COMPETITIVE INTELLIGENCE AND COUNTERINTELLIGENCE – MODERN TOOLS FOR GENERATING PROACTIVE CORPORATE SECURITY

КОНКУРЕНТНО РАЗУЗНАВАНЕ И КОНТРАРАЗУЗНАВАНЕ – СЪВРЕМЕННИ СРЕДСТВА ЗА ИЗГРАЖДАНЕ НА АКТИВНА КОРПОРАТИВНА СИГУРНОСТ

Tsanko V. Ivanov. PhD Student
Faculty of Economics – Industrial Business Dept. University of Economics – Varna, Bulgaria
tsanko_ivanov@ue-varna.bg

Abstract: *There are a much larger number of both present and emerging threats for modern business than ever before in history. Using only classical methods and tools for protecting the enterprises' assets is no longer effective. More and more companies are implementing modern tools such as competitive intelligence and counterintelligence in order to survive in the new hypercompetitive global markets. Those companies strive to gain proactive knowledge for the environment in order to generate successful systems for corporate security and industrial counterespionage.*

Keywords: COMPETITIVE INTELLIGENCE, BUSINESS INTELLIGENCE, COUNTERINTELLIGENCE, CORPORATE SECURITY, KNOWLEDGE MANAGEMENT, INDUSTRIAL COUNTERESPIONAGE

1. Introduction

Forces and factors from the business environment, characterized by perpetual change and uncertainty, are becoming more and more unpredictable and they can easily disrupt even the most comprehensive strategic plans. One group of them includes some classical external forces such as political or macroeconomic crises, social outbreaks or new technological outbursts. The second group also sums up well-known factors related to the existing or emerging competitors. In addition, there is a whole new group of risks such as possible terror attacks, especially against Western companies all over the globe and other forms of hybrid threats. In this regard, managers must learn to understand, anticipate and respond to the threats they face along with other forces likely to have an impact on their business performance (Bernhardt, 2003, p. viii). As Stephen Miller states, realizing the need of implemented competitive strategy, a growing number of the biggest world companies have established intelligence functions within their units but most of them lack fully operational toolkit. Such a toolkit serves as an early warning on future events that can have impact on company performance. On the one side, competitive (or business) intelligence and competitive analysis are implemented in order to predict what all kinds of focus groups such as competitors, suppliers, major customers, etc. will do before they do it and react accordingly to that specific knowledge. On the other side, corporate counterintelligence includes the opposite actions for protecting the company's assets from similar operations conducted by some of the focus groups mentioned above. The military doctrinal fundamentals are similar. Intelligence operations are conducted in order to achieve two objectives: 1) it provides accurate, timely and relevant knowledge about the enemy (or potential enemy) and the surrounding environment; 2) includes active and passive measures intended to deny the enemy valuable information (USMC, 2007, p. 1-1). The aim of this report is to provide readers with the concept that developing proactive corporate security capabilities can provide valuable input to corporate strategy and planning processes.

2. Definitions

2.1. What is Competitive Intelligence?

According to a research conducted by the Global Intelligence Alliance (GIA) competitive intelligence can be defined as knowledge and foreknowledge about the external operating environment which ultimate goal is to improve the decision-making processes of the companies (GIA White Paper, 2004, p. 2).

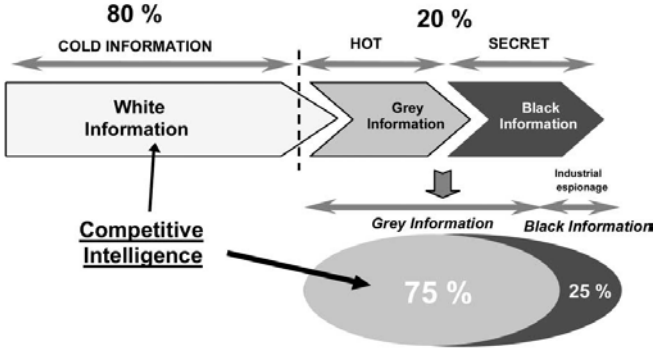
Rouach and Santi refer to competitive intelligence as 'a kind of a radar screen' – a legal and ethical process which tracks the activity of both direct and indirect competitors in a range of fields such as general business activity, business development, strategy and tactics, research and technology and so on in order to help the company shape its future and protect itself against current competitive threats (Rouach and Santi, 2001, p.553).

Competitive intelligence is neither market research nor industrial espionage: it involves the use of public sources to develop data on competition, competitors and the market environment (McGonagle and Vella, 2002, p.3). Sources of such information include business and trade publications, government documents, newspapers in competitor locations, advertisements and promotions, financial reports, industry reviews, market statistics and any other information that can be legally and ethically identified, located and accessed.

In addition, there is a great difference between information and intelligence. Usually, today companies possess too much information and not enough intelligence. Understanding that difference in time would help them protect their corporate secrets as well as improve their decision making. According to Kahaner (1996) *information is factual* – it consists of numbers, statistics, scattered bits of data and it is impossible to make accurate predictions based on it no matter how comprehensive it is. On the other hand, *intelligence is knowledge* – it is a collection of information pieces which have been filtered and analyzed. Authors and professionals are unanimous about distinguishing three types of data (Figure 1 illustrates how collected data are split into the three different categories):

- *White Information* which can be found in a range of data sources, many of them listed above, also called *open-source information*;
- *Grey Information* that includes private domain data such as trade shows and other publications often ignored by competitors; it can also be referred to as *restricted information*;
- *Black Information* can be collected beyond the point of ethics; it is *illegally-obtained information* by means of computer piracy, corporate espionage, telephone wire-taping and so on.

Figure 1: Classification according to information types



(The figure is excerpted from European Management Journal, Vol. 19, No. 5, p. 555, October 2001)

A logical conclusion from the above listed definitions would be that the best competitive intelligence practices are found in the most powerful companies. In relation to enterprise's size and budget, Rouach and Santi (2001) have managed to identify five types of analytical attitudes towards competitive intelligence:

Figure 2: The Five Intelligence Attitudes

Analyst type	*State of mind*	*Methods*
1. WARRIOR	War mentality; always informed; offensive position	Sophisticated tools; unlimited or significant resources
2. ASSAULT	Former law enforcement agents; hunt for strategic intelligence	Significant resources; code of ethics; a lead lookout; value put on HUMINT
3. ACTIVE	Observatory of competition	Limited resources
4. REACTIVE	Opportunists	Reacts to attacks; very limited budget
5. SLEEPERS	No particular action	Blind; passive

To sum up, the most important part of any proactive corporate security system is the competitive intelligence cycle. Logically, as stated by the GIA, companies nowadays are encouraged to implement the classical four-step intelligence cycle used by the CIA and other national security organizations around the globe (GIA White Paper, 2004, p. 9). As Kahaner (1996) describes, such a cycle within a corporation includes 1) planning and direction ('setting goals' within a national intelligence system), 2) collection (obtaining data from different sources), 3) analysis (comparing information) and 4) dissemination (estimating possible future developments). McGonagle and Vella (1996) also agree with that model. However, a number of researchers add more stages to the classical model – Miller (2000) puts a fifth stage called *feedback*; Bernhardt (1994) includes a *processing* level as a link between the collection and the analysis; Ashton and Stacey (1995) expand the original model to a sixth step called *auditing the system's performance*. As a result, GIA's experts develop an eight-step competitive intelligence cycle depicted in figure 3:

Figure 3: The Competitive Intelligence Cycle

(The figure is excerpted from Global Intelligence Alliance (2004) Introduction to Competitive Intelligence. GIA White Paper 1, p. 11)

2.2. What is Corporate Counterintelligence?

Counterintelligence within business units can be defined as the identification and neutralization of numerous threats posed by any rivals' intelligence services, and the manipulation of those services for the manipulator's benefit (Bernhardt, 2003, p. 85).

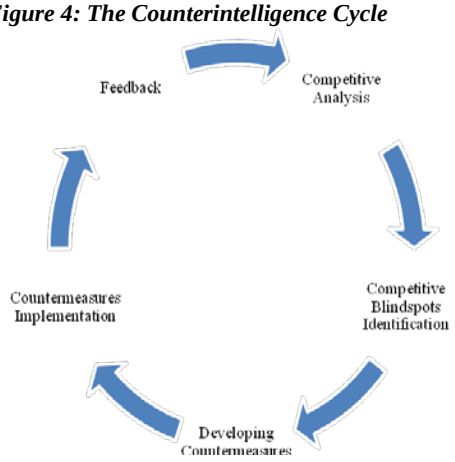
According to Strauss (1999), corporate counterintelligence is the other side of competitive intelligence because it represents the process by which companies defend their internal information.

Corporate counterintelligence possesses both active and passive characteristics (Bernhardt, 2003, p. 89). Corporate security experts are unanimous that passive counterintelligence implements defensive tactics and tools such as software solutions, countersurveillance and penetration testing. On the contrary, active counterintelligence implements offensive tactics and further investigates any illegal, unethical or threatening activities to their sources.

The classical counterintelligence process at all levels includes four steps: 1) develop a counterintelligence estimate; 2) conduct counterintelligence surveys; 3) develop the counterintelligence plan; 4) implement appropriate counterintelligence measures (USMC, 2007, p. 1-5).

John Nolan (1996), a researcher for the Phoenix Group, a world class security company, manages to distinguish the two basic dimensions of corporate security – external and internal. Logically, the Phoenix Group itself proposes a counterintelligence cycle in collaboration with the classical intelligence cycle.

Figure 4: The Counterintelligence Cycle



To sum up, the most fundamental goal of the counterintelligence unit is to ensure proactive countering of threats and to enhance corporate security in general by protecting the assets not only against criminal theft but also against entirely legal competitive intelligence efforts by business rivals.

3. Types of Threats and Industrial Espionage Tools

As mentioned earlier, businesses can easily become a target of foreign intelligence organizations, competitors or corporate spies. According to Steve Whitehead, a lifelong security expert in the field of counterespionage, methods of espionage and motivational factors behind them include (Bernhardt, 2003, p. 90):

- Trespassing;
- Covert surveillance;
- Electronic eavesdropping and bugging;
- Trash collection;
- Burglaries;
- Blackmail and bribery;
- Stealing of documents;
- Insider threat – recruitment of a staff member or infiltration of an agent.

Ira Winkler, a security consultant, adds four large categories of vulnerabilities within a company (Winkler, 1997). They include:

Operational vulnerabilities:

- Social engineering;
- Unchecked internet usage;
- Carrying work around or home.

Physical vulnerabilities:

- Easy building access;
- Open or poor storage of information;
- Lack of computer passwords.

Personnel vulnerabilities:

- No background checks;
- Susceptibility or crime;
- Personal situations causing stress or financial hardships.

Technical vulnerabilities:

- Known bugs in the system;
- Easily broken passwords.

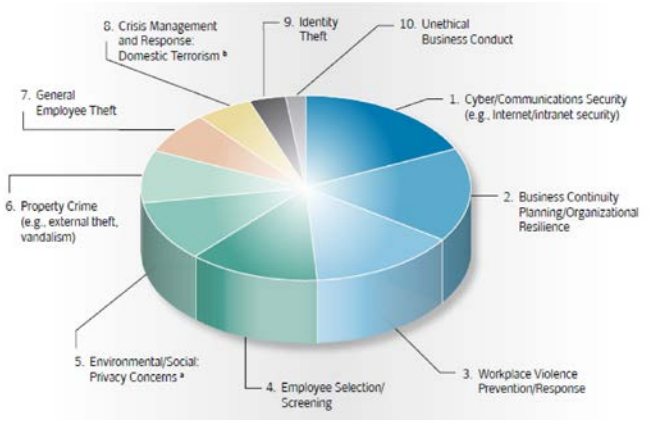
According to Stephen Fink, the most targeted groups include (Fink, 2002, pp. 266-267):

Figure 5: Groups of Targets for Industrial Espionage and Competitive Intelligence

Most targeted trade secrets	Most targeted industries	Most targeted assets
Customer lists	Pharmaceutical	Formulas
Pricing information	Chemical	Patterns
R&D information	Food	Programs
Sales information	Computer software	Devices
Manufacturing information	Aerospace	Methods
Strategic plans	Automobile	Techniques
Cost information		Proprietary processes

In a survey conducted in 2014 experts from Securitas Security Services USA Inc. have identified some trends related to security threats, management challenges and operational issues from Fortune 1000 companies. The study, which is often cited as an industry standard, revealed the issues of greatest concern to corporate security directors:

Figure 6: 2014 Top Security Threats



(The figure is excerpted from "Top Security Threats and Management Issues Facing Corporate America." Securitas Security Services USA Inc., p. 4)

As depicted in the paragraph, the types of threats, espionage tools and management issues vary enormously. That is the reason why the need for establishing proactive corporate security through implementing modern business tools has grown as stated in the beginning of the report.

4. Results and Discussion

As former F.B.I. special agent Edwin Fraumann once said, 'Increasing international economic competition has redefined context for espionage as nations link their national security to their economic security. Spying conducted by intelligence services is expanding from its primary focus on military secrets to collecting economic secrets' (Fraumann, 1997, 303). As a result, any company could become a target for economic or industrial espionage much more regularly than military or political institutions. Logically, corporate counterintelligence along with competitive intelligence must be integrated within the strategy of the organizations. Any other company's attitude towards the issue could be devastating for its very existence.

Whether economic, industrial or corporate espionage has been engaged to harm a company, the company must counteract. To begin with, competitive intelligence and counterintelligence should be implemented within the security strategy of the companies but it should not be confused with security in general. Whether that strategy is defensive or offensive, both tools could possess passive or active components.

Passive components focus mostly on preventive measures. As explained earlier, those measures may include:

- **Security education** strengthens personnel situational awareness towards espionage threats. All security measures and practices become useless without properly trained staff members. Such trainings should be conducted on a regular basis in order to improve employees' knowledge about both competitive intelligence tactics and illegal information gathering.
- **Defensive measures** include a number of programs which identify possible threats among personnel and the related risks that vulnerable to outside influence may bring. Security expert Steve Whitehead mentions an employee assistance program (EAP) which offers solutions for personal problems that are the main reason for recruitment by an industrial spy (Bernhardt, 2003, p. 94).
- **Technical countersurveillance (TSCM)** consists of a set of measures for identifying illegal technical devices planted for information collection purposes. TSCM's purpose is to prevent any technical intrusions which represent the last possible tool used by industrial spies when their ways to targeted organization are cut off.
- **Penetration testing** is used for assessment of the vulnerabilities of critical for the competitive edge facilities, areas and activities. Most security systems are unable to counter professional espionage team. However, regular penetration testing could evaluate the current effectiveness of the security system and improve counterintelligence practices against most commonly hired for industrial espionage.

Active components focus mostly on active and proactive measures which include:

- **Corporate investigations** provide information about companies' most valuable assets – their people. It is a very useful proactive tool which mitigates employee related risks through biographical facts, background checks and thorough research before an employee is even hired.
- **Competitive intelligence and counterintelligence operations** should implement effective policies and procedures for information classification. Such measures could implement a new corporate culture related to the active protection of information by employees.
- **Ethical collective process** could be implemented when the security unit in charge finds proofs for illegal proprietary information collection. Firstly, security officers should inform the law enforcement agencies. Then, they could apply their own counter measures.

Ultimately, as Bernhardt (2003) states, the finished intelligence product is the most important decision-making tool. Although it is a rather new term for companies, finished intelligence is split into five generic categories used by the U.S. Intelligence Community:

1) *Current intelligence* – to provide managers from different levels with arising developments likely to have an impact on corporate strategy, tactics or operations;

2) *Estimative intelligence* – a comprehensive analysis and long-range forecasts developed for the senior management in order to help them predict the possible opportunities and threats;

3) *Research intelligence* – classified studies that are split into two subtypes: *basic research intelligence* and *operational support intelligence*;

4) *Scientific and technology intelligence* – crucial for innovative companies operating within science or technology industries; related to competitors' research and development operations;

5) *Warning intelligence* – includes warning watchlist and alerts.

5. Conclusion

To sum up, the craft of intelligence today has evolved considerably – to the point in which even corporate board members rely on intelligence and counterintelligence units to help them better predict the external environment.

A 'perfect' corporate security system does not exist. However, if the aspects analyzed above are aligned with the organizations' architecture at all levels, a very sophisticated mechanism could be created. That new system provides proactive security to the corporations which bring some specific benefits such as:

- Enhanced knowledge management assets which will ultimately bring to increased shareholder values;
- Intelligence deliverables in the form of high value-added competitive intelligence products;
- Early warning of competitive threats thanks to the counterintelligence cycle within the organization;
- An effective human-source intelligence (HUMINT) capabilities thanks to the proactive security education;
- A trusted internal source of news and trends related to the external environment relevant to strategic and tactical decision-making;
- Improved operational communications related to security within the organization;
- Enhanced corporate security culture between the employees.

6. Literature Review

1. Ashton, W. & Stacey, G. (1995) *Technical Intelligence in Business: Understanding Technology Threats and Opportunity.* International Journal of Technology Management, Vol. 10, pp. 79-104.

2. Bernhardt, D. (2003) *Competitive Intelligence: How to acquire and use corporate intelligence and counter-intelligence.* London: Pearson Education Ltd.

3. Bernhardt, D. (1994) *I Want it Fast, Factual and Actionable – Tailoring Competitive Intelligence to Executives.* Long Range Planning, vol. 27, pp. 12-24.

4. Fink, S. (2002) *Sticky Fingers: Managing the Global Risk of Economic Espionage.* Chicago: Dearborn Trade Publishing.

5. Fraumann, E. (1997) *Economic Espionage: Security Mission Redefined.* Public Administration Review (July/August).

6. Global Intelligence Alliance (2004) *Introduction to Competitive Intelligence.* GIA White Paper 1.

7. Kahaner, L. (1996) *Competitive Intelligence.* NY, USA: Kane Associates.

8. McGonagle, J.J. & Vella, C.M. (1996) *A New Archetype for Competitive Intelligence.* Greenwood Publishing Group Inc.

9. McGonagle, J.J. & Vella, C.M. (2002) *Bottom Line Competitive Intelligence.* Westport: Quorum Books.

10. Miller, J. (2000) *Millennium Intelligence: Understanding and Conducting Competitive Intelligence in the Digital Age.* CyberAge Books.

11. Rouach, D. & Santi, P. (2001) *Competitive Intelligence Adds Value: Five Intelligence Attitudes.* European Management Journal, Vol. 19, No. 5.

12. Strauss, K. G. (1999) *Marketing Telecommunication Services.* Artech House Telecom Company.

13. *Top Security Threats and Management Issues Facing Corporate America."* Securitas Security Services USA Inc.

14. U.S. Marine Corps (2007) *Counterintelligence.* NY: Cosimo Reports, Inc.

15. Winkler, I. (1997) *Corporate Espionage.* Rocklin, CA: Prima Publishing.