The growing use of technology as a fundamental tool for knowledge management has obliged the business world to adapt to the information revolution era. Competitive intelligence is the new management tool companies are using for ensuring positive results both on the short and the long term. The following research paper starts by revealing the needs that companies respond to when implementing competitive intelligence and continues with a summary of the main techniques used by businesses to develop an intelligent market approach. The paper also offers a brief description of corporate espionage practices, underlining the differences between these and the competitive intelligence techniques. A case study showing the way that competitive intelligence is implemented in practice is being offered. Conclusions refer to the main differences between corporate espionage and competitive intelligence as well as the driving forces determining the need for acquiring knowledge on competitive intelligence.

Introduction

The cyber world became a serious source of threats for companies. In April this year, The Norwegian National Security Authority has issued a warning against increased attempts at industrial espionage through e-mails against Norwegian firms while the US think–tank SANS (SysAdmin, Audit, Network, Security) Institute has ranked cyber espionage as No. 3 on its "Top 10 Cyber Security Menaces for 2008" report. In the same time, the German authorities are currently investigating a complaint filed by the luxury car maker Porche SE on April 27, 2008 regarding an attempt to spy on the company’s CEO, Wendelin Wiedeking. The suspect is its second largest shareholder, Volkswagen. Porsche is locked in a battle over its desire to change the rules of the decision making process. Also in Germany, the discount supermarket chain Lidl has been accused of spying on its employees in March 2008.

These are not isolated examples. Corporate espionage started to be famous long ago on the business arena but it is only recently that fears have grown as the means to obtain business secrets have developed enormously with the technological progress. However, taking into account that the XXIth century is characterized by the existence of the knowledge based society, businesses worldwide have to adapt to this reality by creating development frameworks for getting the sufficient amount of information that allows a good market position and protecting against spying attempts from competitors. Keeping a balance in the activities related to these two very different purposes is a daily challenge for companies acting in today’s global environment.
Therefore, while the technological innovation sped up its pace and businesses worldwide started being more and more integrated a new management and marketing technique appeared – competitive intelligence (CI). It was practically born from the need of better understanding the business environment while taking strategic decisions. Intelligence has been however until recently more of a military term than a business one. “The Art of War” by Sun Tzu, considered the first book describing military intelligence practices is showing that managing conflict situations equals anticipating and adapting to the external change. In a military war, a good general will use his alertness, awareness and wisdom to benefit from any given situation. Even if he will try not to go to the battlefield – as he knows that would automatically lead to casualties – once there, his best strategy would lead to gaining strength through his competitors and not winning at their expense. He is fighting for ensuring the integrity and development of his state, gaining assets and access to resources. In other words, a general must first get to know the enemy and then the characteristics of the battle field.

In the business world this would be translated into the fact that a good manager has to know well the competitor and the market. Even if some would argue that this is the reason marketing department exists within companies, the last decades of the last century showed that marketing departments are not sufficient anymore as the world was transformed into a smaller place. During the ‘70s the strategic management concept appeared. The business leaders started to become aware of the need to know more about the competitors and the business environment. The decade that followed was marked by the publication of Michael Porter’s famous books “Competitive Strategy, Competitive Advantage”, “Porter on Competition” and “The Competitive Advantage of Nations”. Since then the Porter Five Forces Model has been used by the business community as a successful tool of strategic management. It was during the ‘80s that benchmarking started to be used in the US as a complementary marketing technique, creating the basis for what would become competitive intelligence (CI). The last decade of the XXth century is characterized by the end of the Cold War and the intensifying process of globalization. Technological process accelerated and formed the basis of a knowledge base society, determining the need for intelligence practices within the business world.

The word “intelligence” is given the following definition in the dictionary: “the ability to acquire and apply knowledge and skills”. The term competitive is associated with the “strong desire to be more successful than others”. Considering both definitions one can sum up an explanation for CI that would define the process through which you acquire and apply knowledge to become more successful than the others. CI should therefore give you insights on what will happen in the future, improving your skills and knowledge and make you better prepared than your competitor.

1 Competitive intelligence and the decision making process

Competitive intelligence is a vital tool to the decision making process. On average, management takes decisions based on 30-40% of the available information, in combination with intuitions. The complex environment of businesses is shaping three distinctive characteristics of the strategic decision-making process that underlines the need for CI: the process’ rationality: the high diversity of socio-economic problems nowadays is requiring good, scientific knowledge based on a clear, rational solving system; the information intensive economies: the high volume of printed, audio, video and internet news is requiring the intensive and efficient use of technology for data treatment so that it may be transformed into
usable resource and the decision’s goal: the clear defined purpose of the process needs to allow the evaluation of each and any contribution to its achievement.

The decision making process results into actions translating decisions into practice. The results are transferred into the business environment through “news” generators – the company PR department, journals focused on the industry, a.s.o. This is actually raw data that is produced and transformed, through business intelligence tools into information and then, through CI process into knowledge. The need for applying CI comes as a consequence of the complex information flow. The core drive of CI is therefore the news flow. However, there are other factors pressing the companies to develop CI capabilities that can be summarized simply into outside and inside factors. The outside factors may be synthesized by the interconnectivity of the socio-economic systems worldwide as well as by the technological progress. The inside factors are referring to internal management – that needs to transform the internal stream of data into accessible and useful information.

Decisions are based on certain assumptions. Over time, assumptions change. Competitive analysis is critical for formulating strategies that take into account the best forecasts. These are in fact assumptions that the analysts are creating, taking into account the company’s and the competitors’ performance levels and trends. Therefore, CI identifies areas of improvement, risks and opportunities while also isolating “best practices”, allowing the company to create and formulate strategies on knowledge and experience instead of crude, generic benchmarking data. It is concerned with creating the right perception on the marketplace and the company, checking the major forces impacting them.

Competitive intelligence is a logical process of testing, validating assumptions and solving critical business problems, therefore it is organized around certain specific steps that relate to the following actions: identifying the intelligence needs of the company, collecting information, analyzing and synthesizing collected information and disseminating results. Due to the short amount of time given, the sequence of the activities must be precisely followed. Besides the four steps that need to be undertaken on key issues and regard specific needs of the company, CI process requires a constant and continuing monitoring process that helps the company to know what the competition is doing and how the business environment changes.

First step ahead for an effective CI analysis requires a correct identification of the company’s intelligence needs. This translates into a good understanding of the industry the company activates in. Michael Porter’s Five Forces Model is used as the main analysis tool at this phase. Indirect forces that influence the business fall under a separate and very important category of factors that needs to be well described. While analyzing the industry characteristics and trends, CI must understand the company it serves. This particular goal is served by a wide range of techniques that use internal data from financial, marketing, human resources’ departments and external data collected through the monitoring process. Except Michael Porter’s Model, there are about nine other analytical models that need to be tested on the company before the information collection starts. A short overview of these is presented in the table bellow:

<table>
<thead>
<tr>
<th>Model</th>
<th>Brief description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Life Cycles</td>
<td>Indicates where the company stands within the product life cycle and tells if the CI should focus on the marketplace more (the company wants to introduce a new product on the market – market intelligence), the customers (the new product is on the market, early phase – customer intelligence) or the competitors</td>
</tr>
</tbody>
</table>
Competitive Intelligence has also developed its special tools for understanding the needs of the company. These combine business, social, psychological and technical knowledge. They create a dynamic profile of the company and the business environment it activates in. Among the most used special analytical techniques are:

- **Monitoring:** Helps focusing on most important factors as it may regard a market segment, competitors, developments within related industries or all; requires people with diverse backgrounds so that the basic understanding of issues is covered but it is also very useful for a continuous business

- **Psychological profiling:** Helps understanding the organizational unique culture by studying the processes and management, checking the ownership structure, decision making personalities

- **Reverse engineering:** Process of taking an existing product or service and breaking it into parts, sub-components in order to understand how it was built and create a model of the production process with the purpose of identifying critical features, develop alternatives or/and making the process more efficient

The second stage of the CI process is **information collection.** This stage is divided into two main phases: the first is taking the smallest amount of time possible to get the most of the published information while the second phase is taking the time needed to get the available
and pertinent information using a direct approach – interviewing sources. Time management is therefore the key for the effectiveness of this stage. For the first phase, the “technical” part of CI – business intelligence – brings in the Web 2.0 technologies that make the information flow instantly into the company’s warehouse. This is when raw data is transformed into information. Currently it is considered that there are three generations of business intelligence solutions: Host Based Query and Reporting – that could be used only by information providers, Data Warehousing – that is used both by information providers and consumers, but still mostly by the providers and Business Intelligence Systems that focus on improving the access and delivery of business information to both information providers and consumers. Using techniques as Data Mining, OLAP (On Line Analytical Processing) or GIS – Geographic Information System, business intelligence transforms data into useful information that, through analysis becomes knowledge.

However, even if technology helps a lot, the human capital is still essential for CI. There are persons that filter the information and sources and not computers. The second phase is even more intense in human capital as it involves the unique human touch, as it focuses on getting the pertinent information through interviews. The spirit of an intelligence directed interview is driven by the art of the negotiation and not by journalism. Soft, trustful questions come first while the ‘offensive’ ones are being asked later and always with attentive and intensive care so that the level of trust between the two parties doesn’t diminish.

Analyzing and synthesizing the collected information is the next step in the process. The clarity and the impact of the information must be taken into account during the analyzing process. The higher the impact of a certain piece of information, the clearer it has to be understood. Reliability and timeline are also very important. While relevant information must also come from a reliable source, it has to be available ‘in time’. All these factors are filtering the information while under analysis.

Competitive Intelligence is dependent on communication with end-users of its products as much as the decision making process depends on the intelligence provided. This is profoundly related to the third step of the CI process – disseminating results. Getting feed-back from decision-makers makes the CI analysts more efficient and effective. However, there are some rules that the analysts who are processing data and are issuing results must follow in order to make the dissemination profitable for both parties involved. Knowing the end-user of the intelligence provided is always a must as the analyst needs to adjust its results’ presentation accordingly. The intelligence analyst needs to focus on the meaningful findings of his work and include information about sources and the way he or she has arrived to the conclusions presented. The golden rule is however related to the relationship between the CI process and the strategic management: CI must be neutral, should speak the truth and let the management decide. It should not support in any way the existing management strategies as it should not look in the past but in the future when issuing results. This is why CI must be an independent function of the company, accessible to the others and interconnected with knowledge management and strategic planning.

During the whole CI process, the most important role is played by human intelligence which is the determining factor behind the process’s capabilities. Of course, there should be a balance between the human sources and the published ones. However, to get “fresh” information, a company should focus on developing its human intelligence capabilities. The
company’s “oral history” is also a useful source of information and knowledge. Taking shape of anecdotic information, this tacit knowledge is in fact the institutional memory of the organization. Therefore it constitutes a premier source when starting to shape the psychological profile of the company and can also offer answers to operational problems.

Knowledge and experience are by definition cognitive qualities of persons. Transferring these to the organizational level of a company creates both opportunities and risks as the knowledge created through CI is imbedded firstly into the human resources that take part into the process.

2 Corporate espionage and easy profits

Espionage is not new in the business world. However, it is considered that economic espionage entered into a new development stage once the Cold War ended. If the governments conducted espionage practices to get publicly unavailable information during the Cold War era, the late ‘90s and the beginning of the new century are characterized by the emergence of new, private espionage techniques. Competitive intelligence is also developing during the same time espionage is transforming into private business. The emergence of the two is creating the sense of an unsecured business world conducting an information war.

Corporate espionage involves stealing trade secrets, blackmail and bribery with the purpose to gain and maintain advantage over the competition. Unlike competitive intelligence, corporate espionage is considered not only non-ethical but also a threat to any business functioning in the knowledge society.

Once the internet transformed itself from an academic and military tool into the “highway of information”, the way companies gather and process data has changed dramatically. The role and way of spying have also suffered transformations. Spies no longer need to brake into offices or managers’ homes to get information and the level of risk for them being caught diminishes. Spying requires the use of almost the same technology used as platform for competitive intelligence – the business intelligence procedures. The only difference is that in the case of corporate espionage, the internet and connections used are equipped with a more advanced ‘attacking’ mode. There is growing evidence that cyber attackers are turning their attention to espionage in both the public and private sectors. Cyber espionage ranks third on the SANS Top Ten Cyber Menaces for 2008. SANS think tank refers to such a development as overseas companies are trying to gain an upper hand while negotiating business deals with large companies based in the U.S. and Europe.

Using empirical evidence, one can see that since the ‘90s corporate espionage evolved from targeting high-tech and strategic industries towards targeting manufacturing ones today. After a qualitative analysis, taking into account the size of the businesses a larger distribution of targets is being shown. However, due to limited data available, one cannot statistically characterize the cases, nor establish a trend. However, it is confirmed by most analysts and think-tanks that corporate espionage is expanding in nature and geography.


The variability of spying ways and cases shows that this is an industry characterized by a lot of creativity. Below there are presented few of the spying cases that have attracted the media’s attention recently.

*Industrial espionage cases*:

**Avery Dennison Corporation** - In April 1999, two Taiwan executives and a Taiwan company were convicted of theft of trade secrets under the Economic Espionage Act of 1996. Pin Yen Yan, president of Four Pillars Company, and his daughter Hwei Chen "Sally" Yang were accused of stealing Avery Dennison adhesive formulas and innovations with the help of an Avery Dennison employee.

**Bristol-Myers Squibb** - In April 1999, Hsu Kai-Lo, technical director of the Yuen Foong Paper Company of Taiwan, pleaded guilty to one count of conspiracy to acquire a trade secret. Hsu attempted to steal the formula for Taxol, a cancer drug patented and licensed by the Bristol-Myers Squibb Company. Another defendant, Jessica Chou, is believed to be in Taiwan and is considered a fugitive by US authorities. Taiwan has no extradition treaty with the United States.

In 2001 **Procter and Gamble** admitted spying on rival Unilever for information on its shampoos.

**Boeing** was punished by the US Air Force in 2003 for resorting to espionage in order to better its defense rival Lockheed Martin.

**Intel** - in September 2003 Say Lye Ow, a 31 year old originally from Malaysia, pleaded guilty for copying sensitive information on Intel’s first 64-bit processor when he left the company in 1998.

2004: **Marks and Spencer** is investigating an apparent attempt to spy on the mobile phone records of its boss Stuart Rose.

2005: **California-based 3DGeo**, a seismic imaging software company – a visiting employee from China was given a two-year jail sentence for downloading its proprietary source code. Another Chinese-owned firm has pleaded guilty in New Jersey to stealing trade secrets from

---

*From selected RSS news feeds using* [http://news.google.com/nwshp?hl=en&tab=wn](http://news.google.com/nwshp?hl=en&tab=wn)
Lucent Technologies, the telecoms equipment maker.

2008: Rani Rahav PR agency - Modi'in Ezrahi, a private security firm’s employees have been convicted by The Tel Aviv District Court of using Internet spyware for the purpose of industrial espionage on the Rani Rahav PR agency (whose clients include Israel's second biggest mobile phone operator, Partner Communications), and the HOT cable television group. Another alleged victim was Champion Motors, who import Audi and Volkswagen motor vehicles.

The favorite targets of spies nowadays are trade secrets, business plans, customers’ lists and pricing data. The information thieves have many available intrusion methods: eavesdropping by bugging offices, wiretapping, capturing telephone conversations, penetrating computer networks and even using attractive men or women to form close relationship with an employee that has access to company’s secrets.

The availability and affordability of surveillance equipment has caused mounting worries about spying. Even primitive stuff such as baby monitors have proven recently to be successfully used for espionage purposes: in April this year, car maker Porsche AG said it had found a baby-monitoring device concealed behind the hotel sofa of its CEO, Wendelin Wiedeking, during his trip to Wolfsburg for meetings with executives at Volkswagen AG. Hollywood has also proved to be a spying spot as Anthony Pellicano was convicted in federal court in Los Angeles\textsuperscript{8} of multiple counts of racketeering and illegal wiretapping in May 2008. He reportedly worked for celebrities and moguls who were involved in personal or business disputes. Some of them are Bertram Fields, one of Hollywood's top entertainment lawyers and Brad Grey, now head of Viacom Inc.’s Paramount Pictures movie studio. To intercept the phone calls, Pellicano paid off phone-company workers and used computer-software programs.

\begin{table}[h]
\centering
\begin{tabular}{|l|l|l|}
\hline
Espionage techniques & Short description & Countermeasures \\
\hline
Keystroke logging programs and hardware & Copies keystrokes entered into computers’ keyboards in order to monitor computers’ activity and obtain passwords; the software can be installed manually or remotely via email attachments & Network firewalls
Computer network security check \\
\hline
WIFI interception & Software monitoring wireless internet connection & Encryption programs
Avoid using WI-FI connections from hotels or public spaces for confidential information
\hline
GPS tracking & Enables localization of one’s position & GPS signal jamming devices \\
\hline
Hidden microphones, & Allow eavesdropping & Technical counter \\
\hline
\end{tabular}
\caption{Tab. 2 – Espionage Mechanisms}
\end{table}

cameras surveillance sweeps that can detect data transmission using special equipment Cell phones jamming devices

Source: conversations with CT specialists, Stratfor

As the corporate espionage business is growing, so is private security. Many of the victimized companies and not only have started to use security contractors and practice Technical Security Counter Measures (TSCM) to protect themselves. But protection has its limits, too: for instance, eavesdropping on the company’s CEO conversation with his business partner in the hall room of a hotel or during a conference cannot really be stopped.

Corporate espionage is at its heart about people as individuals and corporations, even if technology helps a lot. People hold the decision to spy or not on the competitors. This is why the most important countermeasures against spying activities are directly referring to employees’ activities. To show most of the countermeasures that can be implemented, I selected some of the most used espionage techniques that only persons can use:

- **Phishing:** is a form of social engineering in which spies use a collection of techniques to manipulate people into releasing information (such as passwords) or performing actions that compromise confidential data (clicking on a link that enables someone else to remotely control the computer); **Countermeasures:** raise employee awareness of these techniques; avoid exposing too much information on public Web sites (logos and employee e-mail addresses, telephones)

- **Insider theft:** employees are paid to steal information; **Countermeasures:** check employees behavior regularly and notice if any employee uses the access rights to download greater volumes of data than he/she ordinarily does; use the access control capabilities of the operating system; disable the USB ports through the system's password-protected BIOS or use centralized tools that restrict the use of ports and external devices

- **Visitor posing:** a spy can infiltrate the company by posing as a legitimate visitor (a telephone or electrical maintenance person, etc.); **Countermeasures:** check identities of outsiders seeking access to the building using more than ID cards - ask a visitor to identify his employer, and then verify the information on the Web or follow up with a phone call to the company to ensure that the visitor is legitimate

- **Employee posing:** a spy can infiltrate the company pretending he/she is an employee – usually IT support personnel as it enables the spy to look legitimate while sitting at users’ computers; **Countermeasures:** employee awareness; use protective tools such as screensavers with password controls; classify information in terms of how valuable it is and store it accordingly - encrypt data and require strong passwords for employees with liberal access rights, such as IT administrators and C-level executives

The main incentive to conduct espionage practices for a person or a company is the expected reward which is sometimes more persuasive than the concern over the risks involved in getting the data on the competition. Being an unlawful practice, businesses engaging in espionage may face tough repercussions for their actions. The consequences include deterioration of the firm’s reputation and its ability to enter new markets or attract new international partners. However, taking into account strictly the legislation aspect, only the US has implemented legislation directly referring to the spying practices: the Economic Espionage Act 1996. There isn’t a harmonized legislation on copyright issues, every country
holding its rights to impose its own rules. This positively influences the rise of espionage worldwide as differentiated practices also create opportunities for spies. Therefore, the only factor that can impede the growth of the sector is the ethical conduct of businesses.

In the same time, the countermeasures that must be implemented by companies in order to ensure that they are not spied have to be established so that the employees’ privacy is respected. Practices as the one the German retailer Lidl has implemented recently are showing the downturn of being too protective as it reaches an aggressive level.

3 From theory to practice – a case for competitive intelligence

Theory shows that the competitive intelligence should not be ever confused with corporate espionage. The thick line separating the two – represented by ethics – is however showing that there is enough room for competitive intelligence to become espionage or at least use corporate espionage practices. To underline the differences and the similarities, I have chosen to present a case from practice. To protect the companies that are presented in the following case study, trade denominations were excluded from the presentation.

Subject: the company is a producer of soft beverages in UK
Problem: the company has heard 3 rumors about its main competitor: that it was planning to change the name of one of their products to bring it into line with the European names often used for that product’s category; that it was planning to change the sweeteners formulation used; that the new product (with new name and formulation) is tested in another country market where the original (not modified) product has been sold
Question to be answered: What is the competitor next action? (validate/invalidate rumors)

Solution offered by CI analysts:

Steps followed:
- examine the background: UK low sugar soft drinks are using the name ‘diet’ while in Europe ‘light’ or ‘lite’ is used to show the same quality; identify the artificial sweetener used for the sugar-free soft drink under question: Aspartame; identify what other artificial sweeteners are being used: Aspartame/Acesulfame K mixture
- literature search on the rumored test-market country press – a press report was found discussing the proposed change of name and formulation => rumor nr.3 was confirmed
- check what other sweeteners are used in soft-drinks sold on the test market: most of them is using the Aspartame/Acesulfame K mixture
- literature search to find out concerns related to sweeteners and general attituded towards non-sugar soft-drinks names in the test country: there were concerns on all artificial sweeteners, word ‘diet’ was more attractive for women than the word ‘light’ but men were less likely to buy a drink named ‘diet’ but they did buy ‘light’ tagged ones.
- Start primary research – call sources (other competitors, industry analysts, bottling company, PR agency etc); little was found to confirm or infirm the other 2 rumors; all sources confirmed that there will be a change but couldn’t confirmed what kind – both name and formulation or just one of the two
- Use qualitative analysis – game theory approach to model the risk factors for the 3 options available for the competitor (from primary research it was known that ‘there would be no change’ option was impossible)
= name and formulation would change: highest risk strategy. The approach involves a need to convince current customers about new name and taste as well as to entice new customers to try and drink the new product. This meant that the company would need to spend a lot on advertising to both keep current customers and attract new ones.

= changing the name: a high risk strategy. It involves re-educating the current customers on the new name. New customers that wouldn’t like the taste of the old drink under the new name wouldn’t remain customers after trying the drink while existing customers would defect.

= changing the formulation: low risk. It involves enticing new customers with the new taste and convincing the existing customers that the new taste is better. The expenses for promotion are less than required for the name change and leaves the option for name change opened.

- formulate conclusion and recommendations: all that would happen is a formulation change as the other 2 options were too risky. The name change may follow at a later stage after the taste change was accepted.

- Checking and feed-back: the conclusion was similar to what happened on the market; the competitor’s move was anticipated correctly

In the example presented above only competitive intelligence techniques were used. The case-study shows a classic situation of CI success stories. However, corporate espionage can as well be implemented. The main reason for which espionage can be considered is the fact that information is not publicly available, nor it can be easily deducted from open-sources. Instead of spying on CEO, the Marketing Manager or the R&D Manager, competitive intelligence builds a most-likely scenario using all available information from both primary and literature research. The scenario is used for future planning and contingency plans can be drawn up in case one of the less likely scenarios turns out to be true. Competitive intelligence protects the company as it takes into account all the possibilities, drawn after an attentive analysis of the facts.

Conclusion

Competitive intelligence helps answering key questions. It focuses on building and solving hypothesis, explaining things that seem to be inexplicable. Competitive intelligence is intimately linked to the strategic decision making process, supporting a sustainable evolution of the company in a changing business environment. CI creates value added using the collection of intangible assets. In contrast, corporate espionage defines an unethical and continuous search for any details that can be used either to paint a bigger picture about a competitor or for blackmailing purposes. Acquiring and maintaining an advantage over the competition is the common goal that both espionage and CI has. However, through analysis methods, CI is able to create a stable environment for the decision making process. Espionage, even if it provides useful information, doesn’t help the company to create knowledge, being useful only on the short term.

Mainly differentiated by ethical concepts, both competitive intelligence and corporate espionage are emergent in the twenty-first century. While corporate espionage is widely condemned by the business world, competitive intelligence practices are developing and enjoying more attention from the decision makers every day. Theory is demonstrated in practice as companies are implementing their own competitive intelligence departments and business intelligence agencies are developing to offer the new kind of service.
Technological progress and profit are not the only reasons that demand for an intelligent approach of the business environment. They are only the key drivers. What makes intelligence essential today compared to the past is the speed of changes in the society where knowledge became the most important asset.

**Literature:**

[1] *** Aware Competitive Intelligence Case Studies, [www.marketing-intelligence.co.uk](http://www.marketing-intelligence.co.uk), 2005
Between Intelligence and Espionage in the Contemporary Business Environment

Oana – Antonia Colibasanu

ABSTRACT

The growing use of technology as a fundamental tool for knowledge management has obliged the business world to adapt to the information revolution era. Competitive intelligence is the new management tool companies are using for ensuring positive results both on the short and the long term. The following research paper starts by revealing the needs that companies respond to when implementing competitive intelligence and continues with a summary of the main techniques used by businesses to develop an intelligent market approach. The paper also offers a brief description of corporate espionage practices, underlining the differences between these and the competitive intelligence techniques. A case study showing the way that competitive intelligence is implemented in practice is being offered. Conclusions refer to the main differences between corporate espionage and competitive intelligence as well as the driving forces determining the need for acquiring knowledge on competitive intelligence.

Key words: competitive intelligence, corporate espionage

JEL classification: F23, M10, M31