# National Security Intelligence and Business Intelligence: A Comparative Analysis

**Constantin BRATIANU**[1]
**Nicolae Alexandru BUDEANU**[2]

***Abstract***

*Being one of the most important assets in governmental organizations and private companies, intelligence became a subject of interest for both researchers and practitioners in the last decades. In the literature, the concept of "intelligence" has got many meanings and interpretations, like psychological intelligence, emotional intelligence, spiritual intelligence, social intelligence, organizational intelligence, business intelligence, competitive intelligence, and national security intelligence. The core meaning of all these different specialized concepts remains the same: the capacity of processing data, information, and knowledge. Their differences come from the context in which these processes operates and the mission of the organizational structures which perform these specific processes. Business intelligence and competitive intelligence are characteristics of private companies, while national security intelligence is characteristic for the state-owned institutions. This paper aims to present a comparative analysis between business intelligence and national security intelligence based on a critical literature review and adopting a knowledge management perspective. The value of the present paper comes from the semantic tool used in our comparative analysis and the perspective of knowledge management adopted.*

**Keywords:** *national security intelligence, competitive intelligence, business intelligence, knowledge management, intelligence structures.*

**JEL classification:** D83, H83, H56, L32, L33
**DOI:** 10.24818/RMCI.2023.2.188

## 1. Introduction

The concept of *intelligence* is as old as the human beings history. It evolved semantically with the societal development and its challenges, but in its essence, intelligence is "the ability to learn, understand, and make judgments" (Cambridge Dictionary). For a very long time intelligence was conceived as a unique characteristic of the brain power and measured by using the Intelligence Quotient (IQ) framework developed by psychologists (Das, 2002; Sternberg, 1996; Sternberg & Wagner, 1986).

[1] Constantin Bratianu, Bucharest University of Economic Studies, Romania, constantin.bratianu@gmail.com
[2] Nicolae Alexandru Budeanu, National University of Political Studies and Public Administration, Bucharest, Romania, budeanu.alexandru6@gmail.com

Gardner (2006) came with the new paradigm of conceiving a *multiple intelligences* model: "I define an *intelligence* as a biopsychological potential to process specific forms of information in certain kinds and ways. Human beings have evolved diverse information-processing capacities – I term these "intelligences" – that allow them to solve problems or to fashion products. To be considered "intelligent", these products and solutions must be valued in at least one culture or community" (Gardner, 2006, p. 29). The processing power of intelligence is important in predicting further actions and events. "Intelligence is measured by the capacity to remember and predict patterns in the world, including language, mathematics, physical properties of objects, and social situations" (Hawkins & Blakeslee, 2004, p. 97).

Intelligence processes data, information, and knowledge to find solutions for the problems formulated at individual level, organizational level or national level. Thus, intelligence is much more than knowledge, but it depends on knowledge (Kent, 1949; Spender, 1996). At the organizational level experts developed business intelligence in order to acquire the necessary knowledge and understanding for decision making to achieve competitive advantage (Bratianu & Lefter, 2001; Bratianu et al., 2021; Grant, 1996; Nonaka, 1994; Nonaka & Toyama, 2003; Porter, 1985; Zack, 1999). Therefore, it can be considered and widely accepted that intelligence is a driving force for achieving competitive advantage in a certain field (Alnoukaria & Hanano, 2017; Fleisher & Blenkhorn, 2001; Ivan, 2016; Jourdan et al., 2008; McGonagle, 2016; Rajnoha et al., 2016; Søilena, 2017), either at business or national security level.

In this fast-changing world, dominated by uncertainty and turbulence (as the COVID-19 pandemic and the Ukrainian War demonstrated), intelligence and knowledge represent the most important assets of an organization, that can help it overcome all types of threats from the external environment. However, there is a significant gap in the literature between discussing about intelligence at individual (i.e. psychological intelligence) and organizational levels (i.e. business intelligence), and that at national security level (i.e. national security intelligence).

The purpose of this paper is to analyze the main features of business intelligence and to compare it with the national security intelligence, based on a critical literature review. The structure of the paper is the following: a brief introduction, literature review, methodology, results and discussions, and conclusions.

## 2. Literature review

Citing from the Romanian law, national security is "the state of legality, equilibrium and social, political and economic stability required by the existence and development of the national Romanian state as an sovereign, unitary, independent and indivisible state, maintaining the legal order and the climate of unrestricted exercise of fundamental rights, freedoms and duties of citizens,

according to the democratic principles and rules established by the constitution" (article 1, Law 51/1991 regarding Romania's national security).

Kent (1949, p. XXI) defined intelligence "as the knowledge which our highly placed civilians and military men must have to safeguard the national welfare". He also stated that intelligence is "vital for national survival" (Kent, 1949, p. XXI). The triad proposed by Kent was: intelligence is knowledge, intelligence is organization and intelligence is activity, looking at intelligence as what we get of it, what institutions create it and what missions are conducted in order to achieve it (Kent, 1949).

In a report prepared for the United Kingdom's Security Sector Development Advisory Team, intelligence was defined as "a special kind of knowledge, a specialized subset of information that has been put through a systematic analytical process in order to support a state's decision and policy makers. It exists because some states or actors seek to hide information from other states or actors, who in turn seek to discover hidden information by secret or covert means." (Hannah et al., 2005, p. III). Johnson (2010, p. 5) has stated that "the main purpose of intelligence is to provide information to policy□makers that may help illuminate their decision options". In his work, he has also redefined the knowledge-organization-activity triad proposed by Kent (1949), stating that the four significances of national security intelligence are information, process, missions, and organizations (Johnson, 2010).

In the current state of literature, there is confusion between *business intelligence* and *competitive intelligence* (Ivan, 2016). As McGonagle (2016, p. 371) has stated, "business intelligence is an older term for competitive intelligence", but without being the same thing, as competitive intelligence is focused on external environment, while business intelligence is focused on internal environment (Alnoukaria & Hanano, 2017). From a critical thinking point of view, business intelligence and competitive intelligence represent the same domain of activity. The only difference comes from the new perspective introduced by Porter (1985) of competitive advantage as a basic requirement for business success. Thus, we should look more for the similarities than for differences between these two concepts and the associated theories.

According to Fleisher (2001, p.4), "competitive intelligence is the process by which organizations gather actionable information about competitors and the competitive environment and, ideally, apply it to their decision-making and planning processes in order to improve their performance." Also, McGonagle (2016, p. 371) has stated that competitive intelligence is "actionable intelligence, on the entire competitive environment, which includes an enterprise's competitors, suppliers, customers, and potential competitors, as well as its regulatory and political environment." Achieving competitive intelligence requires a high level of organizational intellectual capital and knowledge entropy (Bratianu, 2007, 2019).

Alnoukaria & Hanano (2017, p.9) have given another useful definition of competitive intelligence as "the analytical process of collecting, selecting, and interpreting all the information related to business competitors in order to emphasis

their positions, capabilities, performances and results and in the market." Competitive intelligence is oriented to identifying competitors' opportunities and external threats (Alnoukaria & Hanano, 2017) as well as competitors' strengths and weaknesses (Botos & Radu, 2017; Bratianu, 2002), obeying national laws and business ethics.

Another confusion could be made by both practitioners and researchers, considering competitive intelligence as business espionage, which is illegal. (Fleisher & Blenkhorn, 2001; Ivan, 2016; McGonagle, 2016). Competitive intelligence is ethical, legal, and legitimate, and is using public information obtained in legal manners from open sources (Fleisher & Blenkhorn, 2001; Ivan, 2016). Therefore, competitive intelligence is oriented outside the boundaries of the organizations, aiming at gathering data that can be analyzed and transformed in information required for gaining competitive advantage in a certain field. The generic areas for competitive intelligence are industry attractiveness, market development, customer segmentation, consumer behavior and competitor comparison (Alnoukaria & Hanano, 2017).

Some possible sources of data for competitive intelligence are analyst reports, speeches, interviews, articles, biographies, press releases, resumes, annual reports, investment reports, websites, financial statements, regulatory filings, investment reports, alliance announcements, customers, political reviews, industry handbooks or patent filings (Fleisher & Blenkhorn, 2001). According to Ivan (2016, p. 138), business intelligence "is more an 'internal affair', in a way that it concerns interdepartmental activities, the analysis of material and informational flows and the modalities to improve the activity." Alnoukaria & Hanano (2017, p.7) have stated that business intelligence "can be considered as one of the most important technologies that allows managers and end users to convert masses of non-transparent data into useful information that provide companies with huge capabilities." Also, Skyrius (2021, p.10) has given the following definition: "business intelligence may be defined as the organizational practice that encompasses a coherent set of people, informing processes and conventions of using a comprehensive technology platform to satisfy business information needs that range from medium to high complexity."

Therefore, being internal-focused, business intelligence represents the activities of collecting, processing and analyzing of data about the performance of the organization and dissemination of information needed by the strategic management. Business intelligence is mainly based on data mining, process analysis, performance benchmarking and descriptive analytics (Botos & Radu, 2017) and is oriented on market position, value chain, cost structure, core competences and specific assets beneath the organization (Alnoukaria & Hanano, 2017). The technologies used in the processes specific to business intelligence are mainly analytic tools, and the information created through these activities support the decision-making process and is useful for strategic management in order to formulate the company strategies and objectives.

Therefore, going from the statement formulated by Søilen (2017, p. 34), respectively ”a private organization today with a small intelligence department can gather more data than what the state could do only a decade ago”, we can say that it is rather a necessity than an option for private organizations to develop competitive intelligence and business capabilities, in order to obtain a better view of the internal and external environment and identify the possible opportunities, on one hand, and risks, threats and vulnerabilities, on the other hand.

## 3. Methodology

The research is based on semantic analysis of the main concepts and ideas concerning intelligence at the organizational and national security levels, and on a critical review of the current literature. In the semantic analysis we used the philosophy of grounded theory (Corbin & Strauss, 2015).

Also, the research model integrated both authors' experience in these fields of business intelligence and national security intelligence. The present paper is conceptual and comes with a new perspective offered by the knowledge management to compare the role of intelligence structures used in companies for achieving competitive advantage and in national security systems for applying the governmental strategies in creating a synergy between internal and external forces converging toward national security.

## 4. Results and discussions

The semantic analysis shows that regardless of numerous definitions formulated for both national security and business competitive advantage, the core meanings are the same: data, information and knowledge on one part and the processing power of them as a basis for decision making, on the other part. The following discussions come to focus on some more details of that interpretation showing that differences appear when authors use different perspective of analysis.

MacGaffin & Oleson (2016, p. 4) have shown that “if significant intelligence is available in support of decision making, it can provide a decision advantage so the decision-maker is better informed and understands more aspects of an issue in ways that would not be possible without the intelligence.” Also, Pili (2018, p. 398) has stated that “the intelligence cycle is an entire epistemic activity based on gathering data and information, collecting them in order to analyze them to deliver a report whose goal is to enhance the rationality of a decision maker”.

Based on these definitions we can conclude that national security intelligence represents the capacity to properly process data, information and knowledge by the decision makers of a country in order to take adequate actions for ensuring the national security, as it is defined by the law.

The national security intelligence is obtained by collecting raw data, information and knowledge, processing and analyzing it and, afterwards, disseminating the results to the legal beneficiary. These intelligence activities are

conducted by specialized entities named *intelligence structures*, according to the strategies formulated at government level. Also, the activity of the intelligence structures is regulated by laws and is controlled by state entities (such as government or parliament). Thus, their mission is given by law.

The activity of any intelligence structure is classified and is formed by sources and methods. Wirtz (2010, p.59) have offered some examples of intelligence sources, such as "information gleaned from espionage, images obtained by earth-orbiting satellites, intercepted communications, to publicly available media reporting", and intelligence methods, like "avoiding detection and surveillance, maintaining secret communications, and the fine art of recruiting and "running" clandestine agents" and "various social-science methodologies, computer-based analytic tools, or the use of collaborative work□spaces that exploit emerging information-revolution technologies".

It is also well known that intelligence structures give special importance to the protection of sources and methods secrecy, in order to not give their opponents (either state or non-state entities) information of their strategies, capabilities or areas of interest. Based on how data and information is collected, intelligence is classified as follows: HUMINT - human source intelligence; SIGINT - signals intelligence; IMINT - imagery intelligence; OSINT - open source; MASINT - measurement and signatures intelligence (Oleson, 2016).

Even if both intelligence structures and private companies use the generic model for intelligence, respectively planning, gathering, processing, analyzing and dissemination (Ivan, 2016), the first and main difference in managing national security intelligence and business intelligence comes from the methods and sources of information they use. As we described earlier, national security intelligence use classified and secret methods and sources of information, while business intelligence use open source and internal data. Therefore, managing the entities that work with national security intelligence, respectively intelligence structures, requires the compliance of a different type of legislation and procedures as in the case of managing entities from the business intelligence.

Firstly, the legislation designated for the national security intelligence and for the protection of classified information provides greater penalties (including prison) for breaking its stipulations than the internal regulations and contractual amendments used by private entities for confidential information disclosure. The impact for disclosing national security intelligence is far more greater than disclosing confidential business intelligence. Secondly, the risks to which are subject the intelligence structures employees in their activity, especially in the case of HUMINT, are greater than the risks associated with the activities specific to competitive/business intelligence, which are in most part associated with OSINT.

Then, the difference of subjects between national security intelligence and business intelligence must be discussed. While national security intelligence targets the identification of all types of threats, risks and vulnerabilities towards the state, business intelligence have the purpose to add value to a company.

From this result the differences in the analytic activities conducted in the intelligence structures and private organizations. Even if both intelligence structures and private entities use both quantitative and qualitative analysis as a tool to add value to information in order to be useful to the decision maker (Ivan, 2016), the analysis processes are different. Therefore, in intelligence structures, analysis includes cognitive methods and hypotheses testing, while in the business area, analysis is used mainly for processing and shaping data for obtaining evaluations (Barbu & Rat, 2017).

Another differentiator for management perspective between national security intelligence and business intelligence comes from the planning perspective. While for intelligence structures, the organization, mission, functions, and strategies are defined by the policy-maker, respectively at governmental level, (Oleson & Cothron, 2016; Pili, 2018), in private companies the goals, plans and strategies are defined by the managerial team. Thus, political changes within a country affect the activity of an intelligence structure in a greater way than the activity from a private company, with repercussions on management activity.

From this come the differences between the specific beneficiaries of intelligence. While in the business area, the main beneficiary of the competitive/business intelligence is part of the same organization, the beneficiaries of national security intelligence are all outside the intelligence structure. Having this in mind, there are two main differences in managerial vision: the cost of the intelligence and the relationship the beneficiary and the intelligence creator. The fact that the consumers of the national security intelligence don't have to pay directly for it generates a greater demand for intelligence than the actual possibilities (Oleson & Cothron, 2016). In the same context, the beneficiary of business intelligence will always pay attention to the actual costs of the specific activities. The relationship with beneficiaries in the business intelligence area takes place in the same organization, while the national security intelligence always leaves the organization. Mocanu (2015, 170) has stated that "the interaction between the intelligence structure and the decision□making system is done through two points of the intelligence cycle, one for the transfer of the intelligence requests and that of the beneficiary feed-back, and the other for dissemination – the completion of intelligence support." Therefore, the managers of the intelligence structure need to always be in a relationship with the beneficiaries from outside the organization.

Another difference between national security intelligence and business intelligence, from the managerial point of view, comes in the measurement field. While business intelligence contribute to the performance of a company, and, therefore, its success could be assimilated to profit, in national security field intelligence could be hardly measured. In this case, there are some possible indicators that could help the measurement of national security intelligence, such as the strategic value of the products, the focus on collaborative activities, the early warning capabilities (Posaştiuc, 2011).

The organizational culture in intelligence structures is also very different to organizational cultures from organizations in the business environment. In intelligence structures there was developed a "strong organizational culture, quality-oriented, involving the existence of values, beliefs, perceptions and representations based on this principle" (Popescu, 2011, p.24). In the business environment, we can find different organizational cultures, such as collaborative culture, creative culture or customer-first culture, but mainly all different to the ones developed in intelligence structures. The main differences between national security intelligence and business intelligence emphasized above are synthesized in Table 1.

**Table 1. The differences between national security intelligence and business intelligence**

| Field | Differences | |
|---|---|---|
| | **National security intelligence** | **Competitive/business intelligence** |
| **Methods and sources** | Classified and secret | Open source |
| **Legal framework** | National security and classified information legislation | Internal regulations and contractual amendments |
| **Analysis** | Cognitive methods and hypotheses testing | Processing and shaping data for obtaining evaluations |
| **Planning** | Policy-maker/ governmental level | Managerial team |
| **Cost** | No direct cost for beneficiaries | Direct cost for beneficiaries |
| **Beneficiaries** | Outside the organization | Inside the organization |
| **Measurement** | Cannot be quantified | Could be assimilated to profit and measured |
| **Organizational culture** | Quality-oriented | All types of organizational culture |

## 5. Conclusions

The purpose of this article was to identify the main differences between national security intelligence and business intelligence, by analyzing the literature from these domains and by comparing their semantic domains and the specific environment they are operationalized.

Even if national security intelligence and business intelligence have a common ground, these fields are completely different in terms of methods, sources and objectives. Nevertheless, the challenges faced by the managers from the intelligence structures are totally different from the ones faced by managers from business environment. The mission of national security intelligence structures is given by law, while the mission of business intelligence structures is established by each company in concordance with its vision and strategies. Therefore, managing

these intelligence structures may have specific requirements which should be known by the knowledge managers responsible for the whole activity.

The contribution of this article comes from the fact that it sets the ground for researching further differences between national security intelligence and business intelligence, from a managerial point of view. The present study bridge the gap between intelligence structures used in the national security system and those used in business intelligence activities by private companies in order to achieve competitive advantage.

The main limitation of this research comes from the limited sources found in literature analyzing the role and specific activities of the national security intelligence structures.

## References


1. Alnoukaria, M. & Hanano, A. (2017). Integration of business intelligence with corporate strategic management. *Journal of Intelligence Studies in Business*, 7 (2), 5-16.
2. Barbu, A. & Rat, T. (2017). Big data analysis through the lens of business intelligence – world conflict incidents case study (1989-2016). *Romanian Intelligence Studies Review*, 17-18, 157-164.
3. Botos, H.M. & Radu, G. (2017). Business counterintelligence practices. *Romanian Intelligence Studies Review*, 17-18, 165-175.
4. Bratianu, C. (2002). *Management strategic*. Craiova: Editura Universitaria Craiova.
5. Bratianu, C. (2007). An integrated perspective on the organizational intellectual capital. *Review of Management and Economical Engineering*, 6(5), 107-112.
6. Bratianu, C. (2019). Exploring knowledge entropy in organizations. *Management Dynamics in the Knowledge Economy*, 7(3), 353-366.
7. Bratianu, C. & Lefter, V. (2011). *Management strategic universitar*. Bucharest: RAO.
8. Bratianu, C., Vătămănescu, E.M., Anagnoste, S. & Dominici, G. (2021). Untangling knowledge fields and knowledge dynamics within the decision-making process. *Management Decision,* 59 (2), 306-323.
9. Corbin, J. & Strauss, A. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory.* Fourth Edition. Los Angeles: SAGE.
10. Das, J.P. (2002). A better look at intelligence. *Current Directions in Psychological Science*, 11(1), 28-33.
11. Fleisher, C.S. & Blenkhorn, D.L. (2001). *Managing frontiers in competitive intelligence*. New York: Quorum Books.
12. Gardner, H. (2006). *Changing minds: The art and science of changing our own and other people's minds*. Boston: Harvard Business School Press.
13. Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal*, 17(S2), 109-122.
14. Hannah, G., O'Brien, K.A. & Rathmell, A. (2005). *Intelligence and security legislation for security sector reform*. RAND Corporation.
15. Hawkins, J. & Blakeslee, S. (2004). On intelligence. New York: Times Books.
16. Ivan, L. (2016). Characteristics of information analysis in/for business environment. *Romanian Intelligence Studies Review*, 15, 133-142.

17. Johnson, L.K. (2010). National Security Intelligence. *The Oxford handbook of national security intelligence.* Oxford: Oxford University Press, pp. 3-33.
18. Jourdan, Z., Rainer, R.K. & Marshall, T.E. (2008). Business intelligence: An analysis of the literature. *Information Systems Management*, 25 (2), 121-131.
19. Kent, S. (1949). *Strategic intelligence for American world policy.* Princeton: Princeton University Press.
20. MacGaffin, J. & Oleson, P. (2016). Decision advantage, decision confidence: The why of intelligence. *AFIO's Guide to the Study of Intelligence, Association of Former Intelligence Officers,* 3-12.
21. McGonagle, J. (2016). Competitive intelligence. *AFIO's Guide to the Study of Intelligence, Association of Former Intelligence Officers,* 371-381.
22. Mocanu, M. (2015). Intelligence cycle model dilemmas and solutions. *Romanian Intelligence Studies Review*, 14, 165-178.
23. Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, 5(1), 14-37.
24. Nonaka, I. & Toyama, R. (2003). The knowledge-creating theory revisited: Knowledge creation as a synthetizing process. *Knowledge Management Research & Practice*, 1(1), 2-10.
25. Oleson, P. (2016). Getting started: Initial readings for instructors of intelligence. *AFIO's Guide to the Study of Intelligence, Association of Former Intelligence Officers,* 21-27.
26. Oleson, P. & Cothron, T. (2016). Leading and managing intelligence organizations. *American Intelligence Journal*, 33(1), 6-16.
27. Pili, G. (2018). Intelligence and social knowledge: A philosophical inquiring on the social epistemological nature of intelligence as a state institution. *Romanian Intelligence Studies Review*, 19-20, 397-418.
28. Popescu, A. (2011). Modern management in intelligence organizations. *Romanian Intelligence Studies Review*, 6, 24-35.
29. Porter, M. (1985). *Competitive advantage: Creating and sustaining superior performance*. New York: Free Press.
30. Posaştiuc, C. (2011). Reengineering intelligence. *Romanian Intelligence Studies Review*, 6, 5-13.
31. Rajnoha, R., Štefko, R., Merková, M. & Dobrovič, J. (2016). Business intelligence as a key information and knowledge tool for strategic business performance management. *E+M Ekonomie a Management*, 19 (1), 183-203.
32. Skyrius, R. (2021). *Business intelligence: A comprehensive approach to information needs. Technologies and culture*. Cham: Springer.
33. Søilen, K.S. (2017). Why care about competitive intelligence and market intelligence? The case of Ericsson and the Swedish Cellulose Company. *Journal of Intelligence Studies in Business*, 7 (2), 27-39.
34. Spender, J. C. (1996). Making knowledge the basis of a dynamic theory of the firm. *Strategic Management Journal*, 17, Special Issue, 45-62.
35. Sternberg, R.J. (1996). *Successful intelligence*. New York: Simon & Schuster.
36. Sternberg, R.J., & Wagner, R.K. (1986). *Practical intelligence: nature and origins of competence in the everyday world.* Cambridge: Cambridge University Press.
37. Wirtz, J. (2010). The sources and methods of intelligence studies. *The Oxford handbook of national security intelligence.* Oxford: Oxford University Press, pp. 59-70.
38. Zack, M. (1999). Developing a knowledge strategy. *California Management Review*, 41(3), 125-145.