple repeating of a word, within a sentence or a poetical line, with no particular placement of the words, in order to provide emphasis. This is such a common literary device that it is almost never even noted as a figure of speech. It also has connotations to listing for effect and is used commonly by famous poets such as Larkin.

Stereotyping¹⁸⁴: This technique attempts to arouse prejudices in an audience by labelling the object of the propaganda campaign as something the target audience fears, hates, loathes, or finds undesirable. For instance, reporting on a foreign country or social group may focus on the stereotypical traits that the reader expects, even though they are far from being representative of the whole country or group; such reporting often focuses on the anecdotal. In graphic propaganda, including war posters, this might include portraying enemies with stereotyped racial features.

Testimonial: Testimonials are quotations, in or out of context, especially cited to support or reject a given policy, action, program, or personality. The reputation or the role (expert, respected public figure, etc.) of the individual giving the statement is exploited. The testimonial places the official sanction of a respected person or authority on a propaganda message. This is done in an effort to cause the target audience to identify itself with the authority or to accept the authority's opinions and beliefs as its own.

Third party technique: is a marketing strategy commonly employed by Public Relations (PR) firms, and involves placing a premeditated message in the “mouth of the media”. Third-party technique can take many forms, ranging from the hiring of journalists to report the organization in a favourable light, to using scientists within the organization to present their perhaps prejudicial findings to the public. Industry-sponsored groups used to relay these findings to the public are known as front groups. These groups claim to represent the general public’s agenda, when in reality they are facilitating the hidden interests of the organizations that are sponsoring them. Also related are astroturf groups, which are groups that have been formed by the industry, yet appear to have been formed by ordinary citizens.

Thought-terminating cliché: refers to a cliché that is a commonly used phrase, sometimes passing as folk wisdom, used to quell cognitive dissonance. Though the clichéd phrase in and of itself may be valid in certain contexts, its application as a means of dismissing dissent or justifying fallacious logic is what makes it thought-terminating.

Transfer: is a technique used in propaganda and advertising. Also known as association, this is a technique of projecting positive or negative qualities (praise or blame) of a person, entity, object, or value (an individual, group, organization, nation, patriotism, etc.) to another in order to make the second more acceptable or to discredit it. It evokes an emotional response, which stimulates the target to identify with recognized authorities. Often highly visual, this technique often utilizes symbols, (for example, the Swastika used in Nazi Germany, originally a symbol for health and prosperity), and what do you do superimposed over other visual images. An example of common use of this technique in the United States is for the President to be filmed or photographed in front of the country's flag.

Unstated assumption: is a type of propaganda message which forgoes explicitly communicating the propaganda's purpose and instead states ideas derived from it. This technique is used when a propaganda's main idea lacks credibility, and thus when mentioned directly will result in the audience recognizing its fallacy and nullifying the propaganda.

¹⁸⁴ The term stereotype derives from the Greek words στερεός (firm, solid) and τύπος impression, hence, solid impression. The term comes from the printing trade and was first adopted in 1798 by Firmin Didot to describe a printing plate that duplicated any typography. The duplicate printing plate, or the stereotype, is used for printing instead of the original. The first reference to “stereotype” in its modern use in English, outside of printing, was in 1850, in a noun, meaning “image perpetuated without change”. But it was not until 1922 that “stereotype” was first used in the modern psychological sense by American journalist Walter Lippmann in his work *Public Opinion*.

Virtue words: also known as ideograph is a word frequently used in political discourse that uses an abstract concept to develop support for political positions. Such words are usually terms that do not have a clear definition but are used to give the impression of a clear meaning. Such examples include liberty and rights. Their use is considered of the Transfer propaganda technique.

Selective truth: It is the ability not to tell the whole truth, but to use that piece of truth that will serve your purpose and presented it in a way that is not understood by the recipient¹⁸⁵.

These are some of the main techniques and methods that can be applied to propaganda, the list of techniques - methods are theoretically limitless, as most social, psychological and communication theories can be applied to generate propaganda.

At the following chapter we will present the main theme of this paper which is Open Source Intelligence as an intelligence discipline.

¹⁸⁵ Richard Crossman, the British Deputy Director of Psychological Warfare Division (PWD) for the Supreme Headquarters Allied Expeditionary Force (SHAEP) during the Second World War said: "In propaganda truth pays... It is a complete delusion to think of the brilliant propagandist as being a professional liar. The brilliant propagandist is the man who tells the truth, or that selection of the truth which is requisite for his purpose, and tells it in such a way that the recipient does not think he is receiving any propaganda... [...] The art of propaganda is not telling lies, but rather selecting the truth you require and giving it mixed up with some truths the audience wants to hear".

CHAPTER 3.

Open Source Intelligence (OSINT).

3.1 The History of Open Source Intelligence.

To identify the first signs of understanding the importance - significance of Open Source Intelligence we must go back in February 1941, when President Roosevelt decided the creation of the Foreign Broadcast Monitoring Service (FBMS), under the authority of the Federal Communications Commission. The mandate of the FBMS was to record, translate, transcribe and analyze shortwave propaganda radio programs that were being beamed at the United States by the Axis powers. Its first monitoring station was established in October 1941 in Portland, Oregon.

With the end of World War II, the FBMS was transferred to the Department of the Army. Like many other wartime organizations, the FBMS was threatened with disbandment. The possibility of its disbandment was roundly criticized in many different quarters, which helped ensure its survival.

Upon the passing of the National Security Act of 1947, the FBMS was renamed as Foreign Broadcast Information Service (FBIS), under the authority of Central Intelligence Agency (CIA). Its original mission revolved around radio and press agency monitoring. In 1967, the Service's mission was expanded to cover foreign mass media transmitted by radio, television, and print.

The 1988 is another key point in evolution of OSINT, that year General Alfred M. Gray, Jr., Commandant of the Marine Corps, called for a redirection of US intelligence away from the collapsing Soviet Union and toward non – state actors and Third World zones of instability. He had also pointed out that most of the intelligence which needs to be known could be obtained via open source intelligence discipline, and recommended a substantive increase in resources for this aspect of the intelligence collection spectrum of sources¹⁸⁶.

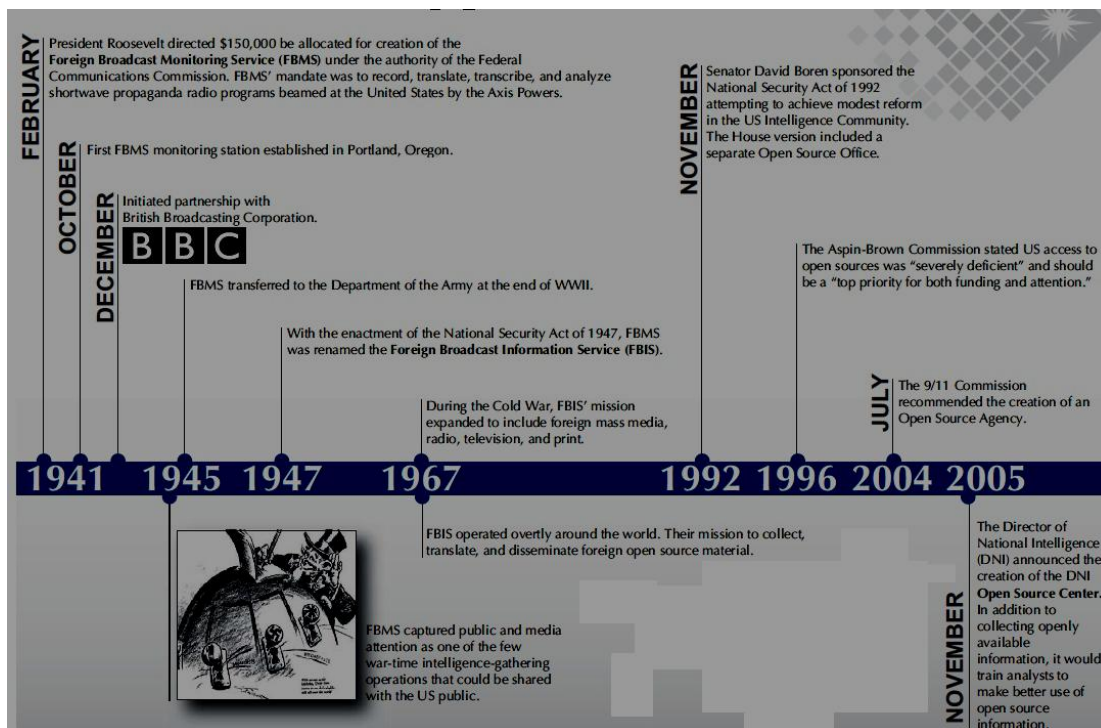


Table 14: The Key Points of Open Source Intelligence Historical Evolution and Development¹⁸⁷.

¹⁸⁶ General Alfred M. Gray, "Global Intelligence Challenges in the 1990s", American Intelligence Journal (Winter 1989–1990), http://en.wikipedia.org/wiki/Open-source_intelligence.

¹⁸⁷ OSINT Handbook by George Cristian Maior Director of the Romanian Intelligence Service, <http://www.opensource.gov>.

In the fall of 1992, Senator David Boren, then Chairman of the Senate Select Committee on Intelligence, sponsored the National Security Act of 1992, attempting to achieve modest reform in the U.S. Intelligence Community. His counterpart on the House Permanent Select Committee on Intelligence was Congressman Dave McCurdy. The House version of the legislation included a separate open – source office, at the suggestion of Larry Prior, a Marine Reservist (who served as a Marine Intelligence Officer for 11 years) and then serving on the House Permanent Select Committee on Intelligence staff.

The Aspin-Brown Commission stated in 1996 that US access to open sources was "severely deficient" and that this should be a "top priority" for both funding and the Director of Central Intelligence (DCI), attention.

In issuing its July 2004 report, the 9/11 Commission recommended the creation of an open-source intelligence agency, but without further detail or comment¹⁸⁸. Subsequently, the Weapons of Mass Destruction Commission (also known as the Robb–Silberman Commission) report in March 2005 recommended the creation of an open – source directorate at the CIA.

Following these recommendations, in November 2005 the Director of National Intelligence announced the creation of the Open Source Center. The Center was established to collect available information from “the Internet, databases, press, radio, television, video, geospatial data, photos and commercial imagery¹⁸⁹”. In addition to collecting openly available information, it would train analysts to make better use of this information. The Center absorbed the CIA's previously existing Foreign Broadcast Information Service (FBIS), originally established in 1941, with FBIS head Douglas Naquin named as director of the Center.

In December 2005, the Director of National Intelligence appointed Eliot A. Jardines as the Assistant Deputy Director of National Intelligence for Open Source to serve as the Intelligence Community's senior intelligence officer for open source and to provide strategy, guidance and oversight for the National Open Source Enterprise¹⁹⁰.

In many ways, open source information holds some of the greatest value for intelligence because of the vast array of diverse, reliable information available for analysis and exploitation. In recent years there has been an extension in the usage of OSINT from the traditional usage field of Business intelligence to National Security Intelligence. Rapid technological development has changed radically both the character and the ways of searching, analyzing, processing, and the exploitation of OSINT. The continuous technological development of computers (memory capacitance, speed processing, transmission capacity – download capabilities of audio, image, video, etc.), as well as the advent of the Internet has radically changed the landscape proliferation and trafficking of all kinds of information. Beginning in the mid-to-late 1990s, the Internet (World Wide Web, www), emerged as the primary source of search traffic for all types and kind of information, in conjunction with this integration and the increasing use of computers in every aspect of daily life has led Internet applications and services providers to increase both the type and the mass of the available content. (due to the mass acceptance and usage by the public worldwide).

This despite the obvious advantages, can also create problems for the information analyst, because the increased amount of information and easier processing and utilization of these does not equal quality of information. OSINT users and information analysts must be very careful to ensure that the collected (from open sources), information which is going to be used for decision making is accurate and reliable. Information that hasn't passed from quality control have little value, is therefore a challenge to properly manage the huge volume of available information, this can be treated with the appropriate and continuing education and the acquisition of expertise by the information analyst. In the following sections we will try to present and analyze the most important issues that deal with OSINT as an intelligence discipline.

¹⁸⁸ 9-11 Commission Report page 413, http://en.wikipedia.org/wiki/Open-source_intelligence.

¹⁸⁹ Office of the Director of National Intelligence. “ODNI Announces Establishment of Open Source Center”.

¹⁹⁰ Office of the Director of National Intelligence “ODNI Senior Leadership Announcement”.

3.2 Terms definition.

There are three main definitions of the term, those are the following:

- “Open-source intelligence is the intelligence discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence and information requirement, OSINT also applies to the intelligence produced by that discipline¹⁹¹”.
- “Open source information is any type of lawfully and ethically obtainable information that describes persons, behaviours, locations, groups, events, or trends¹⁹²”.
- “Publicly available information that anyone can lawfully obtain by request, purchase, or observation¹⁹³”.

As we can see from the above three definitions, the type of information belonging to the category of open source is very wide. This is a very important advantage for military and law enforcement organizations, services and agencies because the search for the necessary information is not subject to legal proceedings, impediments and obstacles¹⁹⁴.

Two also important and related to OSINT terms are open source and publicly available information:

“Open source is any person or group that provides information without the expectation of privacy, the information, the relationship, or both is not protected against public disclosure. Open-source information can be publicly available but not all publicly available information is open source. Open sources refer to publicly available information medium and are not limited to physical persons¹⁹⁵”.

“Publicly available information is data, facts, instructions, or other material published or broadcast for general public consumption, available on request to a member of the general public, lawfully seen or heard by any casual observer, or made available at a meeting open to the general public¹⁹⁶”.

As we have already seen, when raw open source data or information is evaluated, integrated, and analyzed it provides new insight about intelligence targets, issues and trends, this in general is Open Source Intelligence. OSINT collection is normally accomplished through monitoring, data-mining, and research. Open-source production supports all-source intelligence and the continuing activities of the intelligence process (generate intelligence knowledge, analyze, assess, and disseminate)¹⁹⁷. Like all the other intelligence disciplines, OSINT is developed based on the requestor intelligence requirements.

¹⁹¹ US Army Techniques Publication No. 2-22.9 (FMI 2-22.9), 2012.

¹⁹² Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies, page: 284.

¹⁹³ Intelligence Community Directive, Number 301: National Open Source Enterprise, Section F(3), 11 July 2006.

¹⁹⁴ We must always keep in mind the civil rights issues that emerge and related to the retention of open source information for the intelligence process. The main qualifier that classifies information as open source is that no legal process or clandestine collection techniques are required to obtain the data.

¹⁹⁵ US Army Techniques Publication No. 2-22.9 (FMI 2-22.9), 2012.

¹⁹⁶ US Army Techniques Publication No. 2-22.9 (FMI 2-22.9), 2012.

¹⁹⁷ Field Manual No. 2-0, March 2010.

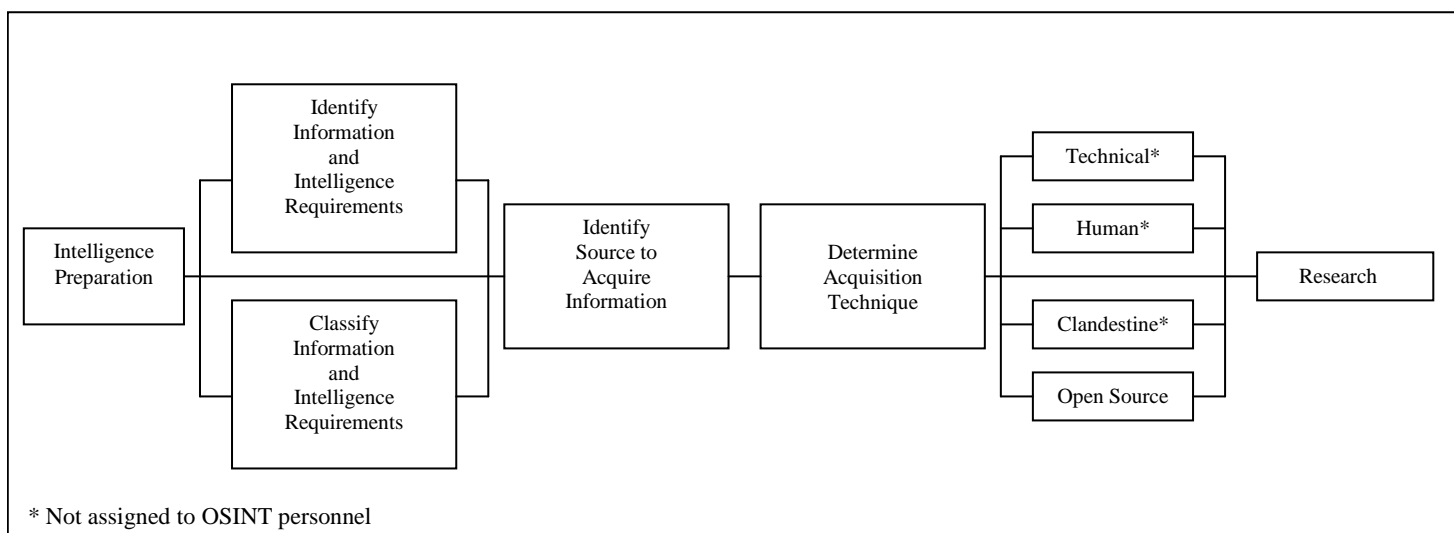


Table 15: Process for collecting publicly available information¹⁹⁸

3.2.1 OSINT as a Discipline.

The source of the information, the type of information, and the collection – gathering means (techniques) rather than a specific category of technical or human resources distinguish OSINT from other intelligence disciplines. Open sources broadcast, publish, or otherwise distribute unclassified information for public use. The collection methods and techniques for collecting – gathering publicly available information from open sources these media of communications are unobtrusive - noninvasive. Other intelligence disciplines use confidential sources or intrusive techniques to collect private information. Confidential sources and private information are:

- ❖ **Confidential Source:** is any person, group, or system that provides information with the expectation that the information, relationship, or both, are protected against public disclosure.
- ❖ **Private Information:** which is data, facts, instructions, or other material intended for or restricted to a particular person, group, or organization. There are two subcategories of private information: classified information and controlled unclassified information.
 - Classified information: requires protection against unauthorized disclosure and is marked to indicate its classified status when in documentary or readable form.
 - Controlled unclassified: information requires the application of controls and protective measures, for a variety of reasons (that is, sensitive but unclassified, or for official use only), not to include those that qualify for formal classification.

¹⁹⁸ US Army Techniques Publication No. 2-22.9 (FMI 2-22.9), 2012.

3.3 Types of OSINT Sources.

One of the biggest advantages is the variety of sources from which one analyst may seek the necessary information, the list of sources is theoretically limitless, in the following paragraphs we will present the main ones.

A. Public Sector:

1. Academia. Courseware, dissertations, lectures, presentations, research papers, and studies in both hardcopy and softcopy on a variety of topics, such as, economics, geography (physical, cultural, political and military), international relations, regional security, science, technology, etc.

1.1 School & Universities: are a source of both labour (students and faculty), and data¹⁹⁹. A lot of Universities across the world serve as “centers of excellence” in various areas of intelligence analysts interests. If the open sources analyst knows how to gain access and exploit such information he/she can save time and money (and improve support and service to the consumer – requestor).

1.2 Libraries: are offering the same as the above opportunities to the open source analysts, especially those “Special Libraries” which are maintained by major national and multinational organizations (both governmental – non governmental, profit – non profit), and corporations.

2. Governmental Organizations (Bureaus, Services and Agencies): Databases, posted information, and printed reports on a wide variety of economic, environmental, geographic, humanitarian, security, science, and technology issues.

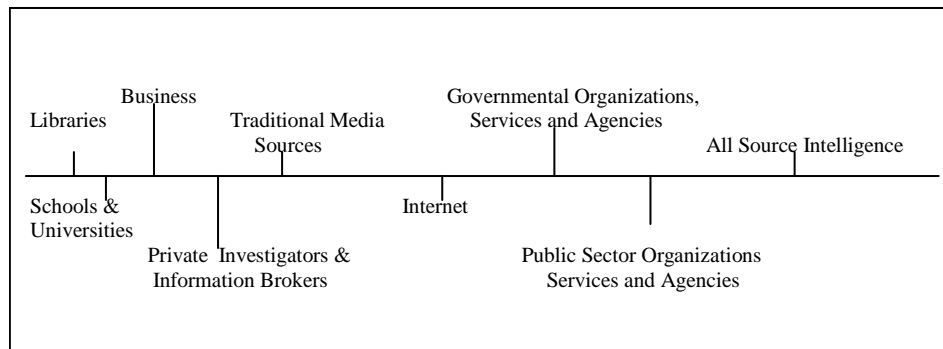


Table 16: “Information Continuum”²⁰⁰

¹⁹⁹ The Mercyhurst College which is the only University in the USA with undergraduate degree for intelligence analysts, has his students using open sources to produce newsletters an various topics (such as drugs smuggling, human trafficking, etc), of interest for Law Enforcement services and agencies.

²⁰⁰ The above figure illustrates “Information Continuum” which comprises the knowledge terrain of the private sector within which each all source analysts must learn to navigate if they are want to make the most effective use of classified as well as open sources.

B. Private Sector:

- 1. Businesses (Companies, both domestic and abroad):** maintain a great amount of information, such as: Databases, posted information, and printed reports on a wide variety of economic, environmental, geographic, humanitarian, science, and technology issues. Most of this information is unpublished but available if asking²⁰¹.
- 2. Private Investigators & Information Brokers:** spend their time and careers developing “special” expertise in certain areas and research methods (which may be particularly useful to an intelligence analyst)²⁰².
- 3. Traditional Media Sources:** for many years they were the only open intelligence sources, this category includes newspapers, journals, magazines, broadcast media, radio and television as well as the current array of electronically available products.
- 4. Internet:** The Internet has, since 1994, literally exploded on to the world scene and changed forever the manner in which individuals might carry out global research. According to Dr. Vinton Cerf, (acknowledged by many to be one of the founders of the Internet), it will grow from 400 million users in November 2000, to an estimated 3.5 billion users by the year 2015. In general, the Internet today provides two benefits to the information analyst:

- ❖ As a means of rapidly communicating with counterparts around the world, primarily to exchange unclassified information and professional insights.
- ❖ As a means of rapidly accessing both free and premium (fee paid for access) information sources.

4.1 Newsletters and Blogs: Newsletters are designed to highlight issues, trends, and developments within a specific topic area. Blogs are web-based opinion discussions also typically focused on a specific topic area where writers and readers express opinions, perspectives, and beliefs. In many cases, a single source will have both a newsletter and a blog; for example, a particularly useful newsletter and blog for intelligence issues is Secrecy News²⁰³ from the Federation of American Scientists²⁰⁴. There are four broad categories of newsletters and blogs:

4.1.1 Professional/academic and government: These sources tend to be the most objective, although never rule out the ideological influence, even if unintentional, of an author or editor. Despite this caveat, these sources are most likely to make statements based on corroborated information and use an approach to analysis and conclusion based on logic and the scientific method rather than emotional arguments. Typically, these sources report facts and data more objectively and most commonly include attribution of facts and data.

4.1.2 Commercial sources: As the name implies, these are profit-driven sources often intended to provide information that supports the sale of products or services. Despite the fact that the motive of the source is to make a profit, the sources can nonetheless be very reliable. Indeed, the reliability of these sources is often an important selling point for the business. While the information is typically accurate, information about alternatives is not likely to be included.

²⁰¹ During the Iraq War, Businesses were providing the most critical information about the Iraqi Command and Control Systems, including detailed plans of communications, radars and computing infrastructures and installations as well.

²⁰² For instance The Burwell Directory of Information Brokers has worldwide specialists which can provide indexed topics by issue, subject, country, and language fluency.

²⁰³ See www.fas.org/sgp/news/secrecy and www.fas.org/blog/secrecy.

²⁰⁴ The Federation of American Scientists web site contains a great deal of interesting and useful information related to intelligence issues, including downloadable documents, many of which are often difficult to gain access to.

4.1.3 Advocacy groups: These sources are agenda-driven based on the ideology and goals of the source. A newsletter from a right-wing extremist source will reflect information that supports that ideology. Similarly, discussions in a blog on environmental extremism will support the goals of that group. The reader should recognize where they are coming from and factor that into one's analysis. Using this approach, these sources can be quite insightful for understanding an ideology or advocacy position.

4.1.4 Pundits: A wide range of individuals' blog on the web as critics and commentators on virtually every subject. Pundits work for a wide variety of news organizations, entertainment media, professional organizations, etc, and some are independent commentators working only for themselves, oftentimes not as a source of income, but as a means to discuss an interest or belief. What is important to recognize is that pundits typically do not seek to be objective, but to comment on a topic of interest from their particular ideology or perspective. This is also true for pundits who blog for news organizations. Often their arguments and observations are persuasive and useful, but typically they are not objective. Pundits tend to be news and policy wonks, hence, their research will often identify issues and sources of information that might otherwise be easily missed. As such, they are often good sources of raw information that can be corroborated through objective sources.

5. Wikis: A wiki is software that allows users to easily create, edit, and link pages. Wikis are often used to create collaborative web sites and to power community web sites, often also referred to as wikis. Perhaps the best known wiki is the online encyclopedia Wikipedia²⁰⁵, however, there are many types of wikis, some with a very specific focus²⁰⁶. Wikis can be a valuable source when dealing with a topic or issue about which the information collector has limited information. Most wikis include external references to materials which helps in the corroboration process. From an intelligence perspective, the wiki can provide subject matter knowledge on an issue as well as direction to more information.

6. RSS Feeds (Really Simple Syndication): is a family of web feed formats used to publish frequently updated content including, but not limited to, blog entries, news headlines, and podcasts. An RSS document (which is called a feed, web feed, or channel) contains either a summary of content from an associated web site or the full text. From an open source perspective, the value of RSS feeds, when available on a web site, is that any new information or changes in content are sent to those registered for the service without the need to check each site. It increases both the efficiency and timeliness of information for the user²⁰⁷.

²⁰⁵ en.wikipedia.org/wiki/Main_Page

²⁰⁶ Intellipedia: www.opensource.gov/providers/intelinku/wiki/Main_Page (access only)

²⁰⁷ As an example, see the terrorism news and analysis RSS feeds at www.2rss.com/rss_5352.html.

7. The Deep Web: or invisible web refers to the following:

“The vast repository of information that search engines and directories don't have direct access to, like databases. Unlike pages on the visible Web (that is, the Web that you can access from search engines and directories), information in databases is generally inaccessible to the software spiders and crawlers that create search engine indexes²⁰⁸”.

Deep Web Database Search Utilities		
Clusty	A metasearch engine that combines the results of several top search engines.	www.clusty.com
Intute	A searchable database of trusted web sites reviewed and monitored by subject specialists.	www.intute.ac.uk
Internet Archive	A database of tens of thousands of movies, live music, audio, texts, and home of the Wayback Machine that allows you to find old versions of web pages, more than 55 billion.	www.archive.org/index.php
Scitopia.org	A federated search engine that consists of a real time search through a disparate group of databases. The user enters a set of query parameters, which are broadcast to the selected databases; the results are collated and presented back to the user in a unified format.	www.scitopia.org
Pipl	As an alternative method to search for people, Pipl searches databases for names of individuals rather than names that are simply incorporated on web pages.	www.pipl.com
GPO's Catalog of U.S. Government Publications ¹	A searchable database of federal publications, with links to those available online.	catalog.gpo.gov
Education Resources Information Center (ERIC)	A catalog of more than 1.2 million bibliographic records, providing links to the full text where available. Sponsored by the U.S. Department of Education and the Institute of Education Sciences.	www.eric.ed.gov/ERICWebPortal/Home.portal
CIA Electronic Reading Room	A searchable database of declassified CIA documents.	www.foia.cia.gov
Global Legal Information Network	A searchable public database of laws, regulations, judicial decisions, and other legal sources.	www.glin.gov
Note: The above are some indicative Database Search Utilities, the list is bigger.		

Table 17: Deep Web Database Search Utilities.

Mike Bergman, founder of Bright Planet and credited with coining the phrase²⁰⁹, said that:

“Searching on the Internet today can be compared to dragging a net across the surface of the ocean: a great deal may be caught in the net, but there is a wealth of information that is deep and therefore missed²¹⁰”.

Most of the Web's information is buried far down on dynamically generated sites, and standard search engines do not find it. Traditional search engines cannot find or retrieve content in the deep Web, (those pages do not exist until they are created dynamically as the result of a specific search). The deep Web is several orders of magnitude larger than the surface Web. Estimates based on extrapolations from a study done at University of California, Berkeley in 2001²¹¹, speculate that the deep Web consists of about 7,500 terabytes. More accurate estimates are available for the number of resources in the deep Web: He detected around 300,000 deep web sites in the entire Web in 2004,

²⁰⁸ websearch.about.com/od/invisibleweb/a/invisible_web.htm

²⁰⁹ Wright, Alex (22-02-2009): "Exploring a 'Deep Web' That Google Can't Grasp", http://en.wikipedia.org/wiki/Deep_Web

²¹⁰ Bergman K. Michael: “The Deep Web: Surfacing Hidden Value”, BrightPlanet LLC, July 2000.

²¹¹ Bergman K. Michael: “The Deep Web: Surfacing Hidden Value”, The Journal of Electronic Publishing, August 2001.

and, according to Shestakov, around 14,000 deep web sites existed in the Russian part of the Web in 2006²¹².

Obviously, a great deal of open source information from the deep web could be valuable to the intelligence process if it could be identified and retrieved. The deep web is searchable, but not using standard search techniques. The goal is to find tools that can locate valuable open source deep web information²¹³. The most effective ways to search the deep web is to use search utilities that are designed to explore specific databases.

Beyond these diverse resources (see the above table), there is a number of fee-based deep web search utilities (see the following table):

Fee – Based Deep Web Database Search Utilities		
Xrefer	A searchable database of 236 titles and more than 2.8 million entries.	www.xrefer.com
LexisNexis	The world's largest collection of public records, unpublished opinions, forms, legal, news, and business information. More than 35,000 sources are searchable with full-text available online.	www.lexisnexis.com
Forrester Research	An independent technology and market research company publishing in-depth research reports on a variety of subjects.	www.forrester.com
Factiva	A searchable collection of more than 10,000 individual sources.	www.factiva.com
Copernic*	Provides indexing, searching, and tracking of databases and deep web resources by using software that seeks and identifies web resources beyond those in HTML.	www.copernic.com
BrightPlanet*	Searches, harvests, consolidates, indexes, merges, analyzes, and categorizes documents and associated metadata in any format and language, from visible and deep sources on the web and from inside and outside the firewall.	www.brightplanet.com and www.completeplanet.com
* Both Copernic and BrightPlanet utilities are particularly comprehensive deep web search tools that go beyond databases that are useful for law enforcement intelligence.		

Table 18: Fee – Based Deep Web Database Search Utilities.

As we have already told estimates saw that the deep web contains 500 times more the content that is found in the visible web. There are Five core types of content constitute the invisible web, those are²¹⁴:

1. The content of web-based databases: Information stored in databases is accessible only by query to the database and are not picked up by the web crawlers used by search engines. A significant amount of valuable information on the web can be generated from databases.

²¹² Garcia, Frank: "Business and Marketing on the Internet", January 1996, http://en.wikipedia.org/wiki/Deep_Web.

²¹³ For a guide to assist your search strategy, see: [www.lib.berkeley.edu/TeachingLib/ Guides/Internet/Strategies.html](http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/Strategies.html).

²¹⁴ See www.internettutorials.net/deepweb.asp.

2. No textual files: this category includes multimedia files, graphics files, software, and documents in formats such as Portable Document Format (PDF). Web crawling has a limitation in searching the content of these types of files. Web crawlers can identify file names and extensions (e.g., .jpg, .wmv, .pdf, etc.) of such files, but cannot identify the content of these files during the web crawling process. Essentially, they are files that are not in Hypertext Markup Language format (HTML), therefore, a great deal of information and data are not picked up from these files by traditional searches.
3. Script-based web pages: These are web pages that are written in script coding, other than HTML and/or those with Uniform Resource Locator (URL), which is the web address.
4. Content available on sites protected by passwords or other restrictions: The content of web sites protected by some degree of access through rigorous password protection or a Virtual Private Network (VPN) will not be identified by search engines. There is a continuum of identifiable and non-identifiable information from these types of web sites depending on what types of information the site owners elect to be publicly accessible, (often for marketing purposes), as well as the degree of security applied to the site, (in some instances the web site's security is limited and some data can be identified).
5. Pages deliberately excluded by their owners: A web page creator who does not want his/her page captured in search engines can insert special meta tags that will cause most search engines' crawlers to avoid the page.

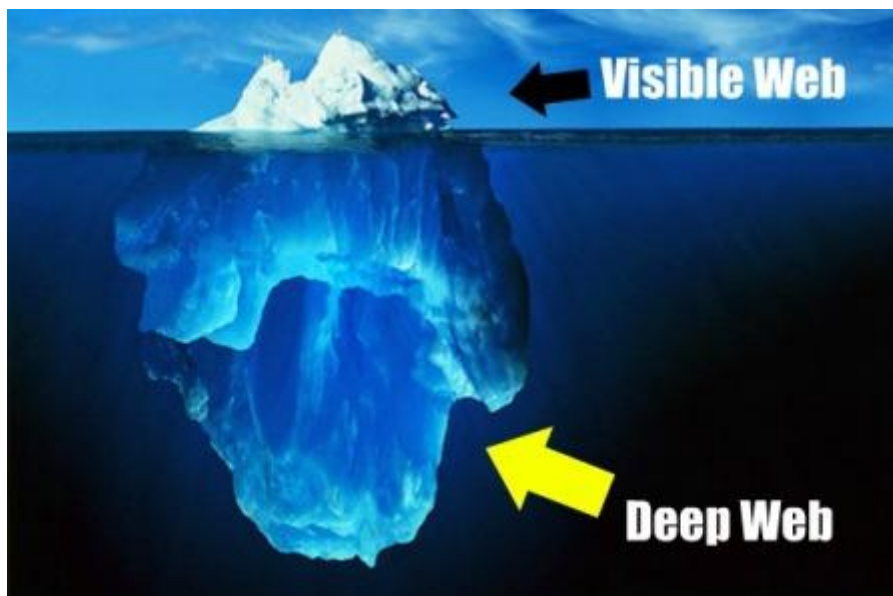
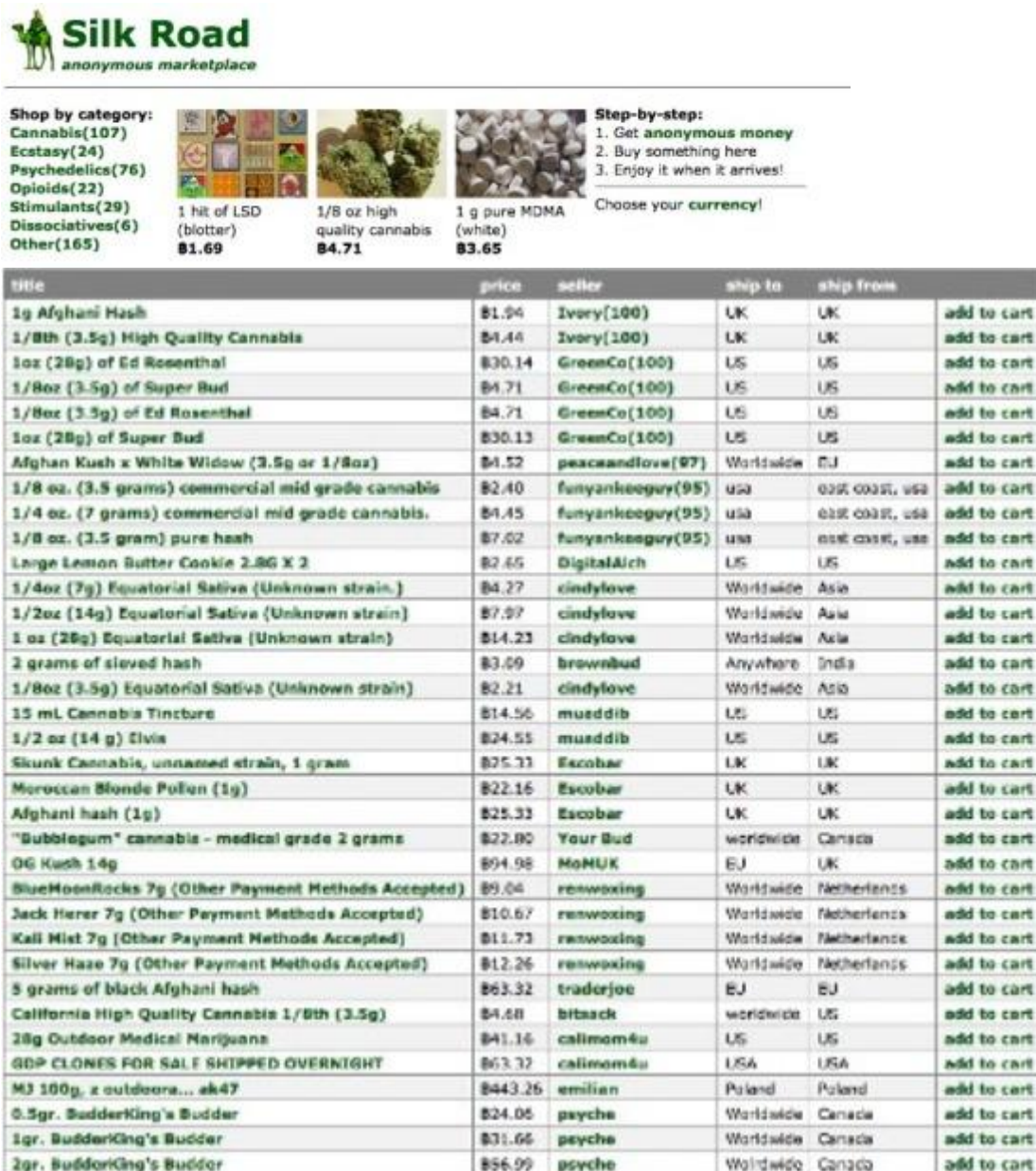


Photo 12: Visible and Deep Web.

8. The Underground Web: There is no definition regarding the term, so we are going to use the description from an article published in Business Week magazine²¹⁵:

“Warning: You are about to enter the dark side of the Internet. It's a place where crime is rampant and every twisted urge can be satisfied. Thousands of virtual streets are lined with casinos, porn shops, and drug dealers. Scam artists and terrorists skulk behind seemingly lawful Web sites. And cops wander through once in a while, mostly looking lost”.

Almost all types of underground web sites exist with the intent to keep their activities as secret as possible from the visible web world (and the authorities). Identity thieves who selling stolen credit card information, pedophiles exchanging photographs, traffickers unlawfully selling controlled substances (drugs), and criminal extremists and terrorists planning criminal and terrorist acts, are examples of open source information that exist in the underground deep web.



Silk Road
anonymous marketplace

Shop by category:
Cannabis(107)
Ecstasy(24)
Psychedelics(76)
Opioids(22)
Stimulants(29)
Dissociatives(6)
Other(165)

Step-by-step:
1. Get **anonymous money**
2. Buy something here
3. Enjoy it when it arrives!

Choose your **currency!**

1 hit of LSD (blotter) **\$1.69**
1/8 oz high quality cannabis **\$4.71**
1 g pure MDMA (white) **\$3.65**

title	price	seller	ship to	ship from	
1g Afghani Hash	\$1.94	Ivory(100)	UK	UK	add to cart
1/8th (3.5g) High Quality Cannabis	\$4.44	Ivory(100)	UK	UK	add to cart
1oz (28g) of Ed Rosenthal	\$30.14	GreenCo(100)	US	US	add to cart
1/8oz (3.5g) of Super Bud	\$4.71	GreenCo(100)	US	US	add to cart
1/8oz (3.5g) of Ed Rosenthal	\$4.71	GreenCo(100)	US	US	add to cart
1oz (28g) of Super Bud	\$30.13	GreenCo(100)	US	US	add to cart
Afghan Kush x White Widow (3.5g or 1/8oz)	\$4.52	peaceandlove(97)	Worldwide	EU	add to cart
1/8 oz. (3.5 grams) commercial mid grade cannabis	\$2.40	funyankeeguy(95)	usa	east coast, usa	add to cart
1/4 oz. (7 grams) commercial mid grade cannabis.	\$4.45	funyankeeguy(95)	usa	east coast, usa	add to cart
1/8 oz. (3.5 gram) pure hash	\$7.02	funyankeeguy(95)	usa	east coast, usa	add to cart
Large Lemon Butter Cookie 2.8g X 2	\$2.45	DigitalAich	US	US	add to cart
1/4oz (7g) Equatorial Sativa (Unknown strain.)	\$4.27	cindylove	Worldwide	Asia	add to cart
1/2oz (14g) Equatorial Sativa (Unknown strain)	\$7.97	cindylove	Worldwide	Asia	add to cart
1 oz (28g) Equatorial Sativa (Unknown strain)	\$14.23	cindylove	Worldwide	Asia	add to cart
2 grams of sieved hash	\$3.99	brownbud	Anywhere	India	add to cart
1/8oz (3.5g) Equatorial Sativa (Unknown strain)	\$2.21	cindylove	Worldwide	Asia	add to cart
15 mL Cannabis Tincture	\$14.56	muaddib	US	US	add to cart
1/2 oz (14 g) Elvis	\$24.55	muaddib	US	US	add to cart
Skunk Cannabis, unnamed strain, 1 gram	\$75.11	Escobar	UK	UK	add to cart
Moroccan Blonde Pollen (1g)	\$22.16	Escobar	UK	UK	add to cart
Afghani hash (1g)	\$25.33	Escobar	UK	UK	add to cart
"Bubblegum" cannabis - medical grade 2 grams	\$22.80	Your Bud	worldwide	Canada	add to cart
OG Kush 14g	\$94.98	MoHUK	EU	UK	add to cart
BlueMoonRocks 7g (Other Payment Methods Accepted)	\$9.04	renwaxing	Worldwide	Netherlands	add to cart
Jack Herer 7g (Other Payment Methods Accepted)	\$10.67	renwaxing	Worldwide	Netherlands	add to cart
Kali Mist 7g (Other Payment Methods Accepted)	\$11.73	renwaxing	Worldwide	Netherlands	add to cart
Silver Haze 7g (Other Payment Methods Accepted)	\$12.26	renwaxing	Worldwide	Netherlands	add to cart
5 grams of black Afghani hash	\$63.32	traderjoe	EU	EU	add to cart
California High Quality Cannabis 1/8th (3.5g)	\$4.68	bitsack	worldwide	US	add to cart
28g Outdoor Medical Marijuana	\$41.14	calimom4u	US	US	add to cart
GDP CLONES FOR SALE SHIPPED OVERNIGHT	\$63.32	calimom4u	USA	USA	add to cart
MJ 160g. 2 outdoor... ak47	\$443.26	emilian	Poland	Poland	add to cart
0.5gr. BudderKing's Budder	\$24.06	psyche	Worldwide	Canada	add to cart
1gr. BudderKing's Budder	\$31.66	psyche	Worldwide	Canada	add to cart
2gr. BudderKing's Budder	\$56.99	psyche	Worldwide	Canada	add to cart

Photo 13: An example of an Underground Web site called “Silk Road”, which selling drugs.

²¹⁵ www.businessweek.com/magazine/ content/02_35/b3797001.htm

Information such as those in the above photo can be particularly useful to law enforcement intelligence services and agencies because painstaking searches of the underground web and labor-intensive reading of underground web content and blogs, (from law enforcement intelligence analysts), can produce evidence and leads for a criminal inquiry. The above described process will be also faster, cheapest and more effective in identifying criminal and terrorist threats than traditional methods of inquiry.

9. Gray Literature²¹⁶: “Grey literature stands for manifold document types produced on all levels of government, academics, business and industry in print and electronic formats that are protected by intellectual property rights, of sufficient quality to be collected and preserved by library holdings or institutional repositories, but not controlled by commercial publishers i.e., where publishing is not the primary activity of the producing body²¹⁷”.

Nonetheless it may be an important source of information for all source analysts, because it tends to be original and recent. Grey literature includes (but not limited to):

- Patents,
- Technical reports from governmental organizations, services and agencies,
- Reports and working papers from scientific research groups or committees (governmental and non governmental),
- White papers, and
- Preprints.

The identification and acquisition of grey literature poses difficulties for open sources information analysts and information professionals in general for several reasons. Generally, grey literature lacks strict bibliographic control, meaning that basic information such as author, publication date or publishing body may not be easily discerned. Similarly, the nonprofessional layouts and formats, low print runs, and non-conventional channels of distribution of grey literature make the organized collection of such publications challenging compared to journals and books, so identify and obtain information through gray literature requires the employment of expert intermediaries²¹⁸.

10. Commercial Imagery: The commercial imagery processing – managing and deliverance industry continues to grow technologically while matures, through development and deployment into orbit more and more satellites (for a variety of usage, such as: military, civilian, commercial and scientific applications). Already there are more than eleven private companies that have put in orbit and commercialize high-resolution commercial remote sensing satellites. Their products are available to anyone who has the ability to pay.

11. Overt Human Experts and Observers: Despite the rapid technological evolution and development there are still countries that have failed to benefit from it, such countries are the so called third world countries. For instance, in most of the countries which are on the African continent it is difficult (and in some cases even impossible), to obtain any type of information (especially published ones).

²¹⁶ http://en.wikipedia.org/wiki/Gray_literature

²¹⁷ There are three definitions of the term, the “Luxembourg definition”, the “New York” and the most resent the “Prague definition” which is the one presented in this paper.

²¹⁸ The concept of grey literature has emerged since the 1970s. When Charles P. Auger published the first edition of his landmark work on "reports literature" in 1975, he did not use the term "grey literature".

For all the above reasons the ultimate “open source” is still considered the Human. A human observer or a team of observers with expertise in different fields (sociology, psychology, health, communication, and intelligence experts), is often the most efficient and the most inexpensive solution in order to “create” new open source intelligence that is responsive to a specific requirement from the requestor.

3.3.1 Open Source Reliability and Credibility.

There are three types of sources which are used to evaluate information, those are:

1. Primary sources: are referring to a document or physical object that was written or created during the time under study. These sources are present during an experience or time period and offer an inside view of a particular event. Primary sources characteristics are the following:

- ❖ Are generally categorized by content.
- ❖ Are either public or private.
- ❖ Are also referred to as an original source or evidence.
- ❖ In fact, are usually fragmentary, ambiguous, and difficult to analyze. The information contained in primary sources is also subject to obsolete meanings of familiar words.

Some types of primary sources are (but not limited to):

- ❖ Original documents, (excerpts or translations), such as diaries, constitutions, research journals, speeches, manuscripts, letters, oral interviews, news film footage, autobiographies, and official records.
- ❖ Creative works such as poetry, drama, novels, music, and art.
- ❖ Relics or artefacts such as pottery, furniture, clothing and buildings.
- ❖ Personal narratives and memoirs.
- ❖ Person of direct knowledge.

2. Secondary sources: a secondary source interprets, analyzes, cites, and builds upon primary sources. Secondary sources may contain pictures, quotes, or graphics from primary sources. Some types of secondary sources include publications such as:

- ❖ Journals that interpret findings.
- ❖ Textbooks.
- ❖ Histories.
- ❖ Magazine articles.
- ❖ Commentaries.
- ❖ Criticisms.
- ❖ Encyclopedias.

3. Authoritative sources: Accurately reports information from the leader, government, or ruling party.

4. Non authoritative sources: are generally unavailable and inaccessible by the public. Non authoritative sources are uncorroborated by multiple public sources of information. The non authoritative sources are included (but are not limited) to:

- ❖ Unreliable documents from self-published Web repositories such as blogs, Wikipedia, political sites, and commercial advertising.
- ❖ Material received via uncorroborated e-mail, hearsay, or statements solely in oral form.
- ❖ Informal personal communications such as letters to the editor and opinion essays.

Non authoritative sources lack reliability and trustworthiness and seldom stand apart from authoritative sources. The information provided by non authoritative sources generally does not support topics agreed upon as being true and reliable in academia.

When an OSINT analyst evaluates sources of information to determine reliability and credibility he/she must consider the following:

- **Identity:** Who produced the information (for example a student, teacher, political organization, a reporter, etc)?
- **Authority:** How much does the source know about the information?
- **Motive:** Why was the information published?
- **Access:** Did the source have direct access to the event or information?
- **Timeliness:** What is the date of the information or when was the information published?
- **Internal and external consistency:** Does the information contradict governmental policies among local citizens?

So the analysts should always evaluate a prior information, (both reliability and credibility, of the source and the content), before they use it. Open-source reliability ratings range from A (reliable) to F (cannot be judged) as shown at the following table:

A	Reliable	<u>No doubt</u> of authenticity, trustworthiness, or competency, has a history of complete reliability.
B	Usually Reliable	<u>Minor doubt</u> about authenticity, trustworthiness, or competency; has a history of valid information most of the time.
C	Fairly reliable	<u>Doubt</u> of authenticity, trustworthiness, or competency, but has provided valid information in the past.
D	Not usually reliable	<u>Significant doubt</u> about authenticity, trustworthiness, or competency, but has provided valid information in the past.
E	Unreliable	<u>Lacking</u> authenticity, trustworthiness, and competency; history of invalid information.
F	Cannot be judged *	<u>No basis</u> exists for evaluating the reliability of the source.
<p>*Note: A first - time source used in the creation of OSINT is given a source rating of F, this does not mean the source is unreliable, but OSINT personnel have no previous experience with the source upon which to base a determination.</p>		

Table 19: Open Source Reliability Ratings²¹⁹.

Similar to open-source reliability are the credibility ratings which range from “1” (confirmed), to “8” (cannot be judged), as shown at the following table:

²¹⁹ Army Techniques Publication No. 2-22.9 (FMI 2-22.9): “Open Source Intelligence”, Headquarters Department of the Army Washington DC, 10 July 2012.

1	Confirmed	<u>Confirmed</u> by other independent sources, logical in itself, consistent with other information on the subject.
2	Probably true	<u>Not confirmed</u> , logical in itself, consistent with other information on the subject.
3	Possibly true	<u>Not confirmed</u> , reasonably logical in itself, agrees with some other information on the subject.
4	Doubtfully true	<u>Not confirmed</u> , possible but not logical, no other information on the subject.
5	Improbable	<u>Not confirmed</u> , not logical in itself, contradicted by other information on the subject.
6	Misinformation	<u>Unintentionally false</u> , not logical in itself, contradicted by other information on the subject, confirmed by other independent sources.
7	Deception	<u>Deliberately false</u> , contradicted by other information on the subject, confirmed by other independent sources.
8	Cannot be judged *	<u>No basis</u> exists for evaluating the validity of the information.
<p>*NOTE: If the information is received from a first-time source, it is given a rating of eight and, like the reliability ratings scale, does not mean the information is not credible but that OSINT personnel have no means to verify the information.</p>		

Table 20: Open Source Content Credibility Ratings²²⁰.

Deception and Bias is something that an OSINT analyst should always be aware of. OSINT exploitation, most of the times do not acquire information by direct observation, so the OSINT analyst has to rely on secondary sources to acquire and disseminate information. Secondary sources, such as government press offices, commercial news organizations, and nongovernmental, can intentionally or unintentionally add, delete, modify, or “filter” the information (which might be a text, a recorded message, an interview, etc), made for the general public. There is also the possibility that these sources might also convey two messages, one in English and one in the local speaking language with the intent to confuse or deceive the messages recipients, causing confusion and vacillation.

From what we have already described we can reasonably conclude that it is crucial for the analyst to know the “background” of open sources exploitation and communication techniques and methods in order to be able of to distinguish communication objectives, factual information, identify bias, or highlight deception efforts against the potential information recipients.

²²⁰ Army Techniques Publication No. 2-22.9 (FMI 2-22.9): “Open Source Intelligence”, Headquarters Department of the Army Washington DC, 10 July 2012.

	Passive	Aggressive	Passive-Aggressive	Assertive
Behavior	<ul style="list-style-type: none"> Keeps quiet. Does not say what is actually felt, needed, or wanted. Frequently puts oneself down. Apologizes when expressing oneself. Denies feelings of disagreements or indifferences. 	<ul style="list-style-type: none"> Expresses feelings and wants as though any other view is unreasonable or stupid. Dismisses, ignores, or insults the needs, wants, and opinions of others. 	<ul style="list-style-type: none"> Fails to meet the expectations of others through 'deniable' means (such as forgetting or delays). Denies personal responsibility for actions. 	<ul style="list-style-type: none"> Expresses needs, wants, and feelings directly and honestly. Does not assume correctness or everyone feels similar. Allows others to hold other views without dismissal or insults.
Nonverbal Communication	<ul style="list-style-type: none"> Minimizes oneself. Looks down, hunches shoulders, avoids eye contact. Speaks softly. 	<ul style="list-style-type: none"> Enlarges oneself and appears threatening. Eye contact is fixed and penetrating. Voice is loud, perhaps shouting. 	<ul style="list-style-type: none"> Typically mimics the passive style. 	<ul style="list-style-type: none"> Body is relaxed, and movements are casual. Eye contact is frequent but not glaring.
Beliefs	<ul style="list-style-type: none"> Others' needs are more important. Others have more rights. Others' contributions are more valuable. 	<ul style="list-style-type: none"> Personal needs are more important and more justified than others'. Others have no personal rights. Personal contributions are more valuable. 	<ul style="list-style-type: none"> Entitled to get own way, even after making commitments to others. Not responsible for personal actions. 	<ul style="list-style-type: none"> Everyone's needs are equally important. Everyone has equal rights to be expressive. Everyone has valuable contributions. Responsible for personal behavior.
Emotions	<ul style="list-style-type: none"> Fears rejection. Feels helpless, frustration, and anger. Bears resentment toward others' mistreatment. Has reduced self-respect. 	<ul style="list-style-type: none"> Angry or powerful at the time of victory. Feels remorse, guilt, or self-hatred for hurting others. 	<ul style="list-style-type: none"> Fears assertiveness. Resents the demands of others. Fears of being confronted. 	<ul style="list-style-type: none"> Feels positive about oneself and the treatment of others. High level of self-esteem.
Goals	<ul style="list-style-type: none"> Avoids conflict. Pleases others at any expense. Gives others control. 	<ul style="list-style-type: none"> Wins at any expense to others. Gets control over others. 	<ul style="list-style-type: none"> Gets personal way without having to take responsibility. 	<ul style="list-style-type: none"> Self-respect is kept by everyone. Expresses oneself without having to win all the time. No one controls anyone else.

Table 21: Comparison of Communication Types²²¹.

²²¹ Army Techniques Publication No. 2-22.9 (FMI 2-22.9): "Open Source Intelligence", Headquarters Department of the Army Washington DC, 10 July 2012.

3.4 The Open Source Intelligence Cycle “The 4D’s”.

The open source intelligence process consists of discovery, discrimination, distillation, and dissemination, also known as the 4 D’s (see the following figure). If the open source analyst applies this analytical approach to the traditional single source intelligence cycle he/she could have easily access and harness private sector knowledge using only legal and ethical means, generally at a very low cost and in less time in comparison to covert technical or clandestine human collection techniques and methods. Because in most cases the time factor is crucial for the requestor the open source intelligence cycle becomes a vital factor for every manager, executive, military commander and policy maker in general.

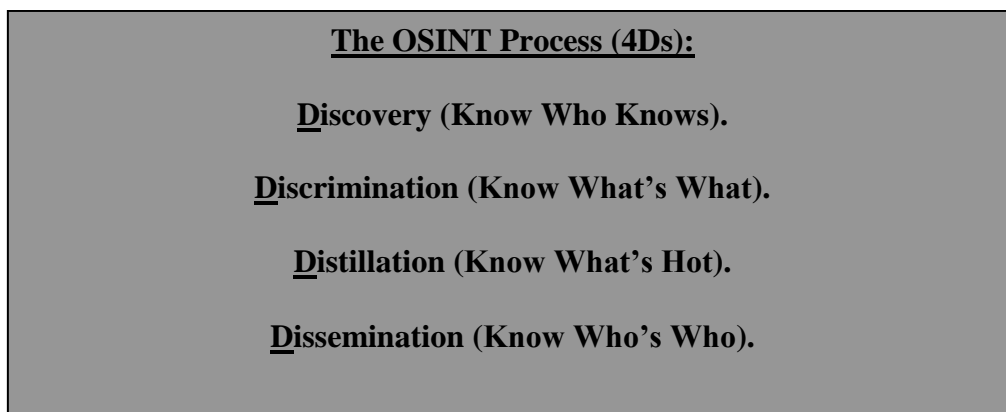


Table 22: The OSINT Process (4D’s)²²².

We will not proceed to a detailed analysis of how an analyst can adjust the “Intelligence Cycle”, to the OSINT discipline because the applications of the OSINT discipline are typically unlimited and the form of “Intelligence Cycle” depends on the application “field²²³”. For this reason we will make a general reference to some general principles that both the requestor and the analyst should adhere.

The biggest challenge for the requestor is the creation and maintenance of a rigorous and disciplined process that ensures and also defines the requirements that must be addressed through open sources. The requestor should evaluate and carefully prioritize his/her specific information needs (always depending on the context – field of interests, plans and intentions), and should give the clearest possible way to the analyst/analysts to understand what is really want to know and why. Only if the analysts clearly understand the context of the requestor’s interests and also the directions of administrative requirements can truly be focused and start a flexible intelligence collection effort.

The foundation of “Intelligence Process” is the “Research process”, which is the matching of validated intelligence requirements to available intelligence sources and disciplines with the aim of producing a product which answers to a valid need. Once an intelligence need has been clearly identified (by the analysts), the intelligence staff should determine if that specific intelligence need can be satisfied through their “organic” resources - information or if there is a need of collecting new information or if a combination of the above approaches is required. The intelligence collection requires the transformation of information need to an information requirement and then devising a collection plan to address this need. This plan should be adapted to exploit in the best way possible the allocated sources. Then the intelligence staff proceeds to the selection of the best available information sources and the collection process begins. The information analysts should also have at their disposal an appropriate information management plan, as there is always the risk that the sheer volume of available information could saturate the analytical capacity of any intelligence department (regardless the staff abilities or their number).

²²² Nato Open Source Intelligence Handbook, November 2001.

²²³ There are slightly differences to the “Intelligence Cycle” which are dependent to the analyst “employer” or to the requestor’s field of interest (military, law enforcement, non – governmental organizations, etc).

The next phase is the information processing which is followed by the phase of information exploitation. Both phases require the application of human judgment (by the analysts), in order to sort out the important from the unimportant, the timely from the dated, the relevant from the irrelevant, the trusted from the un-trusted.

The following phase is the analysis phase. At this phase it is essential that the analysts should remain focused and determine the origin of the information that has been gathered - collected and the degree of trust that can be assigned to that information. The analysts should always be aware in order to be able to distinguish between information (speculations), and facts. If the original source material is not provided in full text, it is important to make reference to it and provide an assessment of the source's credibility. Analysts should always include to their open source reporting the original information sourcing. A full description of how the open source information have been collected, identified, also the timing of acquisition, the timing of the final product production, all these represent half the value of an OSINT product.

The next step through the intelligence cycle is the production phase. At this phase the analysts integrate data into a coherent whole, put the evaluated information in context, and produce finished intelligence products that include assessments with the form of reports. The themes of these reports can vary and include (but not limited to): warnings for decision makers about upcoming risks and threats, political issues, low intensity regional conflicts, etc. Those reports can be in written format, which might be brief, (one page or less), or lengthy studies and papers. A major difference between the OSINT process and the traditional "classified" intelligence process exists in how "reports" are treated. In the traditional "classified" intelligence process, reports are the end of the process on the contrary in the OSINT process, they are the beginning. Usually a report has the following format (for instance, about a regional low intensity conflict): The report will consist of more than one section, for example, it will include sections that will address:

- ❖ Sociopolitical issues, such as: differences between religious or other minorities,
- ❖ Political issues, such as: foreign affairs of the country of interest with neighboring countries, the prevailing political situation (relations of the government with the opposition parties),
- ❖ Military affairs, such as: the state of military forces in the country of interest or the existence of militias - paramilitary forces,
- ❖ Health issues, such as the need for medical care and humanitarian assistance in general, etc.

Each section should in turn be followed by a brief summary and a section with the reports writer commentaries, (no more than one paragraph each). The summaries of each section can be used to create a comprehensive summary of the report. At the first page of the reports it should always be indicated the date and time during which the collection, (not the production), of the information and the time frame (days or hours), which the report covers. Reports can be organized based on the information source, (Internet, Commercial Online, Grey Literature, etc.) or according to their subjects. The reports should also indicate the full contact details of the author or the reviewer of the report so that the reader/readers may, (if the need should arise), communicate quickly requesting additional information from the author or the reviewer's report.

The last phase of the "Intelligence Cycle" is the Dissemination, this phase concerns the distribution of the finished intelligence product to the requestors – consumers. There are limitations concerning the product dissemination which are based on the security policies of the organization producing it. While some OSINT products may be shared openly, others may provide details of interests or intentions and judgements and should therefore be restricted in their dissemination. The dissemination policy should be driven by the mission requirements. Then the recipients of the finished intelligence product take their decisions based on those intelligence products, and these decisions may lead to the levying of more requirements, thus triggering the "Intelligence Cycle". The task of the analysts is not over, at this stage an evaluation of the information products (which have been delivered to the requestor – customer), must be performed in order to understand if those products

manage to cover the requestors – customer requirements, the process ends with a debriefing of the intelligence staff by their manager.

3.5 OSINT Advantages and Disadvantages.

Like all the other disciplines, OSINT discipline has advantages and disadvantages with which we are going to deal in this section. We are going to begin with the advantages which are the following:

- ❖ The first and perhaps most important advantage (especially now with the global economy in recession), is the cost. The information from open sources is clearly cheaper to be acquired, processed and distributed over other methods and disciplines of collecting information that require specialized means of collection (such as satellites), or illegal – clandestine and unethical methods. Small countries have neither the expertise nor the financial ability to proceed with the development of the required specialized technical means (special airborne platforms, satellites, etc.) can be based on open sources of information in order to satisfy their information needs, for instance high definition and resolution aerial images, (economical imagery intelligence via OSINT), can easily be found through Google Earth and similar private services, inexhaustible source of information for the analysts can also be the letter pages of every quality newspaper (with broad topics, from economic to social and political issues and analysis).
- ❖ The second advantage is the shorter time of information acquisition, (in comparison with other intelligence disciplines), and thereof shorter time of processing and inference. The shortest time of collection and processing is achieved because information from open sources are readily available and accessible, there are private agencies and organizations (lexisnexis, oxford analytica, BBC monitoring, etc), which provide, (whether paid or not), ready information and analysis on a variety of topics and issues.
- ❖ The third advantage is the Accessibility and Availability. The products resulting from open information sources elaboration, (because of the legal and ethical manner of collection), may be "fungible" between various governmental and non-governmental organizations, services and agencies worldwide, contributing in this way to the early identification, prevention and confrontation (if necessary), of emerging risks and threats (e.g. new forms of global terrorism). Also because of the OSINT's products high accessibility and availability, those products can contribute to public's situational awareness about upcoming risk and threats (concerning economical, environmental, security issues and topics, etc).
- ❖ The "legality" of OSINT products. As mentioned above, the legal and ethical methods used for collecting information from open sources make them "automatically legitimate" and therefore usable in legal proceedings without the risk of exposure sensitive intelligence assets or clandestine operations. OSINT products can also be used to "support" and confirm the credibility and reliability of information derived from other classified information sources without having to reveal those classified sources.

In the next paragraph of this section we will refer to the disadvantages of OSINT discipline, which are the following:

- ❖ The first drawback of OSINT discipline is perhaps an oxymoron since, as we showed above is both an advantage. The advantage is converted into a disadvantage when taking into account the vast amount of available information that should be elaborated by the analysts. The sheer volume of information implies a great effort on the part of the analyst to divide factual information from "noise" of communication. All this in turn requires more time and effort by the analyst while causing fatigue and faster drop of his/her performance.

- ❖ Chances of misinformation or deception. For example if many TV-broadcast, print media and News Agencies are emphasizing on an “event” or an issue does not automatically mean that it is true or that their judgments are objective and accurate. It is a global policy phenomenon that governmental or non-governmental organizations and agencies are using the mass media in order to channel and present their own “version” of the truth, trying to influence or to misinform the public.
- ❖ The last disadvantage of OSINT discipline is that the OSINT products do not always manage to provide actionable intelligence on the tactical or operational level. While it may provide a rich source of information on the ideology and motivations of a terrorists group it will not reveal the exact location of the group members or to the tactical level the information needed to capture them.

3.6 OSINT Through out the World.

Some countries have soon realized the value of open source information and the significant role of OSINT both as a discipline and as a keystone to an All – Source Intelligence Discipline and managed to integrate and fully exploit the opportunities provided by the OSINT discipline. Those countries can be regarded as pioneers in this area of expertise.

3.6.1 Europe.

Perhaps the best example of a European country that managed to integrate and exploit the opportunities and advantages offered by collecting information from open sources is Sweden. The Swedish government has created an informal committee known as “Swedish open Source Coordination Forum”. The purpose of this committee is the coordination of all the available Swedish resources, (governmental and non-governmental, corporate, technological, scientific, educational, etc.), in order to optimize the collection effort and sharing methods and means to gather information from open sources. The Swedish government is considering the “privatization” of the existing governmental services motivated by the need to reduce governmental costs.

Britain is among the first countries that have created an Open Source Information Center within the Ministry of Defense.

France considered a pioneer - leader in economic intelligence collection and in education – training applied to those fields. The French government continuous to play a “key role” in “sponsoring” and organizing national economic and information strategies and in encouraging academic education applied to the field of economic intelligence. In October of 1993 the French government sponsored an Intelligence Conference which was dedicated to OSINT issues.

The Netherlands proceeded to the reorganization of its Intelligence Disciplines in order to balance information collection from open sources and other technical and cal destine collection methods and disciplines. The Netherlands “model” consists on the usage of a “Task Force” approach, which begins with the information collection from open sources, continuous with optimizing Internet exploitation from specialized staff while analysts perform the decentralized exploitation of the specifically identified sources and adjusting the information products to specific requirements.

3.6.2 Middle East.

Israel has advanced in the creation of an appropriate legislative framework (by introducing laws like the one known as “Freedom of Information Act”), thus achieving to develop in a “host” country for information brokers, managing to acquire large quantities of information at almost no cost.

3.6.3 Asia.

In the wider Asian area, the countries that are considered leaders in the exploitation of OSINT are Japan and Singapore.

Japan covers its informational needs, (from open sources), based primarily on the private sector and in particular to the trading companies with an estimated daily collection of more than 6000 thousand newsprint – size papers. Japan has also managed to improvise Intelligence Management, every major Japanese organization - corporation collects information from open sources (both from governmental and private sector), all over the world and automatically those information are routed to the appropriate Japanese intelligence organizations and services for further elaboration and exploitation.

Singapore has evolved to a major banking center, while soon realized the need to provide a robust information environment for its business community. To achieve this, Singapore “invested” in the development of the appropriate infrastructures (to all necessary fields), methodologies and technological aspects, focusing all efforts primarily on developing capacity to collect financial information through open sources of information. One of the first measures to this direction was the establishment and operation of the National Computer Board (NCB)²²⁴. The NCB has its representatives in every governmental, their job is to collect all types of open source information and reroute – integrate them to the appropriate governmental databases for further exploitation.

3.6.4 North America.

Canada has an “informal world record”, stating that 80% of its information needs comes from collecting and processing information from open sources. Canada is also considered one of the leading powers in the production and distribution of strategic information derived from open sources.

The United States, (as already mentioned), failed to timely adapt to new kinds of threats and it had to happen, (unfortunately), an “unpleasant incident” (the attack of 9/11), to expedite the necessary changes²²⁵. The 9/11 events led to the recommendation of the 9/11 Commission. Commission’s mandate was to investigate the causes that led to the detection and prevention failure of the 9/11 attacks. In its final report (filed on July of 2004), the 9/11 Commission recommended the creation of an open source intelligence agency, but without further detail or comment. Another recommendation for creating an Open Source Directorate (at the Central Intelligence Agency, CIA) had been made (March of 2005), by the Weapons of Mass Destruction, (WMD), Commission²²⁶, (also known as the Robb-Silberman Commission).

Following these recommendations, the Director of National Intelligence (DNI), announced the creation of the Open Source Center (OSC). The OSC administratively “belongs” to CIA intelligence center which is located in Reston, Virginia, and its mandate is providing intelligence analysis from open source information, (including gray literature, through OSC's headquarters and overseas bureaus). It was established on the 1st of November 2005, by the Office of the Director of

²²⁴ The National Computer Board (NBC): was formed on 1 September 1981 under the auspices of the Ministry of Finance, one of the board’s most crucial functions was to implement the computerisation of the civil service. NCB also served as the central authority in promoting, implementing and co-ordinating information systems development work in government ministries. http://en.wikipedia.org/wiki/Infocomm_Development_Authority_of_Singapore.

²²⁵ Two attempts of reshuffle the American Intelligence Services had been already preceded. The first took place in the fall of November 1992, (by Senator David Boren who was at this time the Chairman of the Senate Select Committee on Intelligence), and it was the sponsorship of the National Security Act. The National Security Act of 1992 was an attempt to achieve the reformation of the U.S. Intelligence Community while the House version of the legislation was included the proposal of setting up and operating a separate Open Source Office. The second attempt had been made by the Aspin-Brown Commission. The Committee stated in 1996 that US access to open sources was “severely deficient” and that this should be a “top priority” for both funding and Director of Central Intelligence (DCI) attention.

²²⁶ The official name of this Commission is: Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction Commission. It was created by Executive Order 13328 signed by U.S. President George W. Bush in February 2004, the commission’s mandate was to Explore the causes that led to the false US Intelligence Services impression that Iraq possessed Weapons of Mass Destruction and also to collect intelligence considering the Afghanistan’s and Libya’s Weapons of Mass Destruction programs, as well as to examine the capabilities of the US Intelligence Community to address the problem of WMD proliferation and “related threats”.

National Intelligence. The OSC is also tasked with improving the availability of open sources to intelligence officers and other government officials. To achieve its tasks the OSC provides its “products” through the online news service World News Connection.

Concluding Remarks.

Since their appearance the intelligence services, (through out the world), have managed to establish themselves as one of the major elements of National Security. During the Second World War the first intelligence agencies and services have been appeared, (as we know them today). Those agencies and services were mainly based their collection and intelligence processing needs to the human factor and secondary to technological means of information acquisition. The end of WW II had resulted the separation of the world into two “spheres of influence”, from the one side they were the states that have been attached to the U.S. “bandwagon” (England, France, Italy, etc.) and from the other side, states that have been attached to the Soviet Union “bandwagon” (Poland, Bulgaria, Romania, etc.). The intelligence services of these states were oriented to “compete” one another, continuing to rely on the human factor and to the usage of clandestine methods to cover their intelligence needs. Technological developments gradually led to the emergence of new forms of intelligence disciplines such as IMINT, SIGINT, GEOINT, etc. Since 1950 the competition between the two “superpowers”, (USA and the former Soviet Union), and their allies increased in intensity and became known as the “Cold War”. The Cold War peaked in the late 80’s and came to an end in the early 90’s (the event which triggered the end of the Cold War was the collapse of the former Soviet Union). During those 40 years the competition between the two “superpowers” continued unabated, the competition for the final victory was also “channeled” to the intelligence services of both “superpowers” and their allies. The intelligence services throughout the duration of the Cold War was exclusively designed - oriented to achieve strategic and tactical advantages over their opponent, to achieve this they were relaying on “absolute secrecy”, the usage of clandestine techniques – methods and to covert intelligence operations. Huge amounts of money were spent in their efforts to prevail one over the other. This “unilateral” orientation had as result the creation of “stiff” organized intelligence services and agencies, unwilling to adapt to emerging challenges and threats.

The collapse of the former Soviet Union led to globally chaotic changes. Most of the former Soviet states “seceded” and claimed their democratization, thus creating political instability in many parts of the world, religious and political differences made their reappearance causing regional conflicts (e.g. in the former Yugoslavia, Kosovo, etc), increased fear of the spread of WMD, new forms of Terrorism etc. To all the above we can add the “forced” changes (reduction of available funds and staff), which have been caused by the Globalization and the global economic recession and crisis in the mid of 2000’s. Intelligence agencies and services, (especially in America), failed to timely adjusted to the new up coming risks and threats, so we were led to attacks such as those of 9/11 and the failure of preventing them.

Only in recent years intelligence agencies and services started to understand the need of restructuring their organizational structures, and to adapt to a more “flexible” cluster based on an “All Source Intelligence Discipline”. The “foundation” of this All – Source Discipline could be the Open Source Intelligence Discipline.

Appendixes.

Appendix A: The significance of a National OSINT Center.

As the economic crisis plaguing our country culminates, it increases the demands for governmental budget cuts. These financial cuts will certainly affect the “sensitive” (to national interests), field of National Intelligence Services. The intelligence services of our country will have to face the paradox of satisfying the growing need for intelligence while reducing both their staff and their budget. The crisis creates opportunities and for countries such as Greece, (which at the moment is experiencing perhaps the greatest crisis of its modern history), presents a golden opportunity, to invest in the exploitation of open information sources.

Another key – factor that demonstrates the significance of the OSINT as an intelligence discipline comes from the observation and study of recent regional crisis and conflicts, (low or high intensity), which are demonstrating the growing role that the “human factor” has, both for the collection – processing and the exploitation of information and also for the overall management of a crisis or a conflict²²⁷. Its obvious that the appropriate methodology and know-how already exists, we have already mentioned the examples of Israel, Sweden, France and the USA, countries with which Greece maintains good relations at all levels, and can help our country in the development of the appropriate and necessary infrastructure for the exploitation of information from open sources. The first steps in this direction are:

- ❖ The creation of an appropriate legal framework that will facilitate free and unhindered “trading” of information products while ensuring their “protection”.
- ❖ The second step, (to which we will focus on), is the establishment - creation and operation of a National OSINT Center.

Both of the above steps are equally important, as they are interdependent and mutual, the proper functioning of one depends on the functionality of the other and vice versa (just for the purposes of this work we will focus on the second).

Our country covers its information needs through the National Intelligence Agency and the respective military services of all three branches of the Greek Armed Forces²²⁸. The predecessor of The National Intelligence Service was the Central Intelligence Agency of Greece, this agency was founded at 1953²²⁹ and its organization was based solely on the standards of the US Central

²²⁷ The United States have already, (pioneers in this field are considered the US military intelligence services, which managed to adapt quicker to the upcoming threats and their tactical, strategic and operational demands), advanced to the development and adoption of an interdisciplinary model of collecting – gathering and exploitation of intelligence products, (this model have been already successfully applied to the military operations in Afghanistan).

²²⁸ The collection and processing of military type of information are the sole responsibility and authority of the General Staff of National Defense. To carry out its mission, the General Staff has access to the following services:

E Branch (Military Intelligence), which consists of:

- ❖ E1 Division: Its responsible for setting policy on collecting military intelligence, coordination of information gathering, commissioning work on organic units and intelligence through the General Staff Branches in other intelligence units of the Armed Forces, the standardization of products and intelligence cooperation with other stakeholders (national - allied - foreign countries), information on issues requests for information as part of the Unified System of Military Intelligence (according to Law 2292/95).
- ❖ E2 Division: Handles processing issues, analysis and exploitation of information and prepare a general national estimates and allied level. Propose to shaping the policy on information, cooperate in the exchange of information with foreign countries Information Services, International Organizations (NATO-EU) and prepares the information part of the Business Plans of the National Exercise.
- ❖ E3 Division: Its responsible for Occupational Safety and Counter – Intelligence in National and Allied level.
- ❖ E4 Division: Its responsible for the formulation of policy on information, promotion of cooperation in sharing information with information services of foreign countries, international organizations (NATO, EU, UN) and monitoring of transnational military information exchange agreements at the bilateral level.

Source: <http://www.geetha.mil.gr>.

²²⁹ Before 1953 the mission of gathering and processing was the sole responsibility of the Military Forces.

Intelligence Agency (CIA). Later the name was changed to the Central Intelligence Office. At 1986, the enactment of 1645 Law, (which was published on 26th of August 1986, and published at the Governmental Gazette No. 132A), the “Central Intelligence Office” was renamed to National Intelligence Service (NIS). According to Law 3649/2008, the mission of NIS is within the framework of the Constitution and laws of search, collect, process and notify the competent authorities of information, concerning:

- ❖ The protection and promotion of political, economic, military and general national strategic interests of the country.
- ❖
The prevention and treatment activities constitute a threat to democracy, fundamental human rights, territorial integrity and national security of the Greek State and the national wealth of the country.
- ❖ The prevention and treatment activities of terrorist organizations and other organized crime groups.

The NIS in time of mobilization, war or direct threat to national security its subject to the administration of the National Defense General Chief of Staff, who, through the NIS Director has full control in issues concerning the national defense and security of the country. In case of any action aimed at violent overthrow of the democratic government, the NIS, (following a decision of Government Council for Foreign Affairs and Defense, GCFAD), acts as central information management of the country.

As is readily apparent from the presentation of the above data and the charts of the intelligence services, they don't have a “specialized” department in collecting and processing information from open sources. Therefore it is concluded that we are at the most appropriate time to proceed with the reorganization of our Intelligence Services, both governmental and military²³⁰. This reorganization could be based on international standards (but tailored to our specific needs and requirements), we can also proceed to the adoption of an “All – source” Intelligence collection and exploitation model which can be founded at the OSINT discipline standards.

In order to achieve this “transformation” we can proceed to the establishment of a Joint OSINT Center. By using the term “Joint” we want to emphasize on the interdisciplinary that should govern the OSINT Center. An OSINT Center could be incorporated into an existing national security framework or as an autonomous “entity”. This center will be staffed by personnel²³¹ from both the National Intelligence Agency (NIA) and by relevant military intelligence staff (from all three branches of the Hellenic Armed Forces) and also qualified – specialized personnel with expertise in certain areas – fields (these personnel could be derived from the private sector or to be engaged on contract work if required by the circumstances). A joint OSINT center could be tasked with the following:

- ❖ Provide support to the all-source capabilities of clandestine intelligence services.
- ❖ Combine information products from different intelligence disciplines (HUMINT, SIGINT, GEOINT, etc) and produce integrated intelligence products.
- ❖ To channel these consolidated - integrated products to governmental and military services and agencies.

²³⁰ The Greek Minister of National Defense in collaboration with the Chief of General Staff of Defense announced the creation of the Multidisciplinary Military Intelligence Service and also the creation of an OSINT exploitation department.

²³¹ Staff such as: information professionals, intelligence analysts, IT and computer experts, etc.

- ❖ Design and adopt a suitable computer software and hardware for better and faster collection, compilation and distribution of intelligence products.
- ❖ Develop and communicate best practices concerning the collection, management, analysis, and dissemination of information and intelligence.
- ❖ Develop the methodology and memorandum actions which will be used by all intelligence services.
- ❖ Establish collaborative partnerships in order to acquire know – how and then adapt it to our specific requirements and needs.
- ❖ Track trends in Information Technology (IT).
- ❖ Establish collaborative partnerships with non-government actors, and institutions - organizations on which our country is a member (NATO, United Nations Organization (UNO), etc).
- ❖ Provide training and education to governmental personnel and researchers.
- ❖ To monitor – track international developments and trends regarding informational and intelligence issues (technological, managerial, organizational, etc) and recommend the adoption of the most appropriate ones.
- ❖ The center will have a “commercial department”, project of this segment will be the production of intelligence products on behalf of third parties (for a fee).
- ❖ And list but not last, to conduct early – warning and long – term foresight risk and threat assessments and activities.

The investment that will be required for the establishment and maintenance of such a center would definitely be considered “prohibitive” (due to the difficult economic situation in which our country is), but it is necessary as it will act as a “force multiplier” for our country, and also because, in ways such as those mentioned above can be partly finance itself and be self – sustaining.

Appendix B: Axioms for an Intelligence Analyst²³².

- **Believe in your own professional judgment:** You are the expert, believe in your work and stand your ground if the intelligence supports your position.
- **Be a risk taker:** Do not be afraid of being wrong when forecasting trends or events. Taking risks is part of your job description. Only by taking risks you can maximize your value to your agency.
- **It is better to make a mistake than to do nothing at all:** If you are wrong, and the facts call for it, admit it. Only those who don't do anything make no mistakes.
- **Avoid “mirror imaging” at all costs:** Mirror imaging is projecting your thought process or value system onto someone else. You must learn to think like your “targets”.
- **Intelligence is of no value if it is not disseminated:** Communicate the intelligence, conclusions and recommendations clearly and effectively and in a timely manner. What your client does not know has no value.
- **When everyone agrees on an issue, something probably is wrong:** It is rare and not natural for a group of people in the intelligence community to fully agree on anything. If it does occur, it's time to worry.
- **Your client does not care how much you know:** tell them just what they need to know.
- **Excessive details merely obscure the important facts.**
- **“Form” is never more important than the substance:** A professional appearance and appropriately selected formats are important, but they do not outweigh substance. Clients want to know what intelligence means, and they want it when they need it.
- **Aggressively pursue collection of information that you need:** Never settle for less than all you need. If you fail to get access to the vital data source for any reason, you will be held responsible.
- **Do not take the editing process personally:** If editorial changes do not alter the meaning of your message, accept them. If they do, speak up. Even then, it might be that a brighter mind has seen what you have missed. Believe in your product, but be self – critical.
- **Know your intelligence community counterparts and talk to them:** You are not competitors you are of the same breed. Become part of the network. Do not pick up the phone only when you need something.
- **Do not take your job, or yourself, too seriously:** Avoid burnout. Writing you off as an asset will be a net loss to your agency (although it may not immediately see it exactly like this). The welfare of your family and your health is more important than scaling another rung on the career ladder. Your role in the larger order of things is not self – important. Your commitment, perseverance and dedication to the job will bring results only over a long term.

²³² United Nations Office on Drugs and Crime: “Criminal Intelligence: Manual for Front-line Law Enforcement”, United Nations, December 2010.

Appendix C: Ten Standards for Analysts²³³.

- Analysis should be an integral part of every major investigation the agency pursues.
- Analytical products should contain, as a minimum, a written report. Visual products may also be presented, but are only acceptable as an addition to, rather than in replacement of a written report.
- Analytical products should contain conclusions and recommendations. These are presented to management for their consideration regarding decision-making.
- The development of an analytical product requires the application of thought to data. Data compilation that does not reflect comparison or other considerations is not analysis.
- Analytical products must be accurate. Consumers must be able to rely on the data provided to them by analysts.
- Analysis must be produced in a timely manner.
- Analytical products should reflect all relevant data available through whatever sources and means available to the analyst.
- Analysis should incorporate the best and most current computer software and hardware, compilation, visualization, and analytical techniques available in the analyst's environment.
- Analysis should both reflect, and be evaluated upon, their qualitative and quantitative contribution to the mission and priorities of the agency or organization for which they are being produced.

²³³ United Nations Office on Drugs and Crime: "Criminal Intelligence: Manual for Front-line Law Enforcement", United Nations, December 2010.

APPENDIX D: Categories of Misperception and Bias²³⁴.

- **Evoked-Set Reasoning:** That information and concern, which dominates one's thinking based on prior experience. One tends to uncritically relate new information to past or current dominant concerns.
- **Prematurely Formed Views:** These spring from a desire for simplicity and stability, and lead to premature closure in the consideration of a problem.
- **Presumption that Support for One Hypothesis Disconfirms Others:** Evidence that is consistent with one's pre-existing beliefs is allowed to disconfirm other views. Rapid closure in the consideration of an issue is a problem.
- **Inappropriate Analogies:** Perception that an event is analogous to past events based on inadequate consideration of concepts or facts or irrelevant criteria. Bias of "Representativeness".
- **Superficial Lessons From History:** Uncritical analysis of concepts or event, superficial causality, overgeneralization of obvious factors, inappropriate extrapolation from past success or failure.
- **Presumption of Unitary Action by Organizations:** Perception that behavior of others is more planned, centralized, and coordinated than it really is. Dismiss accident and chaos. Ignore misperceptions of others. Fundamental attribution error, possibly caused by cultural bias.
- **Organizational parochialism:** Selective focus or rigid adherence to prior judgments based on organizational norms or loyalties. Could be resulted from functional specialization. Groupthink or stereotypical thinking.
- **Excessive Secrecy (Compartmentation):** Over-narrow reliance on selected evidence. Based on concern for operational security. Narrows consideration of alternative views. Can result from or caused organizational parochialism.
- **Lack of Empathy:** Undeveloped capacity to understand others' perception of their world, their conception of their role in that world, and their definition of their interests. Difference in cognitive contexts.
- **Mirror-Imaging:** Perceiving others as one perceives oneself. Basis is ethnocentrism. Facilitated by closed systems and parochialism.
- **Ignorance:** Lack of knowledge. Can result from prior-limited priorities or lack of curiosity, perhaps based on ethnocentrism, parochialism, and denial of reality, rational-actor hypothesis (see next entry).
- **Rational-Actor Hypothesis:** Assumption that others will act in a "rational" manner based on one's own rational reference. Results from ethnocentrism, mirror imaging, or ignorance.
- **Denial of Rationality:** Attribution of irrationality to others who are perceived to act outside the bounds of one's own standards of behaviour or decision making. Opposite of rational-actor hypothesis. Can result from ignorance, mirror imaging, parochialism, or ethnocentrism.

²³⁴ Lisa Krizan: "Intelligence Essential for Everyone", Washington D.C, Joint Military Intelligence College, June 1999.

- **Proportionality Bias:** Expectation that the adversary will expend efforts proportionate to the ends he seeks. Interference about the intentions of others from costs and consequences of actions they initiate.
- **Wilful Disregard of New Evidence:** Rejection of information that conflicts with already-held beliefs. Results from prior commitments, and/or excessive pursuit of consistency.
- **Image and Self-Image:** Perception of what has been, is, will be, or should be (image as subset of belief system). Both inward-directed (self-image) and outward-directed (image). Both often influenced by selfabsorption and ethnocentrism.
- **Defensive Avoidance:** Refusal to perceive and understand extremely threatening stimuli. Need to avoid painful choices. Leads to wishful thinking.
- **Overconfidence in Subjective Estimates:** Optimistic bias in assessment. Can result from premature or rapid closure of consideration, or ignorance.
- **Wishful Thinking (Pollyanna Complex):** Hyper-credulity. Excessive optimism born of smugness and overconfidence.
- **Best-Case Analysis:** Optimistic assessment based on cognitive predisposition and general beliefs of how others are likely to behave, or in support of personal or organizational interests or policy preferences.
- **Conservatism in Probability Estimation:** In a desire to avoid risk, tendency to avoid estimating extremely high or extremely low probabilities. Routine thinking. Inclination to judge new phenomena in light of past experience, to miss essentially novel situational elements, or failure to re-examine established tenets. Tendency to seek confirmation of prior held beliefs.
- **Worst-Case Analysis (Cassandra Complex):** Excessive scepticism. Reflects pessimism and extreme caution, based on predilection (cognitive predisposition), adverse past experience, or on support of personal or organizational interest or policy preferences.

Bibliography – Internet.

Lowenthal M. Mark: “From Secrets to Policy”, 2nd & 3rd editions, CQ Press, Washington DC, 2006.

Robert D. Steele: “The New Craft of Intelligence”, OSS International Press, Oakton Virginia, April 2002.

Robert D. Steele: “Intelligence for Earth”, Earth Intelligence Network (EIN), Oakton Virginia, February 2010.

Robert D. Steele: “Relevant Information: A New Approach to Collection, Sharing and Analysis”, OSS Academy, March 1999.

Robert D. Steele: “Special Operations Forces Open Source Intelligence (OSINT) Handbook”, OSS International Press, Oakton Virginia, June 2004.

Robert D. Steele: “On Intelligence: Spies and Secrecy in an Open World”, Fairfax Virginia: AFCEA International Press, 2000.

Field Manual Interim, No 2-0: “Intelligence”, US Department of the Army, March 2010.

Field Manual Interim, No 2-22.9: “Open Source Intelligence”, US Department of the Army, December 2006.

Field Manual Interim, No 2-22.3: “Human Intelligence Collector Operations”, US Department of the Army, September 2006.

Army Techniques Publications, ATP 2-22.9: “Open Source Intelligence”, US Department of the Army, July 2012.

Joint Publication 2-01: “Joint and National Intelligence Support to Military Operations”, January 2012.

Joint Publication 2-03: “Geospatial Intelligence Support to Joint Operations”, March 2007 and June 2007.

Geospatial Intelligence, (GEOINT), Basic Doctrine, Publication 1-0, National Geospatial – Intelligence Agency, September 2006.

North Atlantic Treaty Organization, (NATO): “Open Source Intelligence Handbook”, November 2001.

North Atlantic Treaty Organization, (NATO): “Intelligence Exploitation of the Internet”, October 2002.

North Atlantic Treaty Organization, (NATO): “Open Source Intelligence Reader”, February 2002.

David L. Carter, Ph.D.: “Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies”, 2nd Edition, US Department of Justice: Office of Community Oriented Policy Services, January 2009.

Joint Military Intelligence Center: “Open Source Intelligence Professional Handbook”, October 1996.

Interagency Threat Assessment and Coordination Group (ITACG): “Intelligence Guide for First Responders”.

Dr. Andrew N. Liaropoulos: “A (R)evolution in Intelligence Affairs? In search of a new paradigm”, Research Paper: No. 100, June 2006, Research Institute for European and American Studies (RIEAS).

Harris Minas: “Can the Open Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the 21st Century”, Research Paper: No. 139, Research Institute for European and American Studies (RIEAS).

United Nations Office on Drugs and Crime, (UNODC): “Criminal Intelligence Manual for Front-line Law Enforcement”, United Nations, December 2010.

International Foundation for Protection Officers, (IFPO): “Intelligence as an Investigative Function”, Robert Metscher and Brion Gilbride, August 2005.

Law Enforcement Intelligence, Chapter 5: “The Intelligence Process in Crime Investigation”, <http://www.fas.org/irp/agency/doj/lei/chap5.pdf>.

Law Enforcement Intelligence, Chapter 10: “Intelligence Requirements and Threat Assessment”, <http://www.fas.org/irp/agency/doj/lei/chap10.pdf>.

Open Knowledge Foundation: “Open Data Handbook Documentation”, Release 1.0.0, November 2012.

Ben Benavides: “Targeting Tomorrow’s Terrorist Today Through Open Source Intelligence”, February 2009.

Ben Benavides: “Open Source Intelligence (OSINT) 2oolKit On The Go”, September 2012.

Reg Whitaker: “Security and Intelligence in the Post – Cold War”, <http://socialistregister.com/index.php/srv/article/view/5610#.UW-4QEokKSo>.

“The Evolution of the U.S. Intelligence Community-An Historical Overview”, <http://www.fas.org/irp/offdocs/int022.html>.

Sean Gregory: “Economic Intelligence in the Post-Cold War Era: Issues for Reform”, <http://www.fas.org/irp/eprint/snyder/economic.htm>.

Stephen H. Campbell, B.Sc.: “Intelligence in the Post-Cold War Period: Part I: The Changed Environment”, <http://www.afio.com/publications/Campbell>.

Jason B. Jones: “The Necessity of Federal Intelligence Sharing with Sub - Federal Agencies”, http://www.trolp.org/main_pgs/issues/v16n1/Jones.pdf.

Romanian Intelligence Service: “Open Source Intelligence Handbook”, George Cristian Maior (Director of the Romanian Intelligence Service), http://www.sri.ro/upload/Ghid_OSINT_EN.pdf

Shulsky N. Abram and Gary J. Schmitt: “Silent Warfare: Understanding the World of Secret Intelligence”, 3rd edition, Washington DC: Potomac Books, 2002.

William M . Darley: “Clausewitz’s Theory of War and Information Operations”, <http://www.au.af.mil/au/awc/awcgate/jfq/4015.pdf>, retrieved 14-04-2013.

George Z. Roger and Bruce B. James B: “Analyzing Intelligence – Origins, Obstacles and Innovations”, Georgetown University Press, April 2008.

Robert M. Clark: “Intelligence Analysis: A Target-Centric Approach”, published by Cq Pr, July 2003.

Jerry H. Ratcliffe: “Intelligence-led Policing”, Willan, March 2008.

Krizan Liza: “Intelligence Essentials for Everyone”, Books for Business, 2003.

Douglas Bernhardt: “Competitive intelligence: How to acquire and use corporate intelligence and counter-intelligence”, FT Prentice Hall, 2003.

Rodger Nevill Harding: “Corporate Intelligence Awareness : Securing the Competitive Edge”, Multi-Media Publications Inc., 2006.

Berkowitz Bruce and Alan Goodman: “Best Truth. Intelligence in the Information Age”, New Haven and London: Yale University Press, 2000.

2009 National Intelligence – a consumer’s guide; http://www.intelink.ic.gov/wiki/Intelligence_Community_Customer_Handbook

Jardines E. A: “Theory and history of OSINT: Understanding open sources”.

Magdalena Adriana Duvenage: “Intelligence Analysis in the Knowledge Age”, Stellenbosch University March 2010. <http://www.scholar.sun.ac.za/.../duvenage-m-a-2010.p..>

<http://www.afio.com/> (AFIO - Association of Former Intelligence Officers).

<http://www.cicentre.com/> (CI Centre for Counterintelligence and Security Studies).

<http://www.fas.org/irp/index.html> (Federation of American Scientists).

<http://www.odci.gov/csi/index.html> (CSI - Center for the Study of Intelligence).

<http://www.oss.net/extra/page/> (Open Source Solution).

<http://www.intelink.ic.gov/wiki/Intelligence>

[http://www.intelink.ic.gov/wiki/Intelligence Sources and Methods](http://www.intelink.ic.gov/wiki/Intelligence_Sources_and_Methods)

http://www.intelink.ic.gov/wiki/Intelligence_community

<http://en.wikipedia.org>

<http://el.wikipedia.org>

<http://www.onstrat.com/osint/>

<http://www.rieas.gr>

<http://www.oxfordhandbooks.com/>

<http://www.phibetaiota.net>

<http://osint.deepwebtech.com/categories.html>

<http://www.oss.net>

<http://deep-web.org/osint/intelligence-analyst-resources-and-white-papers/>

<http://www.opsecacademy.org>

<http://publicintelligence.net>

<http://theosintjournal.blogspot.gr>

<http://bdnewsnet.com/war-room/category/open-source-intelligence-analysis/>

<http://www.uk-osint.net/>

<http://www.uzsi.cz/en/open-source-intelligence-osint.html>

<http://futuresworkinggroup.cos.ucf.edu>

<https://courseware.e-education.psu.edu>

<http://www.dps.state.ia.us>

<http://www.dodccrp.org>

<http://www.4sing.com/en/download/turning-osinf-into-intelligence.pdf>

<http://www.drtoconnor.com/4125/4125lect01b.htm> : ANALYTICAL METHODS IN INTELLIGENCE.

<http://www.globalsecurity.org/intell/library/policy/army/fm/34-3/fm34-3.pdf>

http://www.intstudycen.com/docs/strat_meth_guide.pdf

<http://www.51lunwen.com/download/country/australia/7-The how to of intelligence.pdf>

<http://www.americanforeignrelations.com/E-N/Intelligence-and-Counterintelligence-The-intelligence-cycle.html>

<http://www.nelacademy.nhs.uk/media/30503/The National Intelligence Model.pdf>

<http://www.gpo.gov/fdsys/pkg/GPO-INTELLIGENCE/pdf/GPO-INTELLIGENCE-22-2.pdf>

<http://ddanchev.blogspot.gr/2006/09/benefits-of-open-source-intelligence.html>

<http://keshavsintresearch.tripod.com/id18.html> OSINT BENEFITS