Nicolae Sfetcu

Epistemology of Intelligence Agencies

ESSAYS Collection

MultiMedia Publishing

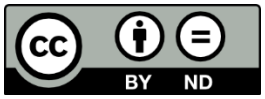
Epistemology of Intelligence Agencies

Nicolae Sfetcu

April 7, 2019

Sfetcu, Nicolae, " Epistemology of Intelligence Agencies ", SetThings (April 7, 2019), MultiMedia Publishing (ed.), DOI: 10.13140/RG.2.2.12971.49445, ISBN: 978-606-033-219-0, URL = https://www.telework.ro/en/e-books/epistemology-of-intelligence-agencies/

Email: nicolae@sfetcu.com



A translation of:
Sfetcu, Nicolae, "Epistemologia serviciilor de informații", SetThings (4 februarie 2019), MultiMedia Publishing (ed.), DOI: 10.13140/RG.2.2.19751.39849, ISBN 978-606-033-160-5, URL = https://www.telework.ro/ro/e-books/epistemologia-serviciilor-de-informatii/

Abstract

In this paper I highlight the analogy between the epistemological and methodological aspects of the activity of intelligence agencies and some scientific disciplines, advocating for a more scientific approach to the process of collecting and analyzing information within the intelligence cycle. I assert that the theoretical, ontological and epistemological aspects of the activity of many intelligence agencies are underestimated, leading to incomplete understanding of current phenomena and confusion in inter-institutional collaboration. After a brief *Introduction*, which includes a history of the evolution of the intelligence concept after World War II, *Intelligence Activity* defines the objectives and organization of intelligence agencies, the core model of these organizations (the intelligence cycle), and the relevant aspects of the intelligence gathering and intelligence analysis. In the *Ontology* section, I highlight the ontological aspects and the entities that threaten and are threatened. The *Epistemology* section includes aspects specific to intelligence activity, with the analysis of the traditional (Singer) model, and a possible epistemological approach through the concept of tacit knowledge developed by scientist Michael Polanyi. In the *Methodology* section there are various methodological theories with an emphasis on structural analytical techniques, and some analogies with science, archeology, business and medicine. In *Conclusions* I argue on the possibility of a more scientific approach to methods of intelligence gathering and analysis of intelligence agencies.

Keywords: intelligence services, secret services, intelligence agencies, intelligence

1 Introduction

Information is power. This perception has intensified during the Second World War, when several intelligence agencies has been formalized and significantly increased. In all countries, new agencies and departments have been set up to deal with threats. Governments are currently spending huge amounts for the intelligence agencies that are considered a major component of national security systems. The intelligence agencies are primarily responsible for identifying and preventing threats to national security, promptly and effectively informing decision-makers about these threats, and accurate and timely assessments and predictions of future conflicts or threats.

Intelligence includes a wide variety of meanings in different contexts, from daily to technical. Stewart believes that the transformation of information into knowledge is a critical one, which is the basis for creating value and competitive advantage for modern activities. (Stewart 2001)

The process of intelligence gathering, processing and analyzing is a major concern for today's society, with the help of areas such as information technology, information systems, and information science. For this purpose, specific processes and techniques are used for gathering or generating intelligence, processing it through analysis and synthesis, generating predictions and strategies, transmitting and presenting it to decision maker, and storing it.

Information science deals with analyzing, collecting, classifying, manipulating, storing, retrieving and disseminating information. (Sfetcu 2016) It is often (mistakenly) considered a branch of computer science. Information science addresses systemic problems from the perspective of the people involved and can be considered as a response to technological determinism. The information philosophy studies the specific conceptual aspects, including the investigation of conceptual nature and the basic principles of information, their dynamics, their use, and the elaboration and application of theoretical information and specific methodologies.

(Floridi 2002) In information science, an ontology formally represents knowledge as a set of concepts, and the relationship between these concepts.

Information extraction is the science of document search, document information, and document metadata, as well as search in relational databases and the Internet. Each type of search has its own features, theories, practices and technologies. Access to information is a field of research aimed at automating the processing of large and cumbersome amounts of information and simplifying users' access to them. The information architecture focuses on the principles of design and architecture in the digital landscape based on a model or concept of information being used in intelligence analysis activities. Information management involves collecting and managing information from one or more sources and distributing this information to one or more segments. Knowledge representation is a field of research that aims to represent knowledge in symbols to facilitate the interference between these elements of knowledge and the creation of new elements of knowledge. Exploring the representation of knowledge implies an analysis of the reasoning. Logic is used to provide formal semantics of how reasoning functions should be applied to symbols in the knowledge representation system, and to define how operators can process and reshape knowledge. (Deshmukh and Ali 2014)

Information systems are organized for collecting, organizing, storing and communicating information. The field of information systems is complementary to that of collecting, filtering, processing, creating and distributing data. (Sfetcu 2016) Any specific information system is intended to support operations, management and decision-making. (Bulgacs 2013) Information systems interrelate with data systems and activity systems on the other, being a communications system in which data is represented and is processed as a form of social memory. An information system can also be considered a semi-formal language that supports decision-making and human

action. Silver et al. have provided two perspectives for SI including software, hardware, data, people, and procedures. (Silver, Markus, and Beath 1995) Zheng offered another approach to the information system, (Zheng 2014) which also adds essential system processes and elements such as environment, limit, purpose, and interactions.

1.1. History

Collecting, analyzing, and using information about opponents have existed since ancient times. Sun Tzu, an ancient Chinese strategist in the Art of War, (Yuen 2014) stressed the need to understand yourself and the enemy through information, identifying different roles: the secret agent, the penetration agent, and the misinformation agent. Sun Tzu highlighted the need for a methodology and noted the role of counterinformation, double agents and psychological warfare. In India, in the 4th century BC, Chanakya (also called Kautilya) wrote *Arthashastra*, a state management and political economy manual, providing a detailed methodology of intelligence gathering, processing, and consumption operations as an indispensable means for maintaining and expanding the security and state power. (Shoham and Liebig 2016) King David IV of Georgia, at the beginning of the twelfth century, used spies to discover feudal conspiracy and infiltration into key locations. (Aladashvili 2017) The Aztecs used traders and diplomats with diplomatic immunity for espionage. (Soustelle 2002)

Francis Walsingham was the first European to use modern espionage methods in Elizabethan England, helping with experts in various fields. (Andrew 2018) In the eighteenth century there was a dramatic expansion of espionage activities. In France under the King Louis XIV (1643-1715) and under the leadership of Cardinal Mazarin (1642-1661), a well-organized information system was set up. To cope with the wars with France, London has also set up a system designed to gather information about France and other powers. During the American Revolution,

1775-1783, US General George Washington successfully developed an espionage system to detect British locations and plans, being the "First Spy of America". (Nagy 2016)

During the American Civil War (1861-1865), Allan Pinkerton first operated a detective agency, then serving as Head of the Union Intelligence Service in the early years. The Austrian Empire founded the Evidenzbureau in 1850 as the first permanent military intelligence service. The topographic and statistical department of T&SD was established at the British War Office as an embryonic military intelligence organization. The French Ministry of War authorized the creation, on June 8, 1871, of the Deuxième Bureau, a service tasked with conducting "research on enemy plans and operations." In Germany, Marshal Helmuth von Moltke set up a military intelligence unit, Abteilung (Section IIIb), of the German General Staff in 1889, which expanded constantly operating in France and Russia. The Ufficio Informazioni del Commando Supremo of Italy was permanently established in 1900. After the defeat of Russia in the Russian-Japanese War of 1904-05, the Russian military service was reorganized under the Seventh Division of the imperial second executive committee.

In the United Kingdom, the Secret Service (OSS), set up in 1909 as the first independent and interdepartmental agency to control all spy government activities, was divided between an external service and counterintelligence in 1910. With the outbreak of the First World War in 1914, all major powers had very sophisticated structures for training and manipulating spies and for processing intelligence obtained through espionage. At that time, modern techniques of espionage were sought and refined to obtain military intelligence, sabotage and propaganda. Two new methods for intelligence gathering were developed during the war - aerial recognition and shooting, and interception and decryption of radio signals. (Wheeler 2012)

During the Second World War, Churchill's order has been devised to train spies and saboteurs under the command of the SOE (Special Operations Executive) and ultimately involve the United States in their training facilities. OSS's research and analysis branch has brought together many academics and experts who have proven to be particularly useful to provide a very detailed overview of the strengths and weaknesses of the German war effort.

MI5 in the UK and the US FBI identified all the German spies and "turned" them into double agents, so their reports to Berlin were rewritten by counterintelligence teams. The FBI played a leading role in American counter-intelligence and gathered together all the German spies in June 1941. (Persico 2002) Counterintelligence included the use of agents to disinform Nazi Germany about the impact points during the blitz and isolation of the Japanese in the US against the Japanese espionage program during the war.

During the Cold War, the Soviet Union was particularly successful in introducing spies into the UK and West Germany but failed in the United States. NATO, on the other hand, also had some important successes.

The focus on the intentions and capabilities of the Soviet Union has dominated thinking in Western intelligence communities. In analyzing information in the 1950s, Walter Laqueur argues that Soviet military capabilities and intentions remain the most important subject for US secret services. (Laqueur 1993)

After the Cold War, governments and intelligence agencies continued to use the conventional model to assess state threats. But security concepts have faded from a highly militarized confrontation between known adversaries and increased concern over non-state threats that were harder to identify. Non-state actors have become strategic threats, the concept of "strategic terrorism" being developed as soon as the September 2001 attacks. Bruce Berkowitz

argues that there have been terrorist actions in the past, but bin Laden was the first to use widespread strategic terrorism against a Super power. (B. Berkowitz 2002) Globalization and people and technology mobility have favored non-state actors. (Waltz 2003) The CIA Director, James Woolsey, told the House of Representatives Committee for National Security in the United States that "we were fighting with a dragon for some 45 years and slew the dragon and then found ourselves in a jungle full of a number of poisonous snakes. And that in many ways, the snakes are a lot harder to keep track of than the dragon ever was." (Woolsey 1998) In 2007, Jonathan Evans, the UK's chief security officer (MI5), described the terrorist threat as "the most immediate and acute threat to peace in the history of my 98-year service." (Evans 2007)

Government publications in developed countries, following the September 11, 2001 attack, reflected a consensus that intelligence services are key to preventing mass attacks.

Currently in the United States there are seventeen (Intelligence.gov 2013) federal agencies forming the United States Intelligence Community. The Central Intelligence Agency uses the National Clandestine Service (NCS) (CIA.gov 2009a) for intelligence gathering and undercover operations. (CIA.gov 2009b) The National Security Agency collects information from the signals. Initially, the CIA led the US-IC. Following the Sept. 11 attacks, the Office of the Director of National Intelligence (ODNI) was created to promote the exchange of intelligence.

2. Intelligence activity

Michael Goodman believes that although intelligence is not a new phenomenon, the academic study of it is an emerging field. (Goodman 2007) The intelligence cycle is generally considered to be composed of five phases: planning and targeting; collect; collection; analyze; and dissemination. (Diane Publishing Company 2000) The most important point in the information

cycle is considered the analysis. Mike McConnell says that intelligence can only help, inform and to make decisions if information is processed through an analyst's mind. (McConnell 2007)

Thus, United States' National Intelligence Strategy supports the need to "“strengthen analytic expertise, methods, and practices; tap expertise wherever it resides; and explore alternative analytic views." (Office of the Director of National Intelligence 2005) Arthur Hulnick writes that "“[t]he intelligence community needs to develop a twenty-first century analytic culture that differs from the conventional intuitive analysis of the past." (Hulnick 2006) To note Rob Johnston's effort to develop a taxonomy of intelligence analysis, arguing that "intelligence needs methodologists to help strengthen the domain of analysis." (Johnston 2003)

David Singer states that the threat is now the main target of intelligence agencies. This idea is also argued by Ken Robertson in his effort to define intelligence:

> "A satisfactory definition of intelligence ought to make reference to the following: threats, states, secrecy, collection, analysis, and purpose. The most important of these is threat, since without threats there would be no need for intelligence services." (K. Robertson 1996)

Carl Von Clausewitz in "*On War*" (1832) defines information activity as "every sort of information about the enemy and his country—the basis, in short, of our own plans and operations." A study of analytical culture has set the following definitions in *consensus*:

- Intelligence is a secret state or group activity to understand or influence foreign or national entities.
- The analysis of information consists in the application of individual and collective cognitive methods to weigh data and test hypotheses in a secret socio-cultural context.
- Informational errors are factual inaccuracies in analysis resulting from insufficient or missing data. Informational failure is a failed prediction resulting from incorrect, missing, rejected, or inappropriate assumptions. (Johnston 2005)

Stephen Marrin considers two reasons for the failure of the development of intelligence theory: (Marrin 2012b) 1) the fact that consensus has not yet been reached on the definitions that are precursors of the formulation of the theory, and 2) intelligence is a applied field, practitioners being basically against theorizations.

Intelligence can be considered as the process through which certain types of information are requested, collected, analyzed and disseminated, and how certain types of secret actions are conceived and carried out. (Shulsky and Schmitt 2002) Berkowitz equates the information community with that of a "Weberian classical" bureaucracy, characterized by centralized planning, routine operations and a hierarchical chain of command, manifested in the traditional informational cycle, like an assembly line. (B. D. Berkowitz and Goodman 2000)

> "Intelligence is more than information. It is knowledge that has been specially prepared for a customer's unique circumstances. The word knowledge highlights the need for human involvement. Intelligence collection systems produce ... data, not intelligence; only the human mind can provide that special touch that makes sense of data for different customers' requirements. The special processing that partially defines intelligence is the continual collection, verification, and analysis of information that allows us to understand the problem or situation in actionable terms and then tailor a product in the context of the customer's circumstances. If any of these essential attributes is missing, then the product remains information rather than intelligence." (Brei 1996)

In intelligence analysis, specialists distinguish three types of information products: (Duvenage 2010)

Operational intelligence, that assists and directs the collection or investigation on a continuous basis, and where the analyst is usually part of the investigation team, finalized by memorandums, operational plans and status reports, and visual analytical support such as diagrams, visual images, etc.

Current intelligence, which contextualizes the "snapshots" of an event or problem for the client in the form of text.

Strategic intelligence, that provides the client with estimates and/or warnings by presenting medium and long-term analysis of the nature, dynamics and impact of an event or problem.

2.1. Organizations

Intelligence services are government agencies that deal with the collection and analysis of sensitive information in order to ensure national security and defense. The methods of intelligence gathering can include spying, interception of communications, cryptanalysis, cooperation with other institutions, and assessment of public sources. (Sfetcu 2016)

Intelligence services are currently focusing on the fight against terrorism, leaving relatively little resources to monitor other security threats. For this reason, they often ignore external information activities that do not pose immediate threats to their government's interests. (Ehrman 2011)

Extremely few external services - CIA, SVR and, to a lesser extent, SIS, French DGSE and Mossad - operate globally. Almost all other services focus on immediate neighbors or regions. These services usually depend on relationships with these global services for information on areas beyond their immediate neighborhoods, and often sell their regional expertise for what they need globally.

Intelligence services are prisoners of government bureaucracy, subject to the same political forces and tendencies as any other. The political situations of intelligence services in authoritarian, totalitarian or corrupt states are more difficult to determine. The absence of effective legal frameworks and the importance of personal networks towards institutional relations for decision make it difficult to study. Examples in the history of communist block service suggests, however, that in these countries their intelligence services positions may be paradoxical. The dependence of these regimes on their repressive services, the integration of services into the governing apparatus,

and the absence of any external control, offer to services immunity from external investigations and the pressure of reforms. (Ehrman 2011)

Even when acting legally, intelligence services protect and promote their interests. The result is that services are almost always engaged in complex political struggles on several fronts. The most important of these is the constant effort to raise as many resources as possible - people, funds and influence on decision-making - from their political superiors, and to oppose external changes.

Intelligence services are not robotic institutions, but rather hundreds or thousands of people who make and execute decisions. There are few sociological or comparative open-source studies of intelligence officers. Foreign service officers tend to be of higher socio-economic classes. The nature of their work - living and operating in other countries, presenting themselves as diplomats or businessmen and interacting with political leaders in the country and abroad - requires university education, knowledge of languages and culture, and trust in interaction with diplomatic officials and politicians. People with these characteristics usually come from the upper middle class or above. Internal service officers tend to be from working classes and from lower middle classes. Their work is similar to police work, and as they perform their tasks on their home ground, the pulse of the street is more important than sophisticated elegance. (Richelson 1988, 72) (Shelley 1990, 479–520)

A feature of both internal and external services is that they behave like a caste. Except for the director, no outsiders hold a position of authority; In the world of intelligence, ambitious politicians, advocates, think tank analysts, and academics, who usually run in government positions, do not get in.

John Ehrman says that intelligence service management tends to be mediocre. (Ehrman 2011) In general, high-performance case officers assume leadership positions. Usually, they do not have any management training before taking up these positions, and then receive little systematic training. As a result, mid-level and top-level managers often have little interest in overseeing critical administrative and planning details or taking initiatives to change or upgrade services before a failure or crisis forces them to do so.

The main objective of intelligence organizations is to ensure security, a concept that assesses the degree of resistance or protection to what is bad. Certain concepts are common to several security domains:

- Warranty - the level of guarantee that a security system will behave as it has been evaluated
- Countermeasure - the way to stop a threat from triggering a risk event
- Defense in depth - never rely on just one measure
- Risk - a possible event that could cause a loss
- Threat - a way to trigger a dangerous event
- Vulnerability - a weakness of a target that can be exploited by a security threat
- Exploitation - a vulnerability triggered by a threat.

Robert M. Clark believes that an organization is a system that "can be viewed and analyzed from three perspectives: structure, function, and process." (Clark 2003, 277) The structure describes the parts of the organization, with an emphasis on individuals and the relationships between them. The function describes the organization's product with a focus on decision-making. And the process describes the activities and knowledge that form the final product.

2.2. Intelligence cycle

The intelligence cycle is a set of processes used to provide useful information for decision-making. The cycle consists of several processes. The related counter-intelligence area is tasked with preventing information efforts from others.

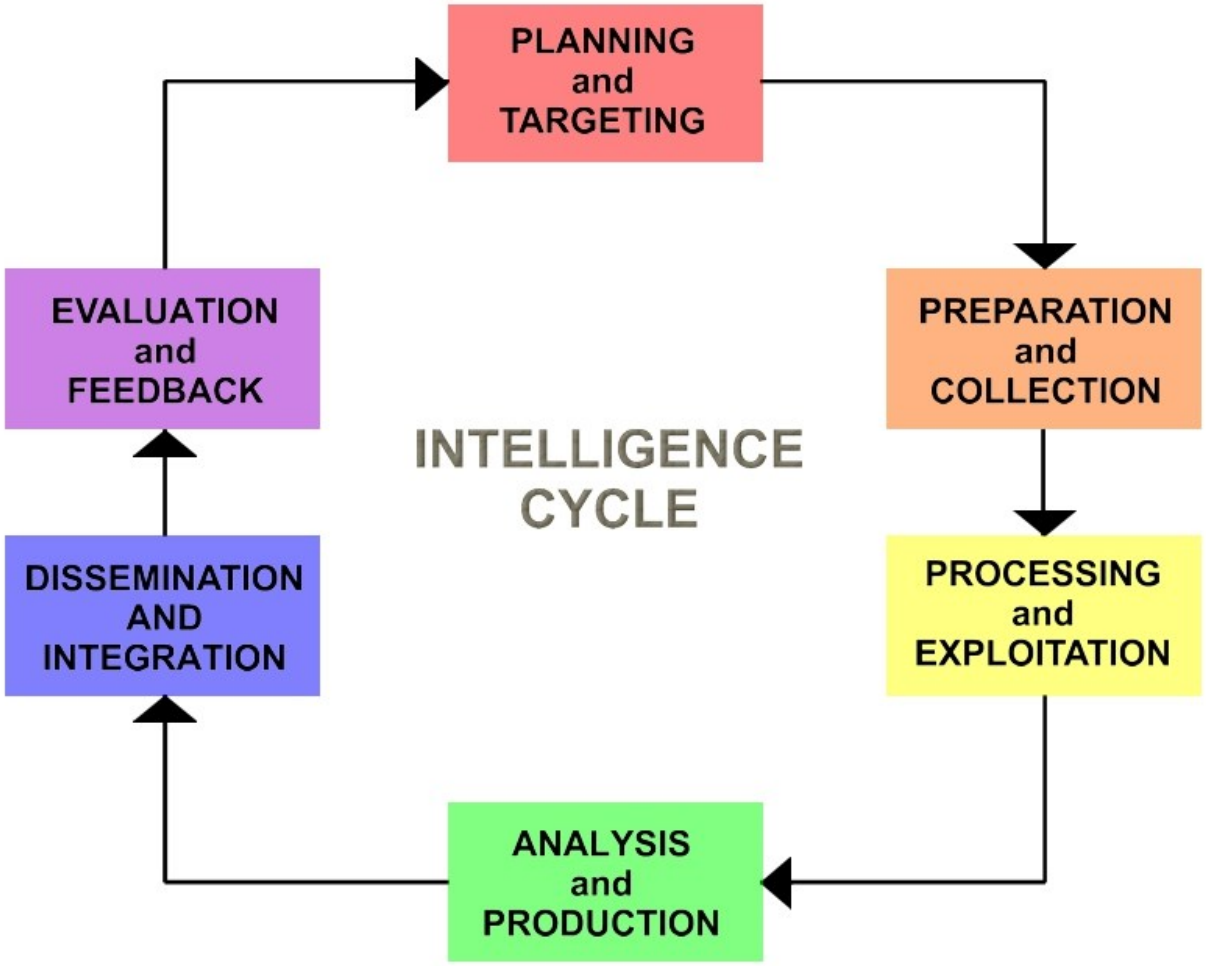


Figure 1 Intelligence cycle or process

A basic model of the process of collecting and analyzing information is called the "intelligence cycle". This model can be applied, and, like all the basic models, it does not reflect the fullness of real-world operations. Through intelligence cycle activities, information is collected and assembled, raw information is transformed into processed information, analyzed and made available to users. The intelligence cycle consists of five phases:

1. *Planning and Targeting*: Decide what needs to be monitored and analyzed. This involves determining information requirements, developing an adequate intelligence architecture, preparing a collection plan, issuing orders and requests to intelligence agencies.
2. *Preparation and Collecting*: Establishing an intelligence officers' own strategy, gathering raw information using a variety of collection types, such as human sources (HUMINT), geo-spatial sources (GEOINT), etc.
3. *Processing and Exploitation*: Refining and primary use of information in primary decisions.
4. *Analysis and Production*: The processed information is translated into a finalized intelligence product, which may include the resulting syntheses, predictions and intelligence measures.
5. *Dissemination*: Providing intelligence products to consumers (including those in the intelligence community)

In addition to these phases, a sixth step, not only in the intelligence activity, but in cooperation with customers and observing the operational environment for the effectiveness of the information provided, is very important:

6. *Evaluation and feedback*

These steps are generally divided within an intelligence organization. The number of steps varies according to the strategy of each intelligence organization, some organizations compressing some of these steps (eg, analysis and production is included in the processing and exploitation phase), or by adding other steps according to the specific requirements.

The initial phase of planning and targeting of the intelligence cycle includes four major stages:

1. Identification and prioritization of information requirements;
2. Development of an adequate intelligence architecture;
3. Preparing a gathering plan; and
4. Issuing order and requests to the intelligence organizations.

The collection coordination intelligence requirements management (CCIRM) is the NATO doctrine of intelligence gathering management, although it differs from the US doctrine.

In the "analysis and production phase", the information is processed only after it has been verified by all available sources, their veracity increasing according to the number and quality of the additional checks.

Intelligence activity is an iterative process in interaction with many actors, so the process of intelligence activity can be characterized as dialectical in that a given hypothesis can be confirmed, revised or rejected based on additional information from other disciplines.

An important condition for the efficiency of intelligence as a finished product is the speed and accuracy of communications between the involved actors.

From an epistemological point of view, it is still unclear when the intelligence becomes knowledge: during the collection, after the analysts have been further verified, after their approval at the organization level, or when an independent body confirms the analysis?

Another aspect to be considered in the intelligence cycle is the relationship with the legal system, as the role of the various actors in the intelligence process is less clear than those involved in the legal act. Human sources can be motivated by numerous personal biases. For example, an analyst may benefit from subtle incentives to reach a conclusion, or information collectors may be forced to collect only certain information. (Morgan 2012) That is why there must be an institutional mechanism that can challenge the assumptions and conclusions made during the intelligence

analysis. In this sense, some intelligence organizations use a so-called "red team analysis", an alternative analysis of information and conclusions in intelligence products. (US Department of the Army 1995) According to the former CIA officer Richard Heuer, such an alternative analysis has the potential to use specific techniques to determine where "analyzes" were "wrong". (Heuer 1999)

Military strategist John Boyd created a different decision and action model (OODA), (Boyd 1976) useful in many areas of conflict. Its model has four phases: 1) ***O****bserving* a threat or opportunity; 2) ***O****rientation* in the context of other information; 3) ***D****ecision* based on the best action plan; 4) ***A****ction* to carry out the plan. Each new iteration of the cycle is faster than the previous one, due to the accumulated experience. By comparing it with the traditional intelligence cycle, observation could be an output of the collection phase, while orientation is an output of analysis.

2.3 Intelligence gathering

A process of intelligence gathering begins when a user enters a query into the system. Several objects can match the result of a query with different degrees of relevance. Most systems estimate a numeric value about how well each object matches the query and classifies objects according to this value. Many researches have focused on practices of intelligence gathering. Much of this research was based on the work of Leckie, Pettigrew and Sylvain, who in 1996 carried out an extensive review of the information science literature on the search for information by professionals. The authors have proposed an analytical model of the behavior of search professionals seeking to be generalizable across the profession, thus providing a future research platform in the field. The model was designed to "prompt new insights... and give rise to more refined and applicable theories of information seeking." (Leckie, Pettigrew, and Sylvain 1996,

188) The distinctive sign of the intelligence activity is to find the type of information others want to conceal.

Knowledge engineering was defined by Edward Feigenbaum, and Pamela McCorduck as follows: (Feigenbaum and McCorduck 1984)

"Knowledge engineering is an engineering discipline that involves integrating knowledge into computer systems in order to solve complex problems normally requiring a high level of human expertise."

Currently, knowledge engineering refers to building, maintaining and developing knowledge-based systems. Knowledge engineering is related to mathematical logic, and heavily involved in cognitive sciences and socio-cognitive engineering where knowledge is produced by socio-cognitive aggregates (especially human) and is structured according to our understanding of how human rationality and logic work.

In knowledge engineering, knowledge gathering consists in establishing knowledge from structured and unstructured sources in a way that must represent knowledge in a way that facilitates inference. The result of the extraction goes beyond establishing structured information or transforming it into a relational scheme, requiring either reuse of existing formal knowledge (identifiers or ontologies) or generating a system based on source data. (Sfetcu 2016)

Traditional information extraction is a natural language processing technology that extracts information from language texts and their typically natural structures in an appropriate way. The types of information to be identified must be specified in a model before the process starts, so the entire process of extracting traditional information is domain dependent. The extraction of information is divided into the following five secondary tasks: (Cunningham 2006)

- Named Entity Recognizing (REN) - Recognizing and classifying all named entities contained in a text, using grammar-based methods or statistical models.

- Coreference resolution (CO) - identifies equivalent entities that have been recognized by REN in a text.
- Construction of the template element (TE) - identifies the descriptive properties of the entities, recognized by REN and CO.
- Construction of the template relationship (TR) - identifies the relationships that exist between the template elements.
- Production of the script template (ST) - will be identified and structured according to entities recognized by REN and CO and relationships identified by TR.

In ontology-based information mining, at least one ontology is used to guide the process of extracting information from the text in natural language. The OBIE system uses traditional information extraction methods to identify concepts, cases and relationships of ontologies used in the text, which will be structured in an ontology after the process. Thus, entering ontologies is the model of information to be extracted. (Wimalasuriya and Dejing Dou 2010, 306–23) Ontology learning automates the process of constructing ontologies in natural language.

Information published in media around the world can be classified and treated as secret when it becomes an intelligence product. All sources are secret, and intelligence is defined to exclude open sources. (K. G. Robertson 1987)

Closed or secret sources involve "special means" to reach information, and the technique may include manipulation, interrogation, the use of technical devices, and extensive use of criminal methods. These techniques are costly, time consuming and labor intensive compared to open source methods. In some cases, hidden collection methods have a strong association with the criminal world. Noam Chomsky noted that there are good reasons why intelligence services are so closely linked to criminal activities.

> "Clandestine terror," he argued, "requires hidden funds, and the criminal elements to whom the intelligence agencies naturally turn expect a quid pro quo." (Chomsky 1992)

The discovery of knowledge involves an automatic process of searching for large volume data, using data mining, and based on similar methodologies and terminologies. (Wimalasuriya and Dejing Dou 2010, 306–23) Data mining creates abstractions of input data, and the knowledge gained through the process can become additional data that can be used later. (Cao 2010)

Investigations in the data collection process are aimed at enriching information, eliminating some doubts, or solving problems.

The process of intelligence gathering from people (abbreviated HUMINT) is achieved through interpersonal contacts. NATO defines HUMINT as "a category of intelligence derived from information collected and provided by human sources." (NATO 2018) Typical HUMINT activities consist of queries and conversations with people who have access to information. The way HUMINT operations are conducted is dictated by both the official protocol and the nature of the information source.

Sources may be neutral, friendly or hostile and may or may not be aware of their involvement in intelligence gathering.

The HUMINT gathering process involves selecting source people, identifying them and conducting interviews. The analysis of information can help with biographical and cultural information. Lloyd F. Jordan recognizes two forms of culture study, both of which are relevant to HUMINT. (Jordan 2008)

Coverage methods are complicated and dangerous but raise ethical and moral questions as well. A well-known technique, for example, is the manipulation of human agents to obtain the information. The process, known as "the development of controlled sources," may involve extensive use of psychological manipulation, blackmail, and financial rewards. (Godfrey 1978)

Intelligence gathering applying these techniques work in hostile environments. But intelligence, Sherman Kent argued, could be likened to familiar means of seeking the truth. (Kent 1966) Intelligence, unlike any other profession, does not work according to known moral or ethical standards. Some of these standards tend to be, at best, cosmetic. The argument is that anything vital to national survival is acceptable in any situation, even when the method provokes everything that is democratic. Clandestine operations remain unclear in international law and there is very little scientific research to cover the subject.

2.4. Intelligence analysis

The analysts are in the field of "knowledge". Intelligence refers to knowledge and the types of problems addressed are knowledge problems. So, we need a concept of work based on knowledge. We need a basic understanding of what we know and how we know, what we do not know, and even what can be known and what is not known. (Vandepeer 2014) Matthew Herbert offers a useful set of principles in discussing the guidance reported by Colin Powell to US intelligence director Mike McConnell. It is said that Powell advised McConnell as follows:

> "As an intelligence officer, your responsibility is to tell me what you know. Tell me what you don't know. Then you're allowed to tell me what you think. But you always keep those three separated." (Weiner 2007)

The analysis of information involves "turning disparate facts into focused conclusion." (Codevilla 1992)

No definition is conclusive in clarifying the meaning of the analysis. Likewise, the same person or group of people can achieve a multitude of roles in the process cycle, sometimes demanded by analysis.

The analysis should provide a useful basis for conceptualizing intelligence functions, of which the most important are "estimation" and "prediction". The intelligence itself, in its basic

form, has a decision-making function. A decision is characterized by two main functions: (1) choices or judgments between competing alternatives, and (2) uncertainty of choices and judgments.

John Maynard Keynes states that, under uncertainty, "there is no scientific basis on which to form any calculable probability whatever. We simply do not know." (Keynes 1937) It follows that, in the absence of certainty, the decision-maker may be obliged to take measures with uncertain consequences, or to base his election on the predictions of the future, an exercise of subjective reasoning.

Radner described a characteristic optimal decision as follows: "For each signal, an optimal decision maximizes the conditional expected utility of the consequence, given the signal," as principle described as "maximizing conditional expected utility". (Radner 1972)

Researchers used concepts such as "incomplete information" and "uncertainty decisions" to study group interactions based on the (subjective) nature of the information that actors possess. (Ekpe 2005) For example, Andrew Kydd used the incomplete information model to explain Jervis's "spiral model of escalation in arms races". (Kydd 1997) The theory of uncertainty decisions also belongs to this family of incomplete knowledge behavior or actions conditioned by subjective feelings. As Arrow Kenneth observes, "uncertainty" means that the agent does not know the state of the world. (Arrow 1966)

Intelligence analysis applies individual and collective cognitive methods to assess data and test assumptions in a secret socio-cultural context. (Hayes 2007) The analyst must detect deceptions and extract the truth. The purpose of intelligence analysis is to reduce ambiguity. Assuming that enemies try to create confusion is not paranoid in the case of analysts, but realistic.

According to Dick Heuer, in an experiment in which the analyst's behavior was studied, the process is incremental refining.

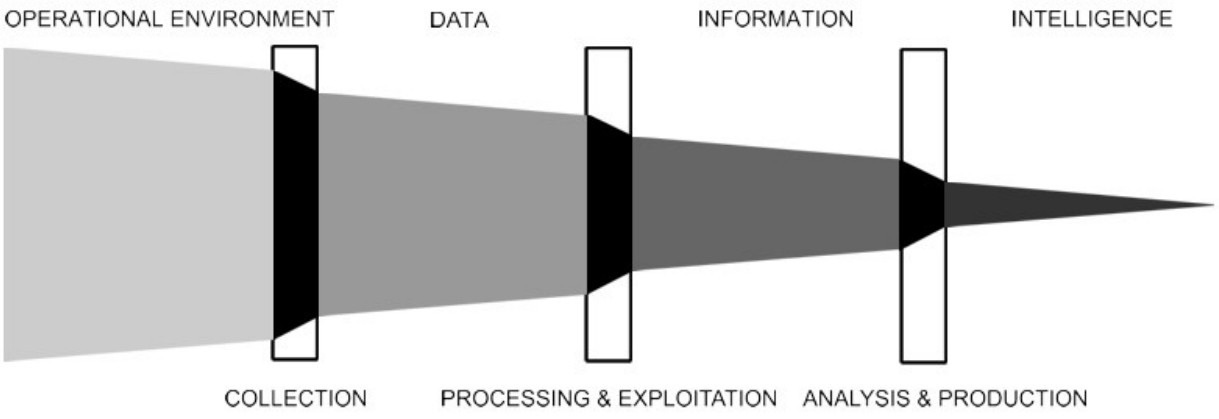


Figure 2 The intelligence activity reflects a progressive refinement of data and information

Academic disciplines examining the art and science of intelligence analysis are most commonly called "intelligence studies" and taught in specific institutions.

The analyst must constantly ask what want/must clients to know, how does they prefer the presentation to be? Are they trying to choose the best way of action or they have already chosen it and now they must know the obstacles and vulnerabilities on the chosen path?

Sometimes, when the producer strives to meet the needs of both internal and external customers, the solution is to create two different types of products, one for each type of customer. An internal product may contain details about sources, collection methods and analytical techniques, while an external product is more journalistic: Which? What? When? Where? Why? "How" is often relevant to journalists, but not recommended in the intelligence activity. Actions are grouped in three stages:

1. The decision to act
2. Action
3. Disengagement from action (Ikle 2005)

Heuristic or semantic maps can help structure information, just like file folders and indexing cards. Also, databases with statistical techniques such as correlation, factor analysis, and time series analysis can provide insight.

The purpose of the information analysis is to reveal to a certain decision maker the underlying significance of the selected information. Analysts should start with confirmed facts, apply specialist knowledge to produce plausible findings but less secure conclusions, and even predict when the forecast is properly qualified. Analysts should not, however, engage in guesses that have no basis in facts.

Intelligence analysis involves the development of recommended predictions of action, based on a wide range of available sources of information, both open and undercover. The analysis is developed in response to the requirements of the organization's or client's management to help make decisions. (Sfetcu 2016)

One of the techniques used in intelligence analysis is the analysis of indicators, which uses historical data to expose trends and identify future major changes in an area of interest, helping to develop evidence-based prognoses with low cognitive bias. (Heuer and Pherson 2010)

Structured analytical techniques (SAT) have come to be used more since the World Trade Tower attacks of September 11, 2001, when the United States National Commission for Terrorist Action, or the 9/11 Commission, found that the intelligence community suffered "a failure to challenge analytic mindsets, examine key assumptions, consider alternative hypotheses, and detect deceptive reporting." (Pherson 2013) These analytical tools, designed to better manage and standardize the performance of the analysis, are an attempt to align the profession to scientific principles. From an epistemological point of view, it can be argued that SATs generate

propositional knowledge and inadequately acknowledge the value of "tacit knowledge" or unprotected knowledge in the problem-solving process in intelligence analysis. (Gentry 2015)

Indicators may be unique events or actions from a factor that signifies a major change, affecting conditions in the rest of the categories or other categories, or a combination of events that serve a similar function. The process is as follows:

1. Identify a set of categories relevant to the requirement
2. Identify a set of relevant factors for each category in the context of the global requirement
3. Identify short-term scenarios that may result from the immediate transfer or improvement of each factor
4. Identify a series of events or indicators that could mean improvement or deterioration within each factor
5. Review historical and ongoing events for indicators within each factor
6. Identify unique indicators and indicator trends to predict which short-term scenario is most likely to occur. (US Government 2009)

U.S. Intelligence Community standardizes its lists of indicators within an agency or across the community. (Artner, Girven, and Bruce 2016)

A common form of intelligence analysis is the use of social networking data, both on the Internet and on the mobile. Many government agencies are investing heavily in research involving social networking. Intelligence communities believe that the biggest threat comes from de-centralizing, without leaders, the geographical dispersal of terrorists, extremists, and other subversive and dissident people. These types of threats are the easiest to counteract by discovering important nodes in the network and eliminating them. For this, a detailed network map is required. (Hogan, Carrasco, and Wellman 2007) It is considered that the use of social networking sites is a

form of "participatory surveillance", where users of these sites are practically supervising themselves, displaying detailed personal information on public sites where can be seen by corporations and governments.

2.5. Counterintelligence

According to William Johnson's definition counterintelligence (CI) is an *activity designed to protect an intelligence organization against state or non-state agents*. (Johnson and Hood 2009) It includes the collection and analysis of specific information, and preventive and counter-offensive activities against intentions and actions directed against national security, including terrorism. (Conrad 1985)

In US doctrine, CI is now seen primarily as a counterbalance to the actions of foreign intelligence services (FIS HUMINT). In the US Army's counterintelligence manual of 1995, CI had a broader scope. More recently, the American Doctrine of the Information Community (Matschulat 2007) limits the main purpose to activities that usually include counter-terrorism. The scope of the doctrine of US military counterintelligence has been shifted to a classified publication, Joint Publication (JP) 2-01.2, *Counterintelligence and Human Intelligence Support to Joint Operations*. For each type of specific foreign action, countermeasures are provided both with defensive and offensive role.

Counter-HUMINT deals with the detection of hostile or potentially hostile HUMINT sources, responsible for monitoring reliable staff to prevent and neutralize risks. (US Department of the Army 1981)

Offensive techniques in today's counterintelligence doctrine are directed mainly against human sources, so counterintelligence can be considered synonymous with offensive

counterintelligence. Offensive counter-attack (and counter-terrorism) acts either by manipulating an opponent (FIS or terrorist) or by interrupting the opponent's operations.

Counterintelligence is primarily considered an analytical discipline, focusing on the study of intelligence services. Taking this into consideration, John Ehrman (Ehrman 2009) proposes an appropriate definition of CI:

> "Counterintelligence is the study of the organization and behavior of the intelligence services of foreign states and entities, and the application of the resulting knowledge." (Samuelson and Nordhaus 1992, 53)

The basis of all counterintelligence activities is the study of individual intelligence services, an analytical process to understand the behavior of foreign entities (formal mission, internal and external policy, history and myths within the entity, the people who compose it).

CI operations are a specialized subassembly of intelligence operations in general, usually trying to create endless feedback loops. In general, there are three types of counterintelligence operations: classic penetration, double agents, and identification and monitoring of the agents of the concerned service.

Counterintelligence is an under-theoreticized field without a clearly defined methodology. John Ehrman identifies several future research directions, such as service policy, service sociology, and counterintelligence economy. Also, future counterintelligence studies in the construction of theory should include comparative and literary studies. A robust counterintelligence theory will have to put the analysis at the center of counterintelligence activity and allow for a multidisciplinary and integrated approach to analytical and operational activities.

2.6. Epistemic communities

Epistemic communities are informal networks of knowledge-based experts who influence decision-makers in defining issues they face, identifying different solutions, and evaluating results.

(Hsu and Hasmath 2017) Peter M. Haas defined the conceptual framework of an epistemic community as

> "... a network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy relevant knowledge within that domain or issue-area." (Haas 1992, 3)

Members of an epistemic community come from academic or professional backgrounds and are characterized by a set of unifying features. (Sebenius 1992)

Epistemic communities are socio-psychological entities that create and justify knowledge. Michel Foucault referred to the *mathesis* as a rigorous episteme appropriate to allow the cohesion of a discourse and thus the unification of a community. In the philosophy of science and system science, the process of forming a self-sustaining epistemic community is sometimes called a mentality, similar to a trend or a faction in politics.

A counterpart of what is NOT an epistemic community is provided by Mai'a K. Davis Cross, considering the European Defence Agency (EDA) and the EU Intelligence Analysis Center (IntCen). (Cross 2015) Cross claims that although they are composed of high-level security experts, these two organizations are not epistemic communities. Real epistemic communities, diplomats, military experts, security researchers and civilian crisis management experts have significantly influenced EU security policy.

Expert groups that are not epistemic communities are not poor or becoming cases. They can fundamentally be different types of actors with divergent features.

An epistemic community rarely includes all members of a formal organization. A strong epistemic community is trying to overcome its professional role as a group and is often able to persuade decision makers to fundamentally change the nature of their political goals.

An epistemic community is a group of people who do not have a specific history together but seek a common idea of origin as if they were an intentional community. For example, an

epistemic community can be found in a network of professionals from a wide variety of disciplines and backgrounds, (Keman 1998) including intelligence services.

According to Haas, the epistemic communities: (1) share the professional opinion on a policy issue, (2) weigh the validity of their political objectives in their field of expertise, (3) engage in a common set of practices on the problematic area with the goal of improving human well-being, and (4) sharing beliefs in principle. (Haas 2001, 11578–79)

Epistemic communities also have a "normative component," meaning that the ultimate goal is always an improvement in society, rather than the own gain of the community itself. (Haas 1992)

In international relations and political science, an epistemic community can also be referred to as a global network of knowledge-based professionals in science and technology that often affects political decisions. (Morin and Louafi 2017)

Epistemic communities have the greatest influence in "conditions of political uncertainty and visibility," (Radaelli 1999, 763) usually following a crisis or triggering event.

The European Union, with its ongoing processes of integration, shared democratic values, supranational institutions and transnational interactions, is very favorable to the formation of epistemic communities. (Loik 2013) The EU's security policy is an area where there are more epistemic communities based on Brussels.

3. Ontology

In intelligence, the ontological problem is related to the nature and characteristics of entities that threaten and are threatened. According to Eric Little and Galina Rogova, "[t]hreat is a very complex ontological item and, therefore, a proper threat ontology must be constructed in accordance with formal metaphysical principles that can speak to the complexities of the objects,

object attributes, processes, events and relations that make up these states of affairs." (Eric G. Little and Rogova 2006)

Björn Müller-Wille's argument on security and threats helps to highlight the interdependence between threatening and threatened entities. In this sense, intelligence analysts must define both what constitutes a threat and what is threatened. Thus, a significant threat ontology must include both threats and threatened entities. (Vandepeer 2011)

Developing a threat ontology requires a taxonomy. A potentially useful taxonomy used in describing the security analysis is provided by Buzan, Waever and Wilde. (Buzan et al. 1998) They argue that the security analysis involves three distinctive actors. From this taxonomy, adapted for the intelligence analysis, the following entities emerge:

- a *referent* is what or who is threatened;
- an *analyst* acts as a "threat determinant"; and
- a *threat actor* who is evaluated by the analyst as threatening the referent.

The threat referent is usually the state, namely the survival of the state and its population. (Singer 1958) *Quadrennial Homeland Security Review* describes security as the requirement to "“[p]rotect the United States and its people, vital interests, and way of life." (Department of Homeland Security 2010, ix) Globalization makes it increasingly difficult to identify the interests of the state, even of the population. Under the Montevideo Convention, the four generally accepted requirements for statehood are: a permanent population; defined territory; a government; and the ability to enter into relations with other states. (Australia Department of Defence 2009) These requirements generally refer to four aspects of a threatened state, namely: population, territory, government, and interests. The nature and characteristics of state and non-state threats consider how these entities can threaten these four factors.

State interests include threatening the political influence of the state, limiting the state's ability to develop favorable or strong relations with other states, regional stability, economic stability, development and financial infrastructure of the state, (Australia Department of Defence 2009) energy resources, communication lines and citizens' ability to travel.

Non-state actors (especially those who threaten) are often undefined. A useful definition for capturing them is "“...any person or group of people who act independently of formal governments." (Australia Department of Defence 2002)

Threat evaluation is defined by Steinberg et al (Omand 2009) as "the process of estimating and anticipating the effects on the situations of planned or expected/anticipated actions by participants, including interactions between the action plans of several actors (e.g., assessing susceptibilities and vulnerabilities to estimated/projected threatened actions, considering their planned actions). " It follows that different functions and elements of threat assessment have to be considered. (Rudd 2008) The ontological complexity of threat elements requires ontological analysis based on metaphysics that can effectively classify different types of complex objects, properties and attributes, events, processes and relationships that are of interest to various decision makers.

Situation and Threat Assessment (STA) processing refers to context-dependent information about the dynamic facets of reality (Eric G. Little and Rogova 2006) so that STA ontologies must be able to capture the reality structure by providing capabilities to describe the multitude of types of relationships (e.g., space-time, intentional, and dependency relationships) that exist between different situational entities (and their aggregations) at different levels of granularity. (Bittner and Smith 2003) For this reason, the ontologies to be used to assess the situation and threats require a wider understanding of the types of relations and relational entities

found initially in Aristotle's writings (Aristotle 1991) and later formalized by Edmund Husserl. (Husserl 1900) It is important for STA ontologies to be structured in a superior general metaphysical framework in order to break down the most abstract elements of the field of interest and the relationships between them.

In *An Ontological Analysis of Threat and Vulnerability*, Eric G. Little and Galina L. Rogova developed a "threat ontology" (ThrO), (Eric G. Little and Rogova 2006) a modified version of the basic formal ontology (Grenon and Smith 2004) composed of two orthogonal sub-levels, SNAP and SPAN, which are designed to capture the spatial and temporal features of ontology. Based on the distinction between the *continuants* and the *occurents*, they have ontologically modeled complex spatio-temporal objects with a formal bifurcation between objects as elements that can exist entirely at some point in space and time versus processual events whose parts and partial relationships are constantly evolving over time, and therefore there are never entirely in a certain place or time. The distinction helped to avoid certain traditional philosophical problems of identity. The basic formal ontology is designed in accordance with the theory of mereotopology, (B. Smith 1996) a theory that combines a logic of parts and partial relationships (e.g., mereology) with a logic of spatial expansion and connection (i.e., topology) language capable of treating the multitude of ontological objects required for higher-level fusion processing, e.g. objects, properties/attributes, spaces, times, and the many simple and complex relationships between them. The information used to assess the threats is extremely uncertain, contradictory, redundant, of varying importance and low fidelity. This makes it necessary to ”incorporate uncertainty, reliability, and imprecision into the characterization of qualitative mereotopological relations.” (Eric G. Little and Rogova 2006)

At a higher level, as a whole, people exist as relational entities, not just as collections of independent elements. The problem here is of ontological significance, where the modeling of the element collections is not the same as the modeling of the whole, because the same complex element can be understood differently depending on whether it is understood as a collection or as a whole. (B. Smith 1996) The theory of mereotopology provides a way to describe formally the types of complex partial relations between them that contain elements such as threats, in which the three elements of intent, capacity and opportunity are in a formal relationship fundamental dependence. The capture of metaphysical relationships, such as fundamental dependence, is necessary for the design of threats ontologies. Given the complexity of the threats, it is essential to design an ontological framework that can include many types of relationships necessary for the correct breakdown of complex elements. (Eric G. Little and Rogova 2006)

The ontological definition of certain essential features of the parts and their relationships, together with proximity and constraint metrics, will then allow better definition and identification of dispersed groups. (E. G. Little and Rogova 2005)

An ontology for threat analysis and action must be able to shape ontological distinctions between potential and viable threats. This provides a better understanding of how threats (ie intentions, capabilities, and opportunities) can exist and can be changed over time. Escalating threats from a state of potency to a state of viability could be avoided by using appropriate threat mitigation techniques. (E. G. Little and Rogova 2005)

On the other hand, for Barry Smith in *Ontology for the intelligence analyst*, (B. Smith 2012) the Strategy of Semantic Enhancement (SE) (Salmen et al. 2011) is based on the use of simple ontologies whose terms are used to mark (or annotate) source data artifacts in a coherent way. Terms in a SE ontology are linked together in a simple hierarchy through the relationship

"is_a" (or subtype). Each term appears once in this hierarchy and is paired in a stable way with parent and child hierarchy terms, even if new terms are added to ontology over time. This stability is important because the success of the strategy requires ontologies that can be repeatedly reused to annotate many different types of data in ways that serve multiple different community of analysts, thus contributing to creating an increasingly common operational picture. SE is designed to be at the same time more stable and more flexible than traditional approaches to harmonization and integration, which are usually based on ad hoc mapping between data models, their effectiveness over time often degrades. (B. Smith 2012)

SE ontologies are organized on three levels with successive degrees of flexibility: 1) a unique, small, domain-neutral Upper-level Ontology (ULO), for which our selected candidate is the official ontology; (Volkswagen Foundation 2002) 2) Mid-level ontologies (MLO), formed by grouping terms that refer to specific areas of action or specific tasks such as inter-agency information exchange; (B. Smith, Vizenor, and Schoening 2009) 3) low-level ontologies (LLO) that focuses on specific areas. The SE approach is designed to be of maximum use to intelligence analyst users. Ontological content is created only as a response to analysts' situational needs, and architectural requirements are designed to ensure a consistent evolution of SE resources without sacrificing the flexibility and expressivity required in real-world deployment. (B. Smith 2012) The SE Strategy can determine collaborative ontological development and re-use for multiple internal and external data collection purposes.

4. Epistemology

In intelligence, epistemology is the study of the threat awareness and the way the threat is understood in the field of intelligence analysis.

Most definitions of intelligence do not consider the fact that the epistemic normative status of the intelligence analysis is knowledge rather than a lower alternative. Counter-arguments to the epistemological status of intelligence are their purpose-oriented action, and their future-oriented content. (Rønn and Høffding 2013)

Following the attacks of September 11, a terrorism commission was set up to identify the failures and weaknesses of US intelligence agencies, to learn from security vulnerabilities and to avoid future attacks on national safety and security. The conclusion was that the US intelligence institutions lacked the imagination and ability to make relevant predictions - that is to connect the relevant "points" and reach relevant conclusions. (Anderson, Schum, and Twining 2009)

Sherman Kent, in *Strategic Intelligence* (1949), divides the field into three components: (Kent 1966) knowledge, organization, and activity. In the opinion of Michael Herman in *Intelligence Services in the Information Age* (2001), the field of intelligence can be divided into: activity, subjects, product, and function. (Herman 2001) Scott and Jackson in *The Study of Intelligence in Theory and Practice*, introductory article in *Intelligence and National Security Journal* no. 19 of 2010, (Scott and Jackson 2004) complements Kent and Herman's divisions by providing an analysis of how to make significant distinctions in the field of intelligence.

The intelligence contrasts with information and knowledge and can be placed in a pyramidal continuum of data, information and knowledge. (Dean and Gottschalk 2007) Intelligence can be inserted into two different positions: either between information and knowledge, or at the top of the knowledge hierarchy. (Rønn and Høffding 2013)

In the first case, the intelligence is an epistemic step above the information: Geoff Dean and Petter Gottschalk consider that "intelligence is placed between information and knowledge on the continuum as ideally intelligence represents (...) a form of validated information." (Dean and

Gottschalk 2007) Normative understanding of intelligence can be seen as the most "plausible information." Intelligence is often referred to as "prior knowledge" understood as information and evaluation of future activities. (Wheaton and Beerbower 2006) Specifically, the pre-scientific attribute of the intelligence is characterized as a warning about events and potentially harmful actions. The question then is whether it disqualifies intelligence as knowledge. (Rønn and Høffding 2013)

If the intelligence is placed above knowledge, it is more than mere knowledge. Jerry Ratcliffe justifies this ranking as follows:

> "So why the extra step of adding intelligence to the continuum? It is due to the fact that intelligence products are inherently action products. In other words, knowledge products can generate understanding, but intelligence products are supposed to generate action." (Ratcliffe 2008)

This means that intelligence generates "actionable knowledge". But this interpretation, though claiming that intelligence is a type of knowledge, seems to confuse its epistemic status with its normative function, that of actions and decisions of orientation.

According to Simon Høffding, when we compare the epistemic status of intelligence according to the above positions, the relationship between information and knowledge in continuum is asymmetric due to the different level of plausibility and relevance. (Rønn and Høffding 2013) However, what matters is the agent's propositional attitude towards the content of an information. In this sense, information and knowledge are interdependent, and both can thus be intelligence.

The main concept of intelligence is the threat. This is reflected in the seminar work of J. David Singer in 1958, *Threat Perception and the Armament-Tension Dilemma*, (Singer 1958) through a quasi-mathematical model:

Threat-Perception = Estimated Capability x Estimated Intent

Intent and *capability* parameters can be described as the dominant episteme used to understand the threat in the field of intelligence analysis. (Vandepeer 2011) Since only the threat actor is important from the ontological point of view, it means that for Singer only the intentions and abilities of the threat actor matter.

Samuel Huntington, in T*he Soldier and the State* (1957), claims that military personnel are qualified to assess their capabilities, but not their intentions. (Huntington 1981) Despite the changes that include non-state actors' assessments as a priority, the threat remains defined using only one model, focusing specifically on the threat actor. This assumes that analysts already know and understand the threat actor they are trying to assess. Threat evaluation is based on the knowledge and understanding of an actor. Identification is presumed.

The Singer model was later extended by adding new parameters, of which the most common are *vulnerability* and *opportunity*. The vulnerability parameter focuses rather on the threat reference, resulting in vulnerability being defined as the susceptibility of a reviewer to an attack. Richard Pilch uses the following formula: (Howard and Sawyer 2003)

Threat = Vulnerability x Capability x Intent

One of the issues of the vulnerability parameter is that the more generic the target (referent) potential, the less correct will be the threat assessment.

The opportunity parameter also appears as a complement to the conventional model:

Threat = Intent x Capability x Opportunity

Opportunity incorporates an understanding of both the threat actor and the referent and can be defined as a favorable time or opportunity for a threat actor in relation to a reviewer. (Vandepeer 2011)

Despite efforts to incorporate additional parameters, the primary assumption is that the dominant episteme, with a primary focus on the threat actor, remains essential to assessing the threat.

Investigation theory addresses different ways in which each type of investigation achieves its purpose. Bennets (Holsapple 2004) distinguishes between data, information and knowledge, stating that:

> "*data* is discrete, objective facts about events which include numbers, letters and images without context, while *information* is data with some level of meaning as it describes a situation or condition. *Knowledge* is built on data and information, and is created within the individual. This knowledge represents understanding of the context, insights into the relationships within a system and the ability to identify leverage points and weaknesses and to understand the future implications of actions taken to resolve problems."

In order to produce objective intelligence, the analyst must use a process tailored to the nature of the problem, using one of the fundamental ways of reasoning: (Krizan 1999) induction (causality search, discovery of the relationships between the studied phenomena), deduction (general application, from general to specific), trained intuition (applying a spontaneous perspective, validated with available facts and tools), scientific method (hypothesis falsification and fictitious scenario testing).

Induction: When analysts make a generalization or discover relationships between phenomena based on observations or other evidence.

> "Induction consists in establishing syllogistically a relation between one extreme and the middle by means of the other extreme, e.g. if B is the middle term between A and C, it consists in proving through C that A belongs to B. For this is the manner in which we make inductions." (Aristotle 1989, chap. 2.23)

Stephen Marrin expands the inductive approach, indicating that analysts have an analytical approach in two stages. (Marrin 2012a) They use intuitive "pattern and trend analysis" - identifying repetitive behavior over time, then relying on ad hoc rules or mental models derived from the study of relevant theory - for example, economics, political science or psychology - to determine the

meaning of the model. (Duvenage 2010) Michael Collier argues that the inductive method leaves too much room for conjecture, superstition and opinion.

Deduction: Judgment starting from general rules to specific cases, if the hypothesis is tested, contrary to the inductive reasoning where the hypothesis is created.

> ”Whenever three terms are so related to one another that the last is contained in the middle as in a whole, and the middle is either contained in, or excluded from, the first as in or from a whole, the extremes must be related by a perfect syllogism. I call that term middle which is itself contained in another and contains another in itself: in position also this comes in the middle. By extremes I mean both that term which is itself contained in another and that in which another is contained. If A is predicated of all B, and B of all C, A must be predicated of all C: we have already explained what we mean by 'predicated of all'. Similarly also, if A is predicated of no B, and B of all C, it is necessary that no C will be A.” (Aristotle 1989, chap. 1.4)

Krizan quotes Clauser and Weir (Krizan 1999) who warn that deductive reasoning should be used with care in the intelligence analysis, as there are rarely closed systems, thus premises based on another set of facts, applied to a new problem and supposed to be true may be false and lead to incorrect conclusions.

Unlike deductive arguments, in inductive reasoning there is the possibility that the conclusion is false, even if all the premises are true. Instead of being valid or invalid, inductive arguments are strong or weak, which shows how likely it is that the conclusion is true.

Abduction: The unofficial or pragmatic way of reasoning to describe how we "justify the best explanation" in everyday life.

> ”We have Reduction (1) when it is obvious that the first term applies to the middle, but that the middle applies to the last term is not obvious, yet nevertheless is more probable [credible] or not less probable [credible] than the conclusion; or (2) if there are not many intermediate terms between the last and the middle; for in all such cases the effect is to bring us nearer to knowledge." (Aristotle 1989, chap. 2.25)

Waltz asserts that abduction is, in intelligence, a practical description of an interactive analysis and synthesis set to arrive at a solution or explanation, creating and evaluating more hypotheses. (Waltz 2003, 173) In abduction, the analyst creatively generates a set of hypotheses

and sets out to examine whether the available evidence is unequivocally supported by each other. The final step, namely testing the evidence, is a deductive inference. Abduction can be likened to the intuition of the analyst. This reasoning is erroneous because it is subject to cognitive errors but has the ability to extend the understanding of the intelligence matter beyond the original premises.

Scientific method: It uses induction to develop the hypothesis, and deduction is used to be tested. If testing does not validate the hypothesis, a new hypothesis should be formulated, and new experiments designed to validate this hypothesis. (Marrin 2012a) In the analysis of information there are no direct experiments and observations of the subject, but the analyst can develop hypotheses or explanations from information obtained from different sources. Hypotheses can then be examined for plausibility and iteratively tested against new information. (Duvenage 2010)

Structural analysis: It represents additional tools for traditional and intuitive analysis methods and are not just alternatives. Using structural analysis methods could not only improve the quality of intelligence analysis but also enhance the credibility of the analysis that is often prone to criticism of actual or perceived politicization and other organizational pressures. Heuer and Pherson (Heuer and Pherson 2010) classifies 50 structural analytical methods in eight categories that correlate with common cognitive traps and indicates the functions that analysts have to meet to overcome these traps. Some of these methods are:

- Decomposition and view: to exceed the limits of the working memory
- Idea generation techniques: stimulating the analyst's mind with new possibilities to investigate and visualize an intelligence problem from different angles
- Scenarios, indicators, bookmarks: identifying those who could change a situation and outlining the various possible scenarios

- Generating and testing hypotheses: analysts, in the subconscious, hypothesize each information and validate them intuitively; structured analytical tools help to examine a wider range of alternative hypotheses, possibilities and explanations
- Analysis of causes and effects: analysts should be cautious in unsafe assumptions and conclusions regarding the cause and effect of certain events or indicators
- Reframing techniques: helps analysts to change their reference/mentality frameworks to an analytical problem by changing questions or perspectives
- Challenge analysis techniques: helps deliver the best possible product to customers where there are major differences in views, highlighting minority views
- Analysis of decision support: allows analysts to see the issue from the perspective of decision-makers.

Biases: Biases can distort the correct application of inductive argumentation, thus preventing the formation of the most logical conclusion based on clues. Examples of such prejudices include availability heuristics, confirmation biases, and prediction biases.

4.1. The tacit knowledge (Polanyi)

Owen Ormerod has developed a theory that Michael Polanyi's opinion on science can contribute to understanding the process and the "product" of intelligence analysis. (Ormerod 2018) Michael Polanyi's arguments about the activities of scientists are transferable in the field of intelligence analysis, providing a nuanced perspective for perceiving the epistemological challenges and the problems faced by analysts. Polanyi's concepts of "tacit knowledge" and "personal knowledge" contribute to the development of a more efficient epistemological understanding of some aspects of the process and the intelligence analysis product.

There is a multitude of attempts, both in the national security literature and in the law enforcement literature, to align the analysis of intelligence to "scientific" principles and practices. (Cooper and Intelligence 2012) Ormerod argues that the theory developed by Polanyi is transferable in the field of intelligence. Polanyi's concepts of tacit and personal knowledge have a strong influence on the perception of the intelligence practice.

At present there is a growing interest in looking for a "theory of intelligence." (Hunter and MacDonald 2017) In this context, epistemological issues will be at the forefront of intelligence analysis. (Lillbacka 2013, 304) Intelligence analysis is a knowledge-building activity, and improved analysis requires an understanding of epistemology or the theory of origin and the nature of relevant knowledge. A discursive mode of perception of the field of intelligence can be distinguished in two fundamental ways: (Bang 2017) a) how to obtain information; b) how intelligence can help policy-makers, based on the information gathered and analyzed. (Mudd and Abbey 2015)

The epistemological bases of intelligence studies are largely extracted from the "national security" paradigm. (O'Malley 2016) Patrick Walsh has presented three fundamental characteristics that clearly represent the foundation of the intelligence profession: the "intelligence medium" (collection and analysis), "secrecy" (undercover and collection) and "supervision" (monitoring of the subjects in question). (Walsh 2010, 29)

The objectives of the intelligence analyst can generally include the following categories: 1. The prescriptive modeling required by analysts to represent how systems might work; 2. Descriptive modeling used to understand a given situation and how it works; 3. Predictive or exploratory modeling of how a dynamic system could work in the future under certain circumstances. (Waltz 2014, 2–3)

There is a strong interest in psychologically looking at the aspects of the analysis. (Heuer 1999) This is particularly true of understanding knowledge in the analysis. (Waltz 2014, 1) Analysts must be sensitive not only to the conclusions they reach, but also to the way they have come to such assertions. As Heuer observed:

> "Intelligence analysts should be self-conscious about their reasoning processes. They should think about how they make judgments and reach conclusions, not just about the judgments and conclusions themselves." (Heuer 1999, 31)

In this psychological sense, intelligence analysis is an activity that engages in meta-knowledge or, as Mark Lowenthal notes, "thought thinking". (Moore and College 2010, 8) A central purpose of intelligence analysis is a transition from "knowledge" to "understanding." (Ellis-Smith 2016, 36)

According to Ormerod, Polanyi's concept of "personal knowledge" contributes to a more nuanced epistemological framework for explaining what analysts mean to "know" the intelligence products. (Ormerod 2018) For Polanyi, truth is an objective condition, and finding truth is accomplished through the correspondence of a theory with an objective reality. (Jacobs 2001, 464) Polanyi rejects cognitive relativism or relativity of reality based on our perception. (Polanyi 1962, 315–16) Polanyi was convinced that there was an objective reality; however, to become intelligible, we must try to "establish and make our own" interpretation and understanding. (Polanyi and Sen 2009, 80) According to Polanyi, the discovery process begins at the moment when certain impressions are considered unusual and suggestive, a problem is presented to the mind; continue with collecting clues with one eye at a particular problem-solving line; and culminates in the assumption of a clear solution. (Polanyi 1964, 25)

Polanyi provides a challenging approach to understanding these epistemological issues in the intelligence analysis. For Polanyi, there is the hypothesis behind the observation act. (Polanyi 1998, 19) According to Polanyi, scientific investigations involve a perennial interaction of

imagination and observation. While the field of information activity recognizes that it is partially involved in a guessing game, the art of investigation, as Polanyi understands, offers a richer language (Colapietro 2011, 58) and the epistemological basis for recognizing this aspect in scientific and intelligence analysis.

Polanyi argues that, in order to take account of the problem-solving and discovery process, we need to recognize sufficiently the important role of tacit knowledge and the relationship that this knowledge has with tacit knowledge. Polanyi locates this form of knowledge as an essential element of his science and epistemology.

> "Polanyi's concept of personal knowledge articulates epistemologically that within the field of intelligence the work of the analyst is too diversified for there to be a single overarching 'top down' approach to understanding knowledge claims as a product ((Bang 2017), ...). According to Polanyi, since there is no 'scientific method', the scientist must draw on their personal knowledge, which importantly posits that knowledge claims must sufficiently acknowledge the role of the 'knower'. This is the central argument underpinning the idea of a bottom-up understanding of what it means to 'know' something. Knowledge claims are affirmed by the 'personal coefficient' of the analyst's personal knowledge, which according to Polanyi, is a fundamental feature of what it means to 'know' something. (Polanyi 1962, 267) Polanyi's arguments in relation to the authority of science as a valid form of inquiry and way of understanding knowledge claims as an enterprise further highlights the bottom-up way of perceiving knowledge as a product. According to Polanyi, the 'authority of scientific opinion' is 'essentially mutual', being 'established between scientists, not above them'. (Polanyi 1969, 56) The authority of knowledge claims can therefore be characterized as being bottom-up, according to Polanyi's view. This perspective has a bearing on the intelligence analysis discipline by offering an alternative way of considering a broad range of epistemological issues, principally in relation to what it means to 'know' something." (Ormerod 2018)

5. Methodologies

Methodology, in intelligence, consists of the methods used to make decisions about threats, especially in the intelligence analysis discipline.

The enormous amount of information collected by intelligence agencies often puts them in the inability to analyze them all. According to McConnell, the US intelligence community collects

over one billion daily information. (McConnell 2007) The nature and characteristics of the information gathered as well as their credibility also have an impact on the intelligence analysis.

The capability parameter is essential to the current understanding of the threat. (Vandepeer 2011) Analysts use two approaches to capacity assessment: the use of measures and proxy measures. A measure allows a direct assessment of the capacity. Proxy measures are indirect measures used to make deductions in terms of capacity.

For the assessment of a country's military weapons and armed forces, in addition to capacity measures, there are five direct measures to assess military capability: leadership and C2 (command and control); order-of-battle; force readiness and mission; force sustainability; and technical sophistication, (Joint Publication 2-01 2012) plus proxy measures (military related subjects assessment), including C4 systems (telecommunications and networks); the state's Defence industries; energy/power; geography; demography; and medical capability. State capabilities may only be known once they are effectively used against an opponent. (Vandepeer 2011)

The nature itself of an intention means that it is not "measurable" like capacity. It is estimated or deduced from observable factors, called indicators (observable factors used to deduce or observe current or future intentions). The indicators provide a means of inferring rather than quantifying.

There are three indicators that appear significantly in assessing state intentions: the military capacity of the state; ideology of the state; and words, actions and behaviors of state leaders. So, military capacity assessments are not enough to infer a state's intentions. The ideology of a state reflects political leadership, the third indicator of intentions.

Intelligence analysts are "essentially information translators, whose role is to review information and provide reliable intelligence in a practical and operational format." (Cope 2004, 188) The U.K. National Intelligence Model describes four major products resulted in the analysis process: strategic assessments, tactical assessments, target profiles and problem profiles,. (Association of Chief Police Officers, Bedford 2005) The evaluation of information implies their credibility, together with an assessment of the reliability of the sources. (Palmer 1991, 22) There are few formal information rating systems used by analysts around the world. The most common of these methods is the Admiralty System (referred to as the NATO System), which is used to demonstrate the net value of certain information based on the reliability of the source and the validity of the data. (Besombes, Nimier, and Cholvy 2009) The traditional model is a 6 x 6 matrix. Agencies operating within the National Intelligence Model in the UK use an alternative classification system commonly called the 5x5x5 system. (Joseph and Corkill 2011)

The prism theory of Robert Flood, termed by others as methodological pluralism, uses the metaphor to describe creative thinking and transformation, a prism that decomposes light into its component colors through double refraction. This type of thinking produces multiple different visions on the same thing and a common vision for many different things. Its purpose is to challenge hypotheses, provoke new ideas and generate unexpected prospects. (Flood 1999) (Duvenage 2010, 81)

The concept of prismatic thinking has gained ground in the analysis of information. Jones states that besides convergent thinking, we also need divergent thinking to ensure an effective analysis and problem solving. (M. D. Jones 2009) Divergence helps analysts analyze a more creative issue, while convergence helps to achieve completion. (Duvenage 2010, 82)

Wolfberg proposes a full-spectrum mindset, in which the analyst applies both intuitive and structural methods, depending on the specific context, assuming at the outset that there are multiple interrelated problems that need to be solved simultaneously. (Wolfberg 2006) (Duvenage 2010, 83)

Waltz conceived the integrated reasoning process, (Waltz 2003) an integrated formal and informal methods of reasoning for analysis-synthesis in the operational environment of the intelligence activity. The process stems from a set of evidence, and a question for them that explains the evidence. This process, from a set of evidence to detection, explanation or discovery, detects the presence of evidence, explains the processes underlying the evidence, and discovers new patterns in the evidence. The model illustrates four basic ways that can use the set of evidence: three fundamental ways of reasoning and a fourth way of feedback: deduction (by testing on models/hypotheses previously known), retroduction (when the analyst conjectures a new conceptual hypothesis causes a return to the set of evidence), abduction (creates explanatory hypotheses inspired by the set of evidence), induction (searching for general statements (assumptions) about evidence). (Duvenage 2010, 84–85)

Waltz typifies the analysis-synthesis process as a process of decomposing evidence and building the model, helping the analyst to identify the missing information, the strengths and weaknesses of the model. The model serves two functions: hypothesis (if the evidence is limited), and explanatory (when more evidence matches the hypothesis). The process involves three phases defined using the term "space" and the use of structural analytical techniques: data space (data is indexed and sorted), argument space (the data are reviewed, correlated and grouped into a set of hypotheses) and explanatory phase (models are composed to serve as explanations). (Duvenage 2010, 86)

The flow of cognitive process is identified as: searching and filtering, reading and extracting, schematizing, building the case, telling the story, reevaluating, looking for support, looking for evidence, looking for relationships, looking for information. (Duvenage 2010, 88)

A rigorous analytical model that can help analysts was developed by Zelik, Patterson and Woods in 2007. This model improves Heuer and Pherson's structured self-critique technique. This model has eight rigorous indicators: exploration of the hypothesis, search for information, validation of information, stance analysis, sensitivity analysis, collaboration of specialists, synthesis of information, explanation critique. This model explains cognitive processes, provides the first metric to test informational products, and provides a framework for collaborative learning. (Duvenage 2010, 91–92)

Duvenage details further the *sensemaking* concept derived from cognitive and especially organizational theory, (Weick 1995) is used in knowledge to investigate and describe how the individual, the group and, specifically, the organization are confronted with uncertainties and adapt to complexity. (Duvenage 2010, 92–93) At the individual level, sensemaking means the ability to perceive, analyze, represent, visualize and understand the environment and the situation in an appropriate contextual manner. (Cooper and Intelligence 2012) This is known in intelligence analysis as *situational awareness* or *environmental scanning*. The relevance of meaning in information analysis becomes clear when seven properties of Weick's significance are applied to the psychology of Heuer's information analysis: social context, grounded in identity construction, retrospective, driven by plausibility rather than accuracy, ongoing, extracting from salient cues, enacting. (Duvenage 2010, 94–95)

Fishbein and Treverton cite Klein, Stewart, and Claxton, who argue that empirical research has shown that intuitive judgment is the basis of most organizational decisions and is superior to analyzing problems marked by ambiguity or uncertainty. (Shulsky and Schmitt 2002)

Robert M. Clark proposed a methodology for analyzing information by addressing the target-centric intelligence cycle (Clark 2003) as an alternative to the traditional information cycle. It has redefined the informational process in the form of an integrated network where information can circulate directly between the different stages of the cycle (practically, nor is it a cycle in the traditional sense of the term).

Sherman Kent encouraged arguments and dissent among intelligence analysts to reach a "wide range of outside opinions", (Davis 1995) encouraging "collective responsibility for judgment" by networking the intelligence with loops of feedback between analysts and various stages of the intelligence cycle.

Conceptual models allow analysts to use powerful descriptive tools to estimate current situations and predict future circumstances. (Clark 2003, 37) After the model was sketched, the analyst populated the model by researching, gathering information and synthesizing. He has to find information from a wide range of classified and unclassified sources, depending on the targets.

The collected data must be collated, organized, and the evidence is evaluated for relevance and credibility. After analyzing the data, the analyst includes the information in the target model, thus determining where inconsistencies exist in the conclusions by further research to support or deny a certain conclusion. The target model shows where there are gaps in the model. Possible discrepancies force the analyst to collect additional information to better describe the goal.

Robert M. Clark's organizational model helps analysts successfully describe the target organization and see the strengths and weaknesses of the target for predictive and reliable analysis. (Clark 2003, 227)

General Stanley A. McChrystal proposed in 2014 a targeting cycle called "F3EA" used in the war in Iraq, which means:

1. Find: A target (person or location) is first identified and located.
2. Fix: The target is then kept under continuous surveillance while a Positive Identification is established.
3. Finish: A raiding force is assigned to capture or kill the target.
4. Exploit: Intelligence material is secured and mined, with detainees interrogated.
5. Analyze: Information is studied to identify further targeting opportunities. (McChrystal 2014)

Richards Heuer states that no method guarantees the success of the conclusions. Analysts need to continually improve it, depending on their specific context and previous personal experiences. (Heuer 1999) Also, in the case of a network cycle approach, it should be borne in mind that these models consume much longer than a traditional cycle. (Johnston 2005)

Structural analytical techniques are used to provoke judgment, identify mentalities, overcome prejudices, stimulate creativity, and manage uncertainty. Examples include verifying the main assumptions, competing hypothesis analysis, the devil's advocate, red team analysis, and alternative futures / scenarios analysis, among others. (US Government 2009) The following methods are ways to validate the analyst's judgment:

Opportunity analysis: Identifies, for decision-makers, opportunities or vulnerabilities that their organization can exploit.

Linchpin analysis: results from information that is certain or likely to be safe. (Davis 1999)

Analysis of competing hypotheses: The analysis of competing hypotheses was a step forward in the methodology of information analysis. More challenges, according to Heuer, are more important than more information, especially to avoid rejecting cheating at hand, as the situation seems to be simple. The steps in the analysis of competing hypotheses are: (Heuer 1999)

1. Identify the possible *assumptions* to be considered. Use a group of analysts with different perspectives to understand the possibilities.
2. Make a list of significant *evidence* and *arguments* for and against each hypothesis.
3. Prepare a matrix with assumptions at the top and evidence at the bottom. Analyze the "*diagnosis*" of evidence and arguments - that is, identify the elements that are most useful in assessing the relative probability of hypotheses.
4. *Refine* the matrix. Review hypotheses and delete proofs and arguments that do not have diagnostic value.
5. Make tentative conclusions about the relative probability and *inconsistency* of each hypothesis. Continue trying to reject assumptions rather than prove them.
6. Analyze how *sensitive* your conclusion is to some critical evidence. Consider the consequences for your analysis if this evidence was wrong, misleading or subject to a different interpretation.
7. Report the *conclusions*. Discuss the relative probability of all hypotheses, not only the most probable.
8. Identify *landmarks* for future observation that may indicate that events have a different course than expected.

Analyzing competing hypotheses is auditable and helps overcome cognitive biases. It allows the return to evidence and hypothesis, and therefore the monitoring of the succession of rules and data that led to the conclusion.

- Realistic ACH activities leave analysts disoriented or confused.

Van Gelder proposed hypothesis mapping as an alternative to competing hypothesis analysis. (van Gelder 2012)

The structural analysis of competing hypotheses provides analysts with an improvement over original limits, (Wheaton and Chido 2007) maximizing possible assumptions and allowing the analyst to divide a hypothesis into two complex assumptions.

A method, used by Valtorta and colleagues, uses probabilistic methods, adding Bayesian analysis to competing hypotheses. (Goradia, Huang, and Huhns 2005) A generalization of this concept led to the development of CACHE (Collaborative ACH Environment), (Shrager et al. 2010) which introduced the concept of the Bayesian community. The work of Akram and Wang applies paradigms in graph theory. (Shaikh Muhammad and Jiaxin 2006)

Pope's and Jøsang's works use subjective logic, a formal mathematical methodology that explicitly deals with uncertainty, (Pope and Jøsang 2005) which forms the basis of Sheba technology that is used in intelligence assessment software.

Analogy: Common in technical analysis, but the engineering features that seem the same does not necessarily mean that both have the same mode of operation just because they are similar.

In the process of intelligence analysis, analysts should follow a series of sequential steps:

1. Definition of the problem: analysts should try to understand both the mind of the opponent and the thinking of their clients and their allies.
2. Generating hypotheses: based on questions.

3. Determining information needs and gathering information: the analyst can request specific collection on the topic or, if this is not possible, identify this information gap in the final product
4. Evaluation of sources: The analyst must evaluate the information for reliability, credibility and possible false or deception.
5. Assessment of assumptions (tests): Testing by methods such as competing hypothesis analysis or linking diagrams, paying attention to cognitive and cultural prejudices inside and outside the organization.
6. Production and packaging: Very well-structured written and oral presentations, including electrical messages, printed reports, briefing, or video; three features are essential to the information product: timeliness, scope, and periodicity.
7. Peer review: Essential for assessing and confirming accuracy.
8. Feedback and product evaluation: after delivery, the process continues with the interaction between the producer and the customer, through mutual feedback, on the basis of which both analyses and requirements are refined.

Effective intelligence analysis must ultimately be tailored for the end user but without lowering the quality and accuracy of the product. (M. L. Jones and Silberzahn 2013)

6. Analogies with other disciplines

6.1. Science

Intelligence analysis has many important epistemological resemblances with science (problem solving, discovery, skillful use of tools, knowledge verification) and is more interested in *a posteriori* than *a priori* knowledge, (Agrell and Treverton 2015) on how or the basis on which a proposition may be known. (Greco and Sosa 1999, 243–70) Both intelligence analysis and

science focus on knowledge gained from empirical observations, knowledge that is typically *a posteriori*. (Ormerod 2018) Regarding the intelligence analysis, epistemological considerations are sometimes implicitly considered in the management of prejudices and uncertainties within complex intelligence systems. (M. D. Smith 2017)

Stephen Marrin and Jonathan D. Clemente note that intelligence is "subject to some amount of both random and systematic error resulting from built-in limitations of the collection instruments themselves, and as a result the information that feeds into the subsequent analysis is never an exact representation of reality." (Marrin 2012a) In order to compare the methods used in intelligence with the scientific methods, three epistemic pivotal criteria can be used: sample size, observation point and data integrity. (Pritchard and Goodman 2009)

Scientific methods involve collecting huge amounts of information to achieve meaningful results. Small sets of data are usually rejected due to statistical uncertainty. In intelligence, the size of the relevant samples is extremely small, often only a few separate sources. Gigantic data volumes are collected, but selecting relevant information is a difficult process.

In science, researchers usually keep the original data, which is examined directly, thus ensuring a high degree of reliability and certainty. In intelligence, data and information rarely come to analysts at first hand. Even the identity of certain people may be uncertain.

In science, researchers are mindful of their own prejudices, but in general the data is not consciously affected. In the intelligence world, the situation is very different: data and information are deliberately and on a large scale manipulated with the intent of distorting reality. Sometimes even members of the same organization included in the intelligence cycle have reason to distort data or even to input false data, often for money or other benefits.

After the September 11 attacks in the United States, efforts have been intensified to make more "scientific" the methods used in intelligence. (Marrin and Torres 2017) Some of the earliest works in the field, including of Sherman Kent, have supported scientific methods not only in understanding certain issues but also in making verifiable evaluations. (Agrell 2012, 130) R. A. Random wrote in 1958 that the rejection of scientific methodology in favor of intuition would be like abandoning rationality in favor of "guessing." (Marrin 2012c, 2) Other researchers in the field of intelligence have argued that the scientific method is fundamental for the intelligence analysis. (Marrin 2012c, 531)

The characteristics of such a "scientific method" are data collection, hypothesis formation, hypothesis testing, and obtaining conclusions that can be used as reliable predictive sources. (Platt 1957, 75)

This analogy is generally considered to be correct insofar as the process is "systematic" and "logical": (Ylikoski 2017) "As a science, intelligence analysis is a systematic process, which generates and tests hypotheses objectively. Following the scientific method, analysts adhere to rules to develop sound and logical judgments." (Martin 2011, 30)

Both science and intelligence refer to "verifying" as well as "falsifying" the assertions of knowledge. (Shrager et al. 2010) Efforts in the field of intelligence to align the analysis with the objectives of science, especially with "falsification", have been promoted by several scientists. (Shaikh Muhammad and Jiaxin 2006) As Polanyi explains, centralizing understanding of knowledge in science is a sufficient recognition of personal knowledge, partly because there are no "rules" in the field of science. (Ormerod 2018) For this reason, according to Polanyi, the scientist must rely on personal knowledge to make decisions about, for example, whether the evidence or clues must be accepted or rejected, just like the intelligence analyst. Polanyi's

arguments have an impact both on the field of national security and on law enforcement from intelligence analysis, as these areas use empirical observations to develop and understand the assertions of knowledge. (Peters and Cohen 2017) In the field of national security, empiricism can be observed in the existence of large systems of intelligence gathering. Polanyi contests the epistemological basis of excessive faith toward the supposed central role of empiricism and the logic of induction in science: "The part played by new observations and experiments in the process of discovery in science is usually over-estimated," (Polanyi 1964, 29) a vision opposed to conventional understanding of the science promoted by Karl Popper. (Popper 1972, 23–27)

6.2. Archeology

The puzzle metaphor is used in both information and archeology. Both disciplines involve collecting evidence to build as complete a picture as possible. (Pritchard and Goodman 2009) Some tracks are not seen from the beginning, and others are deformed and cannot contribute to the logic of assembling. Maybe it would be useful to use the reverse engineering, in order to understand how the original image split, what are the stages, and what happened to the missing pieces.

David Clarke highlighted a theory of archeology based on the relationship between the ancient known culture and the remains discovered by the excavator, a completed puzzle and the missing pieces to be analyzed.

The necessary steps in any archaeological interpretation are:

1. The range of patterns of social and environmental activities and processes that once existed, that is, what the archeologist is trying to understand (ie, the total activity relevant to requesting the intelligence service).

2. The sample and remnants that were stored at that time (intelligence analysts are trying to find out what elements of their opponent's activity becomes intelligence, what is to be collected and from what sources).
3. Sample of that specimen which has survived and is to be recovered (fragments of intelligence held by certain sources, considering their possible distortion).
4. Sample of the specimen which is recovered. (intelligence gathered through different collection systems and sources of primary importance) (Clarke 1968)

The archaeologist might use the intuition for interpretation, but he can make it very easy. The intelligence analyst, in turn, tries to understand the problem using what is available, that is, a part of the sample.

After identifying the accuracy of the intelligence activity for each step, the following applicable theory types can be considered:

Theory of suppositions and depositions: The link between 1 and 2. Determining the relationship between the divided total activity and the sample that is potentially accessible to the collection systems. Which sources should be used? What are the prejudices?

Post-depositional theory: The relationship between 2 and 3. To what extent can the passage of time distort the sample?

The theory of restoration: The link between 3 and 4. To what extent the data collected represents all that it is possible? How much material has been gathered and what nature? Which similar activities could take place elsewhere where access is easy?

Analytical theory: The link between 4 and 1. The intelligence collector must select the relevant information, depending on the analyst's understanding of the intelligence requirements. At the same time, constraints (technological or other) may limit the capacity of the collector to

transmit certain types of data for further analysis. In this case, certain prioritization decisions can be made by giving up some information.

Theory of interpretation: The analyst provides his/her assessments to decision-makers. Here, cognitive biases appear, and methods are used to contract them by questioning hypotheses and generating alternative assumptions.

The archaeological analogy is far from perfect. But it illustrates the steps by which a picture is fragmented into fragments for analysis. Analysts should be aware that their data is incomplete, but the nature of this incompleteness may not be fully understood, leading to the possibility of serious implications. (Pritchard and Goodman 2009)

6.3. Business

Intelligence is traditionally characteristic of governmental organizations involved in national security issues. But innovative private companies are increasingly adapting the model of intelligence services to the business world to help plan their own strategies. The process of converting raw information into actionable processed intelligence is almost identical for governmental and business organizations, the latter developing the intelligence gathering and analysis system with its own methodologies. (Krizan 1999)

The two activities seem to be two independent areas, but the approach to the challenges is quite similar, depending on warning capabilities; (Miscik 2017) decision makers in both cases are expected to find out about threats and opportunities in advance. Academic research has demonstrated that it is possible to perform a comparative analysis of the two areas (government and business) and identify possible parallels between them. (Barnea 2018) In both areas, the product of the intelligence activity is the one that supports the decision-making process as a result of information about changes in the external environment caused by specific threats. But the

ontological, epistemological and methodological study of this process is much better developed today in business (Busenitz and Barney 1997) so that national intelligence services can take on many of the theories and techniques developed in the field of competitive intelligence.

A fundamental resemblance between national intelligence and competitive intelligence is that both operate based on an "intelligence cycle," (Omand 2011) a multi-stage systematic process that ensures the conduct of intelligence under control.

Competitive intelligence (CI) is a domain whose work consists in defining, collecting, analyzing and distributing information on product, customers, competitors, and any environmental aspect needed to assist executives and managers in strategic decision-making for an organization. It is a legal business practice, unlike industrial espionage, which is illegal. (SCIP 2014) The CI focuses on the external business environment, (Haag 2012) being a process involved in collecting information, transforming it into processed intelligence and then using it in decision-making. (McGonagle and Vella 2003)

CI is often seen as synonymous with competitors' analysis, but it is more than just analyzing competitors; includes the entire environment and stakeholders: customers, competitors, distributors, technologies and macroeconomic data. Organizations use CI to compare with other organizations ("competitive comparison") to identify the risks and opportunities in their markets and to test their plans for market response. ("Business Warfare") (Kurtz 2018)

Strategic intelligence focuses on long-term issues, analyzing aspects that affect the competitiveness of a company over a few years. The real time horizon for strategic intelligence ultimately depends on industry and how fast it is changing. This type of intelligence involves, among other things, the identification of weak signals and the application of a specific methodology and process initially developed by Gilad. (Gilad 2014)

In *tactical intelligence*, the emphasis is on providing information to improve short-term decisions, most often related to the intention of increasing market share or revenue.

The technical advances of massive parallel processing offered by the "big data" architecture have allowed the creation of multiple platforms for the recognition of target entities. (Krapohl 2013)

CI was influenced by national strategic intelligence. Fleisher suggests that business intelligence has two forms. Its more limited (contemporary) shape focuses more on information technology and on internal focus than the CI, while the broader (historical) definition is more comprehensive than CI. Knowledge management, when specifically designed, is seen as an organizational practice based on information technology that uses data mining, corporate intranets, and organizational asset mapping to make it accessible to decision-makers. The CI share some aspects with knowledge management; contains human and experience-based information for a more sophisticated qualitative analysis. Knowledge management is essential for effective change. An effective key factor is a powerful IT system dedicated to the execution of the entire intelligence cycle. (Barnea 2009)

Business intelligence (BI) is "a set of methodologies, processes, architectures, and technologies that transform raw data into meaningful and useful information used to enable more effective strategic, tactical, and operational insights and decision-making." (Evelson 2008) BI *technologies* can handle large amounts of unstructured data to help identify, develop, and create new business strategic opportunities. The *purpose* of BI is to allow easy interpretation of these large volumes of data. (Sfetcu 2016) The BI technologies offer historical, current and predictive perspectives of business operations. Common *functions* of BI technologies are reporting, online analytical processing, analytical research, data mining, process mining, complex event processing,

business performance management, benchmarking, text mining, predictive analysis and prescriptive analysis.

BI can be used to support a wide range of business decisions, from operational to strategic. When combined, internal and external data can provide a more complete picture that creates "processed intelligence" that cannot be inferred through any single set of data. (Feldman and Himmelstein 2013)

Often, BI scenarios revolve around distinct business processes, each built on one or more data sources. These milestones of business intelligence include, but are not limited to:

- Data sources to collect the necessary data
- Transform the data into intelligence and present it appropriately
- Querying and analyzing data
- Act on collected data.

A notable similarity between government and business intelligence is the goal of maximizing the profits of customer intelligence products. Changes are difficult to monitor due to the difficulty in assessing the significance of signals and noise in predictions to reduce uncertainty. (Rafii and Kampas 2002) Also, based on the processed information, both proactively act and attempt to obtain information that can send alerts about the relevant changes and their meanings. (Prescott 2012) In both areas, the intelligence provided to decision-makers can often be a catalyst for future action and a new initiative to gain benefits.

6.4. Medicine

The medical practice of diagnosing identification, collection, analysis and dissemination is similar to that of intelligence. (Converse 2008, 1) Marrin and Clemente argue that both disciplines apply similar general approaches to obtain information. (Marrin and Clemente 2005, 709) In order

to better understand the data and intelligence gathered, the analyst calls for related disciplines, similar to doctors in the diagnosis of patients.

According to Owen Ormerod, another similarity occurs in the challenges faced both by integration of diagnosis or analytical assessments in a wider context, ranging from alternative hypotheses to evidence that invalidate, and using deductive and inductive judgments to distinguish relevant intelligence from noise. (Marrin and Clemente 2005, 715)

"Underlying the perceived similarities between intelligence analysis and the medical profession is the belief that as more information is collected, the practitioner will become more confident in their assessment." (Treverton 2011, 40) But this is not always true. Under certain circumstances of the medical profession, the diagnostic process involves considerations that are not "scientific" or structured in a typical way, but are related to doctor bias, craftsmanship and what Polanyi would call "personal knowledge." Post-structuralist Michael Foucault presented a similar argument that the work of the doctor is influenced by the surrounding culture, as it does not "discover" the truth "there" but rather assembles it in the mind, which is partly a product of its environment. It is too simplistic to understand the activity of the doctor or intelligence analyst as neutral observers who only collect and analyze "the facts." (Ormerod 2018, 28)

Some intelligence experts have argued that intelligence analysis can benefit from adopting models similar to those in the medical field. (Manjikian 2013, 1) Richards Heuer has indicated the medical field as a profession that could be imitated by the intelligence. As he states, (Heuer 1999, 62) the physician observes the symptoms of the patient and, by using his expert knowledge of the body, a hypothesis is generated to explain such observations, followed by tests to collect additional information to evaluate the hypothesis and apply a diagnosis. This medical analogy emphasizes the ability to correctly identify and evaluate all plausible assumptions. In this sense, the collection

is focused on information that might reveal alternative assumptions: "While analysis and collection are both important, the medical analogy attributes more value to analysis and less to collection than the mosaic metaphor." (Heuer 1999, 62)

7. Conclusions

There is no universal consensus on how we need to better understand intelligence analysis. There are gaps in the literature on the epistemological dimensions of intelligence analysis, both in terms of the analysis process and the products or what it means to "know" something. Polanyi's views on how scientists engaging in problem solving will contribute to understanding the epistemological process and the intelligence analysis product. He stressed that "practical knowledge" of scientists about understanding phenomena is an illustration of the instrumental function of tacit knowledge. (Ormerod 2018) The relationship between tacit and explicit knowledge is the key to understanding the value of treating this concept of Polanyi. He argued that there was a strong link between tacit knowledge and personal knowledge, concluding that the logic of perception (partly obtained by tacit knowledge) is the same as the logic of discovery and hence of the knowledge produced - personal knowledge. Polanyi's nuanced language to cover perceptual awareness provides a new context for intelligence to analyze a series of conceptual and practical issues in an epistemological sense. These ideas, applied to the epistemological considerations faced by the analyst in the analysis process and the use of structural analytical techniques, will enrich the language and logic for understanding these issues. Polanyi's personal knowledge theory brings new arguments about analyzing intelligence as a product

According to Owen Ormerod, intelligence analysis can be characterized as an epistemological enterprise that seeks to develop a clear understanding of knowledge products. Polanyi's perspective on knowledge serves fundamental epistemological considerations on

knowledge as a product. The perspective reverses the traditional epistemological hierarchy, which usually apprehends the propositional knowledge of more than "tacit" or "personal" ways to understand the claims of knowledge. This epistemological position contributes to intelligence discipline by giving a more solid image of the personal dimension of knowledge as a product. Approaches to what it means to "know" something gives the analysis of intelligence a nuanced and detailed epistemological understanding of the personal dimension of knowledge and knowledge as a product.

This is a nuanced way of understanding deeper, from an epistemological point of view, the process of problem solving in the intelligence analysis process. Adequate recognition of the primacy of tacit knowledge is fundamental to better appreciate the problem-solving process of intelligence analysis. This provides a robust epistemological explanation of the problem-solving process, which serves to articulate the familiar general aspect of "knowledge" in the intelligence activity. Importantly, this framework for understanding the process of a skilled practice involving the tacit knowledge of the practitioner underscores the centralization of these epistemological issues facing the intelligence analyst and extends the discourse in this area. (Ormerod 2018)

Since the activity of the intelligence analyst is sometimes "messy and contingent" (Dahl 2017) rather than "systematic" and "logical", it may be possible to understand the activities of analysts as an "artistic enterprise" involving both aspects of "art" as well as science. (Bang 2017)

Analysts should be aware of their reference frameworks, the intuitive methods they use, and the other more structural methods available to add value, especially when individual interpretation is insufficient. The various analytical tools and techniques will help analysts and decision-makers understand, verbalize, and communicate their thinking processes. Analysts should ideally be trained in all different tools and techniques so that they can apply the most

appropriate, intuitive/unauthorized or structured tool to a specific problem and stage of the intelligence process. (Duvenage 2010)

The biggest challenge could be to persuade analysts, their management and their clients of the advantages of structural analytical methods. A gradual and natural introduction of these methods into the usual flow of processes and intelligence products could be more effective than real-world thinking on a large scale. Creating training opportunities as well as educating clients to request evidence of application of techniques could contribute to this process.

This would involve a strong commitment from intelligence services, with the potential to change the perishable nature of those who have remained tributary to traditional methods. The "space" of intelligence has expanded from governments to NGOs, transnational institutions and corporations, private firms and interest and pressure groups representing diverse communities, concepts and ideologies. Warning on time has become crucial. The decision-making process has become dispersed and granular. The current "democratization" of intelligence services has a major impact on the collection and analysis of information and decision-making, causing intelligence services to become more transparent, to consider public debates about their actions, and sometimes to justify publicly.

Also, the recent terrorist attacks in the United States, Great Britain, Spain, France, etc., have demonstrated the need for integrating factors, a collaboration between all intelligence organizations to get an overview and to effectively and timely prevent actions against national security, redefining not only the new paradigm of the threat but also how organizations respond and adapt to these new challenges.

Law enforcement and intelligence institutions in developing countries rarely have adequate information systems, underestimating the value of analysts. Quiggin presents a daunting image,

(Quiggin 2007) stating that less than 1% of country's budgets for intelligence are spent for analysis, while 99% is spent on technology, secrecy, infrastructure and other items. All specialists agree that, in the current geopolitical situation, a synergy between intelligence organizations, intelligence analysts and academia is mandatory. The trend in the United States is to provide bachelor, master and doctorate programs related to intelligence.

An area that can benefit from intelligence services is knowledge management, involved in a rigorous debate on concepts, theories and approaches to knowledge and its use. Knowledge management theorists such as Firestone and McElroy suggest intelligence organizations take into account the benefits that this discipline could bring to their activity. (Firestone and McElroy 2003)

The major changes in the US intelligence analysis framework in recent years, through the establishment of alternative analysis methods and facilitating inter-organizational collaboration through the latest web technologies, including social networks, have produced over-expectations. Unfortunately, very few countries have gone along this path by renouncing the convenience of traditional strategies. The new intelligence paradigm requires major organizational changes and training of professionals to understand and adopt new concepts and technologies.

Intelligence services have gradually begun to grasp the need to study other disciplines, including business or philosophical (ontological, epistemological, methodological) aspects of their own activities, to see how they can improve their skills and deal with new challenges. An excellent example is how the FBI reinvented after September 11 following a notable study by three Harvard researchers led by Jan Rivkin. (Gulati, Raffaelli, and Rivkin 2016)

Bibliography

Agrell, Wilhelm. 2012. "The Next 100 Years? Reflections on the Future of Intelligence." *Intelligence and National Security* 27 (1): 118–32. https://doi.org/10.1080/02684527.2012.621601.

Agrell, Wilhelm, and Gregory F. Treverton. 2015. *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*. Oxford, New York: Oxford University Press.

Aladashvili, Besik. 2017. *Fearless: A Fascinating Story of Secret Medieval Spies*.

Anderson, Terence, David Schum, and William Twining. 2009. *Analysis of Evidence*. 2 edition. Cambridge; New York: Cambridge University Press.

Andrew, Christopher. 2018. *The Secret World: A History of Intelligence*. New Haven, CT: Yale University Press.

Aristotle. 1989. *Prior Analytics*. Hackett Publishing.

———. 1991. "The Metaphysics." 1991. https://www.amazon.com/Metaphysics-Great-Books-Philosophy/dp/0879756713.

Arrow, Kenneth J. 1966. "Exposition of the Theory of Choice under Uncertainty." *Synthese* 16 (3): 253–69. https://doi.org/10.1007/BF00485082.

Artner, Stephen, Richard S. Girven, and James Bruce. 2016. "Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community." Product Page. 2016. https://www.rand.org/pubs/research_reports/RR1408.html.

Association of Chief Police Officers, Bedford. 2005. "Guidance on the National Intelligence Model." https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf.

Australia Department of Defence. 2002. "Future Warfighting Concept." http://www.defence.gov.au/publications/fwc.pdf.

Australia Department of Defence, Canberra. 2009. "Defending Australia in the Asia Pacific Century: Force 2030 (2009 Defence White Paper)." Text. 2009. https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1516/DefendAust/2009.

Bang, Martin. 2017. "A Shared Epistemological View Within Military Intelligence Institutions." *International Journal of Intelligence and CounterIntelligence* 30 (1): 102–16. https://doi.org/10.1080/08850607.2016.1177401.

Barnea, Avner. 2009. "Intelligence Solutions Through the Use of Expert Tools_CIM_March_April_09 | International Politics | Israel." Scribd. 2009. https://www.scribd.com/document/17752171/Intelligence-Solutions-Through-the-Use-of-Expert-Tools-CIM-March-April-09.

———. 2018. "Nationak Strategic Intelligence and Competitive Intelligence: How a Comparative View and Mutual Learning Can Help Each?" ResearchGate. 2018. https://www.researchgate.net/publication/323884850_Nationak_Strategic_Intelligence_and_Competitive_Intelligence_How_a_Comparative_View_and_Mutual_Learning_Can_Help_Each.

Berkowitz, Bruce. 2002. "Intelligence and the War on Terrorism." ResearchGate. 2002. https://www.researchgate.net/publication/248543624_Intelligence_and_the_War_on_Terrorism.

Berkowitz, Bruce D., and Allan E. Goodman. 2000. *Best Truth: Intelligence in the Information Age*. Yale University Press.

Besombes, Jérôme, Vincent Nimier, and Laurence Cholvy. 2009. "Information Evaluation in Fusion Using Information Correlation." ResearchGate. 2009. https://www.researchgate.net/publication/224577351_Information_evaluation_in_fusion_using_information_correlation.

Bittner, Thomas, and Barry Smith. 2003. "A Theory of Granular Partitions." In *Foundations of Geographic Information Science*, edited by M. Duckham, M. F. Goodchild, and M. F. Worboys, 117–151. London: Taylor & Francis.

Boyd, John R. 1976. "Destruction and Creation." http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf.

Brei, William S. 1996. *Getting Intelligence Right: The Power of Logical Procedure*. Joint Military Intelligence College.

Bulgacs, Simon. 2013. "The First Phase of Creating a Standardised International Innovative Technological Implementation Framework/Software Application." *International Journal of Business and Systems Research* 7 (3): 250. https://doi.org/10.1504/IJBSR.2013.055312.

Busenitz, Lowell W., and Jay B. Barney. 1997. "Differences between Entrepreneurs and Managers in Large Organizations: Biases and Heuristics in Strategic Decision-Making." *Journal of Business Venturing* 12 (1): 9–30. https://doi.org/10.1016/S0883-9026(96)00003-1.

Buzan, Barry, Ole Wæver, Ole Waever, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

Cao, Longbing. 2010. "(PDF) Domain-Driven Data Mining: Challenges and Prospects." ResearchGate. 2010. https://www.researchgate.net/publication/220073304_Domain-Driven_Data_Mining_Challenges_and_Prospects.

Chomsky, Noam. 1992. *Deterring Democracy*. Reissue edition. New York: Hill and Wang.

CIA.gov. 2009a. "Our Mission — Central Intelligence Agency." 2009. https://www.cia.gov/offices-of-cia/clandestine-service/our-mission.html.

———. 2009b. "Who We Are — Central Intelligence Agency." 2009. https://www.cia.gov/offices-of-cia/clandestine-service/who-we-are.html.

Clark, Robert M. 2003. *Intelligence Analysis: A Target-Centric Approach*. Washington, D.C: Cq Pr.

Clarke, David L. 1968. *Analytical Archaeology*. Methuen.

Codevilla, Angelo. 1992. *INFORMING STATECRAFT (INTELLIGENCE FOR A NEW CENTURY)*. Free Press.

Colapietro, Vincent. 2011. "Intellectual Passions, Heuristic Virtues, and Shared Practices: Charles Peirce and Michael Polanyi on Experimental Inquiry." Tradition and Discovery: The Polanyi Society Periodical. 2011. https://doi.org/10.5840/traddisc2011/201238326.

Conrad, Sherri J. 1985. "Executive Order 12,333: Unleashing the CIA Violates the Leash Law." https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=4410.

Converse, Ray. 2008. "Intelligence and Medicine: Parallel Cognitive Traps." http://www.pherson.org/wp-content/uploads/2013/11/03.-Intelligence-and-Medicine-Parallel-Cognitive-Traps_FINAL.pdf.

Cooper, Jeffrey R., and Center for the Study of Intelligence. 2012. *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*. CreateSpace Independent Publishing Platform.

Cope, Nina. 2004. "'Intelligence Led Policing or Policing Led Intelligence?' Integrating Volume Crime Analysis into Policing." *The British Journal of Criminology* 44 (2): 188–203. https://doi.org/10.1093/bjc/44.2.188.

Cross, Mai'a K. Davis. 2015. "The Limits of Epistemic Communities: EU Security Agencies." ResearchGate. 2015. https://www.researchgate.net/publication/270578352_The_Limits_of_Epistemic_Communities_EU_Security_Agencies.

Cunningham, Hamish. 2006. "Information Extraction, Automatic." ResearchGate. 2006. https://www.researchgate.net/publication/228630298_Information_Extraction_Automatic.

Dahl, Erik J. 2017. "Getting beyond Analysis by Anecdote: Improving Intelligence Analysis through the Use of Case Studies." *Intelligence and National Security* 32 (5): 563–78. https://doi.org/10.1080/02684527.2017.1310967.

Davis, Jack. 1995. "A Policymaker's Perspective On Intelligence Analysis." https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol38no5/pdf/v38i5a02p.pdf.

———. 1999. "Improving Intelligence Analysis at CIA: Dick Heuer's Contribution to Intelligence Analysis." 1999. http://www.au.af.mil/au/awc/awcgate/psych-intel/art3.html.

Dean, Geoff, and Petter Gottschalk. 2007. *Knowledge Management in Policing and Law Enforcement: Foundations, Structures and Applications*. Oxford, New York: Oxford University Press.

Department of Homeland Security. 2010. "Quadrennial Homeland Security Review Report: A Strategic Frameworkfor a Secure Homeland." https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

Deshmukh, Pranita P., and Mir Shabbar Ali. 2014. "Overview of Xml Based Knowledge Representation Using Scripts." In .

Diane Publishing Company. 2000. *A Consumer's Guide to Intelligence*. Diane Publishing Company.

Duvenage, Magdalena Adriana. 2010. "Intelligence Analysis in the Knowledge Age : An Analysis of the Challenges Facing the Practice of Intelligence Analysis." Thesis, Stellenbosch : University of Stellenbosch. https://scholar.sun.ac.za:443/handle/10019.1/3087.

Ehrman, John. 2009. "Toward a Theory of CI — Central Intelligence Agency." 2009. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no2/toward-a-theory-of-ci.html.

———. 2011. "What Are We Talking About When We Talk about Counterintelligence?" ResearchGate. 2011. https://www.researchgate.net/publication/237421011_What_are_We_Talking_About_When_We_Talk_about_Counterintelligence.

Ekpe, Bassey. 2005. "Theories of Collective Intelligence and Decision-Making: Towards a Viable United Nations Intelligence System." Doctoral, University of Huddersfield. http://eprints.hud.ac.uk/id/eprint/7481/.

Ellis-Smith, James. 2016. "Analysis and Influence in Combat Intelligence." *Journal of the Australian Institute of Professional Intelligence Officers* 24 (1): 34. http://search.informit.com.au/documentSummary;dn=256667623307302;res=IELHSS.

Evans, Jonathan. 2007. "Jonathan Evans, MI5 Director General's Speech on Intelligence, Counter-Terrorism and Trust, 5 November 2007." https://www.theguardian.com/uk/2007/nov/05/terrorism.world.

Evelson, Boris. 2008. "Topic Overview: Business Intelligence." 2008. https://www.forrester.com/report/Topic+Overview+Business+Intelligence/-/E-RES39218#.

Feigenbaum, Edward A., and Pamela McCorduck. 1984. *The Fifth Generation: Artificial Intelligence and Japan's Computer Challenge to the World*. New American Library.

Feldman, David, and Jason Himmelstein. 2013. *Developing Business Intelligence Apps for SharePoint: Combine the Power of SharePoint, LightSwitch, Power View, and SQL Server 2012*. 1 edition. Beijing: O'Reilly Media.

Firestone, Joseph M., and Mark W. McElroy. 2003. *Key Issues in the New Knowledge Management*. Butterworth-Heinemann.

Flood, Robert L. 1999. *Rethinking The Fifth Discipline: Learning Within the Unknowable*. Psychology Press.

Floridi, Luciano. 2002. "What Is the Philosophy of Information?" *Metaphilosophy* 33 (1–2): 123–45. https://doi.org/10.1111/1467-9973.00221.

Gelder, Tim van. 2012. "Exploring New Directions for Intelligence Analysis." *Tim van Gelder* (blog). 2012. https://timvangelder.com/2012/12/11/exploring-new-directions-for-intelligence-analysis/.

Gentry, John A. 2015. "Has the ODNI Improved U.S. Intelligence Analysis?" *International Journal of Intelligence and CounterIntelligence* 28 (4): 637–61. https://doi.org/10.1080/08850607.2015.1050937.

Gilad, Ben. 2014. "CI Education Harvard Style?" http://www.academyci.com/wp-content/uploads/2014/09/CI_Harvard_Style.pdf.

Godfrey, E. Drexel. 1978. "Ethics and Intelligence." *Foreign Affairs*, 1978. https://www.foreignaffairs.com/articles/united-states/1978-04-01/ethics-and-intelligence.

Goodman, Michael S. 2007. "Studying and Teaching About Intelligence: The Approach in the United Kingdom — Central Intelligence Agency." 2007. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol50no2/html_files/Studying_Teaching_6.htm.

Goradia, Hrishikesh, Jingshan Huang, and Michael N Huhns. 2005. "Extending Heuer's Analysis of Competing Hypotheses Method to Support Complex Decision Analysis." ResearchGate. 2005. https://www.researchgate.net/publication/241836758_Extending_Heuer's_Analysis_of_Competing_Hypotheses_Method_to_Support_Complex_Decision_Analysis.

Greco, John, and Ernest Sosa. 1999. *The Blackwell Guide to Epistemology*. 1 edition. Malden, Mass: Wiley-Blackwell.

Grenon, Pierre, and Barry Smith. 2004. "SNAP and SPAN: Towards Dynamic Spatial Ontology." http://ontology.buffalo.edu/smith/articles/SNAP_SPAN.pdf.

Gulati, Ranjay, Ryan Raffaelli, and Jan Rivkin. 2016. "Does 'What We Do' Make Us 'Who We Are'? Organizational Design and Identity Change at the Federal Bureau of Investigation." https://www.hbs.edu/faculty/Pages/item.aspx?num=50565.

Haag, Stephen. 2012. *Management Information Systems for the Information Age: Ninth Edition*. McGraw-Hill Higher Education.

Haas, Peter M. 1992. "Introduction: Epistemic Communities and International Policy Coordination | International Organization | Cambridge Core." 1992. https://www.cambridge.org/core/journals/international-organization/article/introduction-epistemic-communities-and-international-policy-coordination/CE9CFC049E0F2A14635F1E3EB51960C9.

———. 2001. "Policy Knowledge: Epistemic Communities." In *International Encyclopedia of the Social and Behavioral Sciences*, edited by N. J. Smelser and B. Baltes, 17–11578.

Hayes, Joseph. 2007. "Chapter One — Central Intelligence Agency." 2007. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_1.htm.

Herman, Michael. 2001. *Intelligence Services in the Information Age: Theory and Practice*. Taylor & Francis.

Heuer, Richards J. 1999. *Psychology of Intelligence Analysis*. Lulu.com.

Heuer, Richards J., and Randolph H. Pherson. 2010. *Structured Analytic Techniques for Intelligence Analysis*. CQ Press.

Hogan, Bernie, Juan Antonio Carrasco, and Barry Wellman. 2007. "Visualizing Personal Networks: Working with Participant-Aided Sociograms." *Field Methods* 19 (2): 116–44. https://doi.org/10.1177/1525822X06298589.

Holsapple, Clyde, ed. 2004. *Handbook on Knowledge Management 1: Knowledge Matters*. International Handbooks on Information Systems. Berlin Heidelberg: Springer-Verlag. //www.springer.com/gp/book/9783540435273.

Howard, Russell, and Reid Sawyer. 2003. *Terrorism and Counterterrorism: Understanding the New Security Environment, Readings and Interpretations, Revised & Updated 2004*. 1 edition. Guilford, Conn.: McGraw-Hill/Dushkin.

Hsu, Jennifer Y. J., and Reza Hasmath. 2017. "A Maturing Civil Society in China? The Role of Knowledge and Professionalization in the Development of NGOs." SSRN Scholarly Paper ID 2563696. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2563696.

Hulnick, Arthur S. 2006. "What's Wrong with the Intelligence Cycle." 2006. https://www.researchgate.net/publication/245493621_What's_Wrong_with_the_Intelligence_Cycle.

Hunter, Duncan, and Malcolm N. MacDonald. 2017. "The Emergence of a Security Discipline in the Post 9-11 Discourse of U.S. Security Organisations." *Critical Discourse Studies* 14 (2): 206–22. https://doi.org/10.1080/17405904.2016.1268185.

Huntington, Samuel P. 1981. *The Soldier and the State: The Theory and Politics of Civil–Military Relations*. Revised edition. Cambridge, Mass: Belknap Press: An Imprint of Harvard University Press.

Husserl, Edmund. 1900. "Logische Untersuchungen." 1900. https://philpapers.org/rec/HUSLU.

Ikle, Fred. 2005. *Every War Must End (Columbia Classics)*. Revised edition edition. Columbia University Press.

Intelligence.gov. 2013. "Seventeen Agencies and Organizations United Under One Goal." 2013. https://web.archive.org/web/20130502012837/http://www.intelligence.gov/about-the-intelligence-community/.

Jacobs, Struan. 2001. "Michael Polanyi, Tacit Cognitive Relativist." *Heythrop Journal* 42 (4): 463–479.

Johnson, William R., and William Hood. 2009. *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer*. 3.2.2009 edition. Washington, D.C: Georgetown University Press.

Johnston, Rob. 2003. "Integrating Methodologists into Teams of Substantive Experts." https://apps.dtic.mil/dtic/tr/fulltext/u2/a525552.pdf.

———. 2005. *Analytic Culture in the US Intelligence Community: An Ethnographic Study*. University of Michigan Library.

Joint Publication 2-01. 2012. "Joint and National Intelligence Support to Military Operations." https://www.bits.de/NRANEU/others/jp-doctrine/jp2_01%2812%29.pdf.

Jones, Milo L., and Philippe Silberzahn. 2013. "Constructing Cassandra: Reframing Intelligence Failure at the CIA, 1947–2001 | Milo Jones and Philippe Silberzahn." 2013. http://www.sup.org/books/title/?id=22067.

Jones, Morgan D. 2009. *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*. Crown Publishing Group.

Jordan, Lloyd F. 2008. "The Arab Mind by Raphael Patai. Book Review by Lloyd F. Jordan — Central Intelligence Agency." 2008. https://web.archive.org/web/20080213114422/https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v18i3a06p_0001.htm.

Joseph, John, and Jeff Corkill. 2011. "Information Evaluation: How One Group of Intelligence Analysts Go about the Task." *Australian Security and Intelligence Conference*, January. https://doi.org/10.4225/75/57a02d74ac5c9.

Keman, Hans. 1998. *Autonomous Policy Making By International Organisations*. Edited by Bob Reinalda and Bertjan Verbeek. London ; New York: Routledge.

Kent, SHERMAN. 1966. *Strategic Intelligence for American World Policy*. Princeton University Press. https://www.jstor.org/stable/j.ctt183q0qt.

Keynes, J. M. 1937. "The General Theory of Employment." *The Quarterly Journal of Economics* 51 (2): 209–23. https://doi.org/10.2307/1882087.

Krapohl, Don. 2013. "Working .NET Entity Extractor Using OpenNLP Models." *A | I – Augmented Intelligence* (blog). 2013. http://www.augmentedintel.com/wordpress/index.php/augmented-intel-free-online-analytics-applications-for-corporate-intelligence/working-net-entity-extractor-using-opennlp-models/.

Krizan, Lisa. 1999. "Intelligence Essentials for Everyone." ResearchGate. 1999. https://www.researchgate.net/publication/235073074_Intelligence_Essentials_for_Everyone.

Kurtz, Jay. 2018. "What Is A Business Wargame?" 2018. http://competitive-intelligence.mirum.net/competitive-intelligence-methods/what-is-a-business-wargame.html.

Kydd, Andrew. 1997. "Game Theory and the Spiral Model." *World Politics* 49 (3): 371–400. https://www.jstor.org/stable/25054007.

Laqueur, Walter. 1993. *The Uses and Limits of Intelligence*. Transaction Publishers.

Leckie, Gloria J., Karen E. Pettigrew, and Christian Sylvain. 1996. "Modeling the Information Seeking of Professionals: A General Model Derived from Research on Engineers, Health Care Professionals, and Lawyers." ResearchGate. 1996. https://www.researchgate.net/publication/237440858_Modeling_the_Information_Seekin

g_of_Professionals_A_General_Model_Derived_from_Research_on_Engineers_Health_Care_Professionals_and_Lawyers.
Lillbacka, Ralf G. V. 2013. "Realism, Constructivism, and Intelligence Analysis." *International Journal of Intelligence and CounterIntelligence* 26 (2): 304–31. https://doi.org/10.1080/08850607.2013.732450.
Little, E. G., and G. L. Rogova. 2005. "Ontology Meta-Model for Building a Situational Picture of Catastrophic Events." *2005 7th International Conference on Information Fusion* 1: 8-NaN.
Little, Eric G., and Galina L. Rogova. 2006. "An Ontological Analysis of Threat and Vulnerability." *2006 9th International Conference on Information Fusion*, 1–8. https://doi.org/10.1109/ICIF.2006.301716.
Loik, Ramon. 2013. "Security Integration in Europe: How Knowledge-Based Networks Are Transforming the European Union, by M.K. Davis Cross (Ann Arbor, MI: University of Michigan Press, 2012, ISBN 9780472117895); Xviii+281pp., £55.95 Hb." *JCMS: Journal of Common Market Studies* 51 (3): 576–77. https://doi.org/10.1111/jcms.12016_5.
Manjikian, Mary. 2013. "Positivism, Post-Positivism, and Intelligence Analysis." *International Journal of Intelligence and CounterIntelligence* 26 (3): 563–82. https://doi.org/10.1080/08850607.2013.758002.
Marrin, Stephen. 2012a. *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice*. Routledge.
———. 2012b. "Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful." *Intelligence and National Security* 27 (3): 398–422. https://doi.org/10.1080/02684527.2012.668082.
———. 2012c. "Is Intelligence Analysis an Art or a Science?" *International Journal of Intelligence and CounterIntelligence* 25 (3): 529–45. https://doi.org/10.1080/08850607.2012.678690.
Marrin, Stephen, and Jonathan D. Clemente. 2005. "Improving Intelligence Analysis by Looking to the Medical Profession." *International Journal of Intelligence and CounterIntelligence* 18 (4): 707–29. https://doi.org/10.1080/08850600590945434.
Marrin, Stephen, and Efren Torres. 2017. "Improving How to Think in Intelligence Analysis and Medicine." *Intelligence and National Security* 32 (5): 649–62. https://doi.org/10.1080/02684527.2017.1311472.
Martin, Kirsty. 2011. "The Paradox of Intuitive Analysis and the Implications for Professionalism." ResearchGate. 2011. https://www.researchgate.net/publication/258839553_The_Paradox_of_Intuitive_Analysis_and_the_Implications_for_Professionalism.
Matschulat, Austin B. 2007. "Coordination and Cooperation in Counterintelligence — Central Intelligence Agency." 2007. https://web.archive.org/web/20071010091345/https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v13i2a05p_0001.htm.
McChrystal, General Stanley. 2014. *My Share of the Task: A Memoir*. Reprint edition. New York, NY: Portfolio.
McConnell, Mike. 2007. "Overhauling Intelligence." 2007. https://www.researchgate.net/publication/293761677_Overhauling_intelligence.

McGonagle, John J., and Carolyn M. Vella. 2003. *The Manager's Guide to Competitive Intelligence*. Greenwood Publishing Group.
Miscik, Jami. 2017. "Intelligence and the Presidency How to Get It Right." ResearchGate. 2017. https://www.researchgate.net/publication/319978753_Intelligence_and_the_presidency_how_to_get_it_right.
Moore, David T., and National Defense Intelligence College. 2010. *Critical Thinking and Intelligence Analysis*. Books Express Publishing.
Morgan, Richard O. 2012. "Latif v. Obama: The Epistemology of Intelligence Information and Legal Evidence." https://gould.usc.edu/why/students/orgs/ilj/assets/docs/7%20-%20Morgan%20V2.pdf.
Morin, Jean-Frederic, and Selim Louafi. 2017. "Boundary Organizations in Regime Complexes: A Social Network Profile of IPBES." ResearchGate. 2017. https://www.researchgate.net/publication/320657829_Boundary_Organizations_in_Regime_Complexes_A_Social_Network_Profile_of_IPBES.
Mudd, Philip, and Greg Abbey. 2015. *The HEAD Game: High-Efficiency Analytic Decision Making and the Art of Solving Complex Problems Quickly*. Unabridged edition. Audible Studios on Brilliance Audio.
Nagy, John A. 2016. *George Washington's Secret Spy War: The Making of America's First Spymaster*. St. Martin's Press.
NATO. 2018. "AAP-6 - NATO Glossary of Terms and Definitions." https://apps.dtic.mil/dtic/tr/fulltext/u2/a574310.pdf.
Office of the Director of National Intelligence. 2005. "National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation." https://www.dni.gov/files/documents/CHCO/nis.pdf.
O'Malley, Pat. 2016. "'Policing the Risk Society' in the 21st Century." SSRN Scholarly Paper ID 2729631. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2729631.
Omand, David. 2009. "TheNationalSecurityStrategy: Implications for the UK Intelligence Community." https://warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/national_security_strategy1.pdf.
———. 2011. *Securing the State*. UK ed. edition. London: C Hurst & Co Publishers Ltd.
Ormerod, Owen. 2018. "Advancing the Epistemology of Intelligence Analysis: A Polanyian Perspective." ResearchGate. 2018. https://www.researchgate.net/publication/328232543_Advancing_the_epistemology_of_intelligence_analysis_A_Polanyian_perspective.
Palmer, Bill. 1991. *Strategic Intelligence for Law Enforcement*. Canberra: Australian Bureau of Criminal Intelligence.
Persico, Joseph E. 2002. *Roosevelt's Secret War: FDR and World War II Espionage*. Random House.
Peters, Adrienne M. F., and Irwin M. Cohen. 2017. "The Mandate and Activities of a Specialized Crime Reduction Policing Unit in Canada." *Police Practice and Research* 18 (6): 570–83. https://doi.org/10.1080/15614263.2017.1363970.
Pherson, Randolph. 2013. "The Five Habits of the Master Thinker." *Journal of Strategic Security* 6 (3). http://dx.doi.org/10.5038/1944-0472.6.3.5.
Platt, Washington. 1957. *Strategic Intelligence Production: Basic Principles*. F.A. Praeger.

Polanyi, Michael. 1962. *Personal Knowledge: Towards a Post-Critical Philosophy*. https://www.press.uchicago.edu/ucp/books/book/chicago/P/bo19722848.html.
———. 1964. *Science, Faith and Society*. Later Printing edition. Chicago: University of Chicago Press.
———. 1969. *Knowing and Being*. Edited by Marjorie Grene. 1st Edition edition. Chicago: University of Chicago Press.
———. 1998. *The Logic Of Liberty*. First Edition. Indianapolis: Liberty Fund Inc.
Polanyi, Michael, and Amartya Sen. 2009. *The Tacit Dimension*. Reissue edition. Chicago ; London: University of Chicago Press.
Pope, Simon, and Audun Jøsang. 2005. "Analysis of Competing Hypotheses Using Subjective Logic (ACH-SL)." https://apps.dtic.mil/dtic/tr/fulltext/u2/a463908.pdf.
Popper, Karl R. 1972. *Objective Knowledge: An Evolutionary Approach*. Revised edition. Oxford Eng. : New York: Oxford University Press.
Prescott, John E. 2012. "The Evolution of Competitive Intelligence." *Revista Inteligência Competitiva* 2 (2). https://doi.org/10.24883/ric.v2i2.45.
Pritchard, Matthew C., and Michael S. Goodman. 2009. "Intelligence: The Loss of Innocence." *International Journal of Intelligence and CounterIntelligence* 22 (1): 147–64. https://doi.org/10.1080/08850600802487018.
Quiggin, Thomas A. 2007. *Seeing The Invisible: National Security Intelligence In An Uncertain Age*. Hackensack, NJ: Wspc/Others.
Radaelli, Claudio M. 1999. "The Public Policy of the European Union: Whither Politics of Expertise?" *Journal of European Public Policy* 6 (5): 757–74. https://doi.org/10.1080/135017699343360.
Radner, Roy. 1972. "Normative Theory of Individual Decision: An Introduction." http://pages.stern.nyu.edu/~rradner/.
Rafii, Farshad, and Paul J. Kampas. 2002. "How to Identify Your Enemies Before They Destroy You." *Harvard Business Review*, 2002. https://hbr.org/2002/11/how-to-identify-your-enemies-before-they-destroy-you.
Ratcliffe, Jerry H. 2008. *Intelligence-Led Policing*. 1 edition. Cullompton, Devon: Willan.
Richelson, Jeffrey. 1988. *Foreign Intelligence Organizations*. Ballinger Publishing Company.
Robertson, K. G. 1987. "Intelligence Requirements for the 1980s." *Intelligence and National Security* 2 (4): 157–67. https://doi.org/10.1080/02684528708431921.
Robertson, Ken. 1996. "Intelligence, Terrorism and Civil Liberties." https://journals.lib.unb.ca/index.php/JCS/article/viewFile/14756/15825.
Rønn, Kira Vrist, and Simon Høffding. 2013. "The Epistemic Status of Intelligence: An Epistemological Contribution to the Understanding of Intelligence." 2013. https://www.researchgate.net/publication/263573379_The_Epistemic_Status_of_Intelligence_An_Epistemological_Contribution_to_the_Understanding_of_Intelligence.
Rudd, Kevin. 2008. "The First National Security Statement to the Australian Parliament, Address by the Prime Minister of Australia." https://dfat.gov.au/people-to-people/public-diplomacy/programs-activities/Pages/speech-by-prime-minister-kevin-rudd-to-the-parliament.aspx.
Salmen, David, Tatiana Malyuta, Alan Hansen, Shaun Cronen, and Barry Smith. 2011. "Integration of Intelligence Data through Semantic Enhancement." In *STIDS*.
Samuelson, Paul Anthony, and William D. Nordhaus. 1992. *Economics*. McGraw-Hill.

SCIP. 2014. "Code of Ethics - Strategic and Competitive Intelligence Professionals (SCIP)." 2014. https://www.scip.org/page/CodeofEthics.
Scott, Len, and Peter Jackson. 2004. "The Study of Intelligence in Theory and Practice." *Intelligence and National Security* 19 (2): 139–69. https://doi.org/10.1080/0268452042000302930.
Sebenius, James K. 1992. "Challenging Conventional Explanations of International Cooperation: Negotiation Analysis and the Case of Epistemic Communities." *International Organization* 46 (1): 323–65. https://doi.org/10.1017/S0020818300001521.
Sfetcu, Nicolae. 2016. *Cunoaştere şi Informaţii*. Nicolae Sfetcu.
Shaikh Muhammad, Akram, and Wang Jiaxin. 2006. "Investigative Data Mining: Connecting the Dots to Disconnect Them." Intelligence Tools Workshop. http://www.huitfeldt.com/repository/ITW06.pdf.
Shelley, Louise I. 1990. "Policing Soviet Society: The Evolution of State Control." *Law & Social Inquiry* 15 (3): 479–520. https://www.jstor.org/stable/828493.
Shoham, Dany, and Michael Liebig. 2016. "The Intelligence Dimension of Kautilyan Statecraft and Its Implications for the Present." *Journal of Intelligence History* 15 (2): 119–38. https://doi.org/10.1080/16161262.2015.1116330.
Shrager, Jeff, Dorrit Billman, Gregorio Convertino, J. P. Massar, and Peter Pirolli. 2010. "Soccer Science and the Bayes Community: Exploring the Cognitive Implications of Modern Scientific Communication." *Topics in Cognitive Science* 2 (1): 53–72. https://doi.org/10.1111/j.1756-8765.2009.01049.x.
Shulsky, Abram N., and Gary James Schmitt. 2002. *Silent Warfare: Understanding the World of Intelligence*. Potomac Books, Inc.
Silver, Mark S., M. Lynne Markus, and Cynthia Mathis Beath. 1995. "The Information Technology Interactive Model: A Foundation for the MBA Core Course." 1995. https://misq.org/catalog/product/view/id/668.
Singer, J. David. 1958. "Threat-Perception and the Armament-Tension Dilemma." *The Journal of Conflict Resolution* 2 (1): 90–105. https://www.jstor.org/stable/172848.
Smith, Barry. 1996. "Mereotopology: A Theory of Parts and Boundaries - ScienceDirect." 1996. https://www.sciencedirect.com/science/article/pii/S0169023X96000158.
———. 2012. "Ontology for the Intelligence Analyst." 2012. https://philarchive.org.
Smith, Barry, Lowell Vizenor, and James Schoening. 2009. "Universal Core Semantic Layer." In .
Smith, Michael Douglas. 2017. "A Good Intelligence Analyst." *International Journal of Intelligence and CounterIntelligence* 30 (1): 181–85. https://doi.org/10.1080/08850607.2016.1230708.
Soustelle, Jacques. 2002. *Daily Life of the Aztecs*. Courier Corporation.
Stewart, Thomas A. 2001. *The Wealth of Knowledge: Intellectual Capital and the Twenty-First Century Organization*. New York, NY, USA: Doubleday.
Treverton, Gregory F. 2011. *Intelligence for an Age of Terror*. Reprint edition. Cambridge ; New York: Cambridge University Press.
US Department of the Army. 1981. "Executive Order 12333. (1981, December 4). United States Intelligence Activities, Section 3.4(a). EO Provisions Found in 46 FR 59941, 3 CFR." https://fas.org/irp/doddir/army/fm34-60/.
———. 1995. "Field Manual 34-60: Counterintelligence." https://fas.org/irp/doddir/army/fm34-60/.

US Government. 2009. “A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis.” https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf.
Vandepeer, Charles. 2011. “Rethinking Threat: Intelligence Analysis, Intentions, Capabilities, and the Challenge of Non-State Actors.” Thesis. https://digital.library.adelaide.edu.au/dspace/handle/2440/70732.
———. 2014. “Applied Thinking for Intelligence Analysis : A Guide for Practitioners.” 2014. //www.awm.gov.au/index.php/collection/LIB100045502.
Volkswagen Foundation. 2002. “Basic Formal Ontology.” http://basic-formal-ontology.org/.
Walsh, Patrick F. 2010. *Intelligence and Intelligence Analysis*. 1 edition. New York, NY: Willan.
Waltz, Edward. 2003. *Knowledge Management in the Intelligence Enterprise*. Artech House.
———. 2014. *Quantitative Intelligence Analysis: Applied Analytic Models, Simulations, and Games*. Lanham, Maryland: Rowman & Littlefield Publishers.
Weick, Karl E. 1995. *Sensemaking in Organizations*. SAGE.
Weiner, Tim. 2007. “Pssst: Some Hope for Spycraft.” *The New York Times*, 2007, sec. Week in Review. https://www.nytimes.com/2007/12/09/weekinreview/09weiner.html.
Wheaton, Kristan J., and Michael T. Beerbower. 2006. “Towards a New Definition of Intelligence.” Stanford Law School. 2006. https://law.stanford.edu/publications/towards-new-definition-intelligence/.
Wheaton, Kristan J., and Diane E. Chido. 2007. “Structured Analysis of Competing Hypotheses: Improving a Tested Intelligence Methodology.” 2007. https://web.archive.org/web/20070928154654/http://www.mcmanis-monsalve.com/assets/publications/intelligence-methodology-1-07-chido.pdf.
Wheeler, Douglas L. 2012. “A Guide to the History of Intelligence 1800–1918.” https://www.afio.com/publications/Wheeler_Hist_of_Intel_1800-1918_in_AFIO_INTEL_WinterSprg2012.pdf.
Wimalasuriya, Daya C., and Dejing Dou Dejing Dou. 2010. “(PDF) Ontology-Based Information Extraction: An Introduction and a Survey of Current Approaches.” ResearchGate. 2010. https://www.researchgate.net/publication/220195792_Ontology-based_information_extraction_An_Introduction_and_a_survey_of_current_approaches.
Wolfberg, Adrian. 2006. “Full-Spectrum Analysis: A New Way of Thinking for a New World.” Military Review, July-August 2006. http://cgsc.cdmhost.com/cdm/ref/collection/p124201coll1/id/414.
Woolsey, James. 1998. “Testimony, 12 February 1998, US House of Representatives Committee on National Security.” https://fas.org/irp/congress/1998_hr/h980212w.htm.
Ylikoski, Petri. 2017. “The Illusion of Depth of Understanding in Science.” https://doi.org/10.31235/osf.io/qz7sg.
Yuen, Derek M. C. 2014. *Deciphering Sun Tzu: How to Read “The Art of War.”* Oxford University Press.
Zheng, Jack. 2014. “Information System a System View.” Technology. https://www.slideshare.net/jgzheng/information-system-a-system-view.