Güvenlik ve İstihbarat Çalışmaları Dergisi
Journal of Security and Intelligence Studies

Yıl/Year: 2023
Cilt/Volume: 1
Sayı/Issue: 1

Makale Geliş Tarihi: 11/11/2023 **Makale KabulTarihi:01/12/2023**
Received: 11/11/2023 **Accepted: 01/12/2023**

Atıf Bilgisi/Citation
Altıntaş, Kadir Murat. "Strategic Analysis and Methodology of Corporate Espionage for Global Companies within the Framework of Post-Modern Management Functions". Güvenlik ve İstihbarat Çalışmaları Dergisi, c.1 s.1 (2023): 1-23.

Makale Bilgisi/Article Information
Araştırma Makalesi/Research Article

STRATEGIC ANALYSIS AND METHODOLOGY OF CORPORATE ESPIONAGE FOR GLOBAL COMPANIES WITHIN THE FRAMEWORK OF POST-MODERN MANAGEMENT FUNCTIONS

Kadir Murat ALTINTAŞ[1]

Abstract

Corporate espionage through the misuse or theft of trade secrets and/or intellectual properties threaten the innovation ability and growth potential of business organizations as well as national economies. The potential damage can be faced by companies such as losing their competitive superiority, declining in stock unit prices, losing of prestige/trust among customers/stakeholders, descending in market share or loss of investment opportunities, or the disappearance of effectiveness in internal decision-making mechanisms. The primary purpose of this study is to emphasize the conceptual framework and strategic importance of corporate espionage, which has a guiding function, especially in terms of the global commercial activities of multinational companies. In addition, the study aims to comparatively analyze the economic/financial effects of such kind of recent espionage attacks on global markets. Strategically important corporate espionage attacks are a serious source of threat, especially for companies operating on a global scale, but these initiatives also contain serious opportunities. Therefore, the ideal strategy for companies is, on the one hand, to protect their technological know-how against corporate espionage attacks in line with the CI principles, and on the other hand, not to ignore the extraordinary gains of corporate espionage by remaining within legal limits.

Key Words: *Intelligence, Corporate Espionage, Counter-Intelligence, Industrial Espionage, Post-Modern Management Functions.*

POST-MODERN YÖNETIM FONKSİYONLARI KAPSAMINDA KÜRESEL ŞİRKETLERE YÖNELİK KURUMSAL CASUSLUĞUN STRATEJİK ANALİZİ VE METODOLOJİSİ

Öz

Ticari sırların ve/veya fikri mülkiyet haklarının kötüye kullanılması veya çalınması yoluyla icra edilen kurumsal casusluk faaliyetleri, ulusal ekonomilerin yanı sıra ticari kuruluşların inovasyon yeteneğini ve büyüme potansiyelini tehdit etmektedir. Kurumsal casusluk saldırıları sonucu mağdur şirketlerin rekabet üstünlüğünü

[1] Prof. Dr.
Abant İzzet Baysal Üniversitesi Uygulamalı Bilimler Fakültesi
kadiraltintas@ibu.edu.tr.
ORCID:0000-0001-8422-1086

kaybetmesi, hisse senedi birim fiyatlarının düşmesi, müşteriler/paydaşlar nezdinde prestij/güven kaybı, pazar payının düşmesi veya yatırım fırsatlarının kaybedilmesi ya da iç karar alma mekanizmalarındaki etkinliğin ortadan kalkması gibi potansiyel zararlar ile karşılaşabilmeleri muhtemeldir. Bu çalışmanın temel amacı, özellikle çok uluslu şirketlerin küresel ticari faaliyetleri açısından yol gösterici bir işleve sahip olan kurumsal casusluğun kavramsal çerçevesini ve stratejik önemini vurgulamaktır. Ayrıca çalışma, son dönemde gerçekleşen bu tür casusluk saldırılarının küresel piyasalar üzerindeki ekonomik/finansal etkilerini karşılaştırmalı olarak analiz etmeyi amaçlamaktadır. Stratejik öneme sahip olan kurumsal casusluk saldırıları, özellikle küresel ölçekte faaliyet gösteren şirketler için ciddi bir tehdit kaynağı olmakla birlikte, bu girişimler aynı zamanda kendi içinde önemli fırsatlar da barındırmaktadır. Bu nedenle şirketler için ideal olan strateji, bir yandan kurumsal casusluk saldırılarına karşı teknolojik bilgi birikimini istihbarata karşı koyma prensipleri doğrultusunda korumak, diğer yandan da yasal sınırlar dahilinde kalınmak şartıyla kurumsal casusluğun olağanüstü kazanımlarını da göz ardı etmemek gerekmektedir.

Anahtar Kelimeler: *İstihbarat, Kurumsal İstihbarat, İstihbarata Karşı Koyma, Endüstriyel Casusluk, Post-Modern Yönetim Fonksiyonları.*

Introduction

The initial benefit of Research and Development (R&D) activities for global commercial entities increases the profitability and maximizes the value of enterprise within the scope of commercialization of technology tendency in the last half century. The possible commercial results created by value added activities, which we can express as 'mental capital', also have a substantial role in economic and financial development of societies. Today, global companies that continue their activities under intense competition and productivity pressure have to ensure 'differentiation' for the products and services they produce. Otherwise, they cannot achieve the relative advantage that we can briefly summarize as commercial sustainability. In other words, within the scope of innovative product development efforts in the last half century, knowledge-intensive technology investments of global companies have further highlighted the strategic importance of R&D activities and almost turned them into the unique requirement of financial success of corporations.

At this point, it was necessary to ensure both the physical and the virtual security of technological savings achieved by multinational global companies as a result of high-scale R&D investments. Establishing the security of registered assets containing high technology within the scope of intellectual property rights against all kinds of hostile attacks originating particularly from rival companies (sometimes with the help of foreign intelligence services behind the scenes) have gained strategic importance. This approach, which can be summarized as ‘data and information security’ that directly affects the global competitiveness of innovation-oriented companies, has found its place among the traditional management functions of companies.

A comprehensive survey was conducted by the European Union in 2013 on the economic importance of trade secrets. This survey, which includes questions about the use of trade secrets, potential risks and legal protections, received responses from 537 companies, including small and medium sized companies (SMEs), which constitute approximately 60% of the sample. It was understood that 75% of the participants agreed that trade secrets are of strategic importance in terms of companies' growth, competitiveness and innovative capabilities. The survey reveals that in the last decade, one in five respondents has been subjected to a corporate espionage attack to misappropriate trade secrets within the European Union at least once. Additionally, approximately two out of every five participants stated that the risks of exploitation of trade secrets increased remarkably during the same period. In this study, senior managers also stated that trade secrets play an important role in protecting the returns to corporate investments and is actually an integral part of general protection system of intangible assets (European Commission 2013). Again, as of 2004, more than 50% of Fortune 1000 companies admitted to being victims of corporate espionage attacks and the overall costs of these attacks was approximately 200 billion dollars annually for American companies (Rodgers and Marrs, 2004, p. 61).

The result of the "industrial protection" survey conducted by a non-governmental organization (BITKOM-representing more than 2200 companies in Germany's information, communication and new media sectors) with 503 senior managers in 2018 have been announced. Announcing the survey results in the Berlin, BITKOM President Achim Berg said that 7 out of every 10 industrial companies in the country have been the victims of sabotage, data theft or corporate espionage attacks in the last two years. Berg underlined that companies that do not adequately invest in the security of information technologies are negligent and endanger their business. He was also stated that, contrary to popular belief, small and medium-sized companies were more vulnerable to such kind of attacks (Gönültaş, 2018).

Since the beginning of 21st century, global companies have discovered that intelligence and espionage activities can be considered as a strategic management function in order to obtain higher sales volumes or to increase their market shares under intense market competition. In order to strengthen the medium-long term business plans of global companies and increase the efficiency of their decision-making processes, the activity of collecting strategic data and information after that subjecting them to a comprehensive analysis is extremely valuable in terms of making sense of the difficulties faced in international markets as well as eliminating potential disabilities.

Corporate espionage, between rival companies, can cause serious damage to companies' commercial activities and financial sustainability, though it occurs within more limited means compared to public based espionage activities. This damage can be faced by companies such as losing their competitive superiority, declining in stock unit prices, losing of prestige/trust among customers/stakeholders, descending percentage in market share or loss of various investment opportunities, or the disappearance of effectiveness in internal decision-making mechanisms. More clearly, espionage attacks on trade secrets or intellectual property may cause target companies to lose their financial performance and innovation capabilities and also may bring negative changes in customers' loyalty as well as stakeholders' perception. For instance; a study conducted specifically in the US claims that the cost of espionage attacks to capture trade secrets or intellectual properties to the US economy corresponds to one third of the GNP (PricawaterhouseCoopers, 2014). Therefore, the carelessness of employees to physical and virtual security measures or their unconsciousness about the degree of confidentiality to data and information has caused corporate espionage attacks to become widespread and effective at nowadays.

When the effects of corporate espionage attacks on both the country's economies and the financial structures of companies are evaluated, it becomes clear from official data how serious a problem we actually face. In a study conducted in 2008, the International Chamber of Commerce estimated that the potential financial losses caused by corporate espionage at $600 billion annually, while the US Department of Commerce calculated the possible loss as $250 billion. Moreover, both institutions agreed that corporate espionage attacks caused approximately 700.000 employees to lose their jobs in the United States every year (Burgess and Power, 2008, p. xvii). To make this general appearance more perceptible, it could be useful to analyze a corporate espionage conflict, which was happened between two well-known global companies in 2001. As a result of mutual negotiations, Proctor&Gamble has agreed to pay $10 million to Unilever (for not resorting to legal processes) for the corporate espionage attack it carried out in order to obtain details about a newly launched shampoo brand. Proctor&Gamble, which captured more than 80 documents containing Unilever’s plans regarding its hair care unit, calculated the loss of prestige it would experience in the sector as a result of the exposure of this corporate espionage attack, and could easily agree to pay such an amount in order to prevent from further scandals (Barnes, 2001).

In today's global markets where hyper competition exists, companies have increasingly consulted to espionage attacks carried out within the scope of intelligence activities in recent

years, in order to increase the efficiency in their decision-making processes. The fact that corporate espionage attacks are a serious source of risk for companies' data/information security and that such kind of charges directly threaten the intangible/tangible assets of companies has caused corporate espionage to be included within the scope of post-modern management functions. However, this situation has also revealed the need (even necessity) for a protective security system that includes strict measures within the scope of traditional Counterintelligence (CI) principles.

The primary purpose of this study is to emphasize the conceptual framework and strategic importance of corporate espionage, which was a guiding management function, especially in terms of the global commercial activities of multinational companies. In addition, the study aims to comparatively analyze the economic/financial effects of such kind of recent espionage attacks on global markets. Besides, improving a new model of theoretical implementation methods as a result of the analysis of many corporate espionage cases that have occurred in recent years is another intention of this study. Within the scope of the research methodology, descriptive content analysis was conducted on the data/information obtained from scientific and open sources through document review, one of the most preferred qualitative (quantitative) research methods. Descriptive research is a study in which the main emphasis is on determining the frequency of something (Bless et al., 2013). This study, designed with a qualitative research pattern, aimed to interpret the findings obtained as a result of descriptive content analysis and tried to reach final judgments with the help of intuitive reasoning. Salaria (2012) states that descriptive research is aimed at collecting information about existing conditions or situations for the purpose of explanation and interpretation.

1. Conceptual framework of corporate espionage attacks and their strategic importance for global companies

The extraordinary progress in information and communication technologies in the last quarter century has caused a radical transformation of national industrial infrastructures. Companies that can keep up with innovation-oriented technological improvements in their country have become the locomotive of economic development. This process, in which technological data and knowledge have become the primary subject of progress for societies. There has been a need for a contemporary perception of security concept, especially required by intelligence/security bureaucracies of developed countries. Accordingly, task description and limits of responsibility of the members of intelligence community of countries have been

restructured and the cornerstones of the combat against involuntary technology transfer have almost been redesigned.

The mutation of global companies into economic giants in the world economy depends mostly on their R&D investments. This situation actually points to the absolute existence of high correlation between innovation and selling. The strategic data/information and technological infrastructures of developed countries have evolved into the sole key to the economic welfare of their societies and have brought the issue of data and information security within the scope of intellectual property rights to the agenda of the world public opinion.

The sustainable growth rate due to the technological development of countries based on R&D expenditures can be interpreted similarly for commercial legal entities. More clearly, the ability of global companies, which are under severe pressure of competition, to increase their market shares or to enhance sales volume largely depends on the protection of their registered assets and commercial/technological secrets within the framework of intellectual property rights.

At this point, Schumpeter's "Creative Destruction Theory" helps to better understand today's commercial trends. According to Schumpeter, the main driving force of Capitalist System is new consumer goods, new production methods and/or new markets. This trend constantly transforms the existing economic structure from within, that is, it destroys the old and creates the new (Schumpeter, 1970, p. 83). To better understand the challenge with the help of a different point of view, there is an alternative that some of companies which do not want to make extraordinary R&D expenditures or long-term technology investments can choose. Today, unfortunately, among the primary business strategies of some companies, the activities of seizing the commercial and technological know-how of rival companies through unethical initiatives have a remarkable place.

Whether a company is owned by public/private or is engaged in production/service sector does not change the fact that an espionage case has been occurred. Such kind of corporate espionage attacks are generally carried out in order to regain the economic/technological potential it has lost, the companies' prestige it has wasted in commercial environment, the market share it has difficulty in developing, or the structural advantages it has lost in competition. Companies that make a strategic choice to realize such kind of achievements in short term must also have not been sensitive enough to social issues such as business ethics or social responsibility. Therefore, companies that are generally overshadowed by rival companies

in the sector and do not have sufficient motivation to reverse this situation can easily be deceived by the extremely attractive cost-benefit analyzes of corporate espionage activities.

Corporate Espionage, in short, is taking the control of economic, financial or technological data, information and documents owned by the target company, without the confirmation of rival companies or their employees. More precisely, it is the systematic seizure of confidential information regarding commercial/technological secrets or proprietary assets, by using unethical methods. The fact that corporate espionage attack is carried out with the support from a professional security-intelligence company through outsourcing, does not change the fact that corporate espionage has not been committed.

Although they are the concepts that have very similar meanings, there are also some notable differences among the concepts of Corporate, Economic and Industrial Espionage activities in terms of purposes, executioner and legal aspects. For this reason, it is useful to briefly clarify the possible differences among relevant concepts. When we examine the issue in terms of possible purposes, it is necessary to distinguish companies that aim to seize confidential data/information of rival companies through corporate espionage attacks from publicly supported (Economic or Industrial) espionage activities that do not have adequate sensitivity to remain within legal limits. Moreover, the administrative position of performing party also becomes crucial and makes the boundaries regarding the content of the concepts clear. Industrial Espionage differs from corporate espionage in that it involves public intelligence authorities behind the scenes and supports the activities of national companies on a global scale. On the other hand, Economic Espionage activities, which are carried out entirely under the direction and management of public intelligence authority, are generally carried out with the aim of destroying public resources of target countries or preventing their macroeconomic/industrial development. Therefore, industrial and economic espionage attacks are considered completely illegal, that is, an activity contrary to existing criminal laws.

Contrary to the popular belief that 'large companies are more exposed to corporate espionage attacks', small businesses are also exposed to corporate espionage attacks because they have many more competitors in the market (Fink, 2002, p. 18). It is necessary to distinguish corporate espionage attacks, which are more common in high-technology sectors (and oligopolistic markets) such as pharmaceuticals, automotive, software and defense industries, from 'Competitive Intelligence' activities, that is a legal intelligence gathering method for companies. Besides, the source of risks posed by corporate espionage attacks for companies may even originate from employees within the company or sometimes in the form of hostile

attacks originated from outside the company. Therefore, it would be more accurate for companies to evaluate the source of the potential threat within two main classifications: internal or external.

Sources of internal threats generally consist of current/former employees, business partners or stakeholders (contractors) collaborated with during outsourcing process. Internal threats cause greater damage than external attacks because current/former employees have more details of internal security protocols. According to the cybercrime research (2017) conducted annually by the Computer Emergency Response Team (CERT) of the Software Engineering Institute at Carnegie Mellon University, approximately 30 percent of the participants reported that the incidents caused by internal attacks were costlier or damaging with respect to outsiders. This study also revealed that 45% of incidents where sensitive information was unintentionally disclosed and 40% of incidents where customer records have been stolen caused by an 'in-house' employee. It has also been revealed in this study that 38% of the incidents in which personnel records were stolen, 35% of the incidents in which sensitive information was deliberately disclosed, and 33% of the incidents in which confidential records were obtained have 'internal' origin (Miller, 2018). Similar results were obtained in other studies (Trzeciak 2017; Colins et. al. 2016; PricewaterhouseCoopers 2017; Kellett 2015). Additionally, according to the Statistical Analysis of Trade Secret Lawsuits in US Federal Courts, in 85% of trade secret cases in federal courts, the responsible side was found to be either an employee or a business partner (Almeling, 2010). The motivation sources of current or former employees who are involved in corporate espionage attacks generally believe that they have been treated unfairly in the workplace, unusual reactions caused by differences (religious or political views), and inaccurate beliefs that similar attempts go unpunished, or even thrill-seeker. In addition, threats or blackmail against current/former employees are also triggered individuals to corporate espionage.

External threat sources are corporate espionage attacks by rival companies or (proxy) espionage attacks originating from outsourced firms such as intelligence or detective enterprises. Besides, organized crime organizations are also responsible from the external espionage attacks. However, it would be useful to emphasize the structural differentiation regarding corporate espionage. Since cyber-attacks originating from rival companies or hostile governments are considered as judicial 'crime' in the local legislation of all countries, it is not correct to structurally classify such kind of attacks under the concept of corporate espionage.

However, it is possible to associate cyber-attacks, which have become widespread in recent years, with data breaches through unauthorized entry into computer systems or electronic

building access systems. At this point, virtual threats from rival companies or hostile governments have increased due to factors such as the internationalization of business world, the fact that hackers have technology to access trade secrets from anywhere in the world, and the diseased preference of some countries-the only way of developing economy is illegal technology transfer (Almeling, 2012).

The main purpose of corporate espionage attacks on trade secrets or intellectual properties, either internally sourced within the company or carried out directly by a rival company (or proxies), is to save resources allocated to R&D activities, to ensure that rival companies suffer from reputational loss, to achieve absolute competitive advantage, and to increase the efficiency at decision-making process. Achieving such kind of returns mean that the performing organization acquires its mid/long term commercial and financial goals successfully.

It is possible to give some examples to corporate espionage operations, which we can briefly summarize these types of attacks as originating from "white-collar" employees. For example; monitoring and analyzing the preferences of a rival company or target employee at international commercial/technology expositions, "overhearing" phone conversations of target individuals at airports or obtaining the password of their laptop through "shoulder surfing", monitoring and analyzing the social relationships and professional connections of strategically positioned employees working in a rival company, ‘persuading’ employees to take know-how or codes out of the company via e-mail, leaking information from managers of rival companies at official negotiations, facility presentations or job interviews, secret surveillance and analysis of retail stores and their selling preferences, especially their internal activities, etc.

Corporate espionage activities are an increasing source of concern for global companies and they are generally aware that their competitors are trying to obtain information about them though they generally take various measures to prevent them. However, despite all the protective measures taken, rival companies can engage in highly successful espionage activities (Billand et al., 2009, p. 3). All companies, whether large, medium or small, face with various challenges arising from theft and misuse of their confidential information or trade secrets by internal or external units. Trade secrets or intellectual properties, which are the most strategic assets of a company, also reflect the economic value of corporation’s products, innovations and progressive capacity (Lippoldt & Schultz, 2014, p. 7) Intellectual property is the rights owned individually or corporately over a product that has economic value and is invented as a result of creative activities in scientific, artistic or industrial matters. Today, registered assets protected

by trade secrets laws and intellectual property rights are among the primary targets of corporate espionage attacks.

Corporate espionage attacks through the misuse or theft of trade secrets threaten the innovation ability, growth potential and investment capacity of business organizations and national economies (OECD, 2016; PricewaterhouseCoopers, 2014). Such activities may cause a commercial enterprise to terminate its operations or destruct business areas unless some precautions are taken to minimize the risks. The World Intellectual Property Association (2018) defines trade secrets as follows; 'In general, confidential data and information that provides a competitive advantage to any company in the market and has a commercial value (that is unknown to others) should be protected within the scope of trade secret.' Trade secrets include technical information such as manufacturing processes, pharmaceutical test data, designs and drawings of computer programs, as well as commercial information such as distribution methods, lists of suppliers and customers, or advertising strategies. Other examples of data and information that may be protected by trade secrets include financial information, formulas and recipes or source codes (WIPO, 2018).

In a study conducted by Baker Mckenzie in 2017 (on a sample of 400 top managers), it was concluded that trade secrets are more important than patents or brands, and that they also have a primary value in terms of brand value and corporate strategy. Approximately 32% of the managers participating in the research accepted the existence of threats and agreed that the theft risk of trade secrets was among top five issues of vital importance for companies. In the same study, 20% of companies declared that their trade secrets had been stolen before, 33% stated that they were the victims of espionage attacks on trade secrets, but 11% admitted that they were not even aware of whether they were the victims of any abuse or theft attack (Baker Mckenzie, 2017). The insufficient number for official applications to legal authorities actually hides the magnitude of the destruction. The main reason why many victims do not take legal position is the hesitation from reputational deficiency (loss of trust in customers/stakeholders, etc.) and possible financial losses (descending unit stock price or declining market share, etc.) or to prevent from economic/financial failures.

2. Methodology of corporate espionage and its effect on economic/financial markets

In addition to the studies on the conceptual framework of corporate espionage (Winkler 1999; Rothke 2001; Javers 2011; Mashingaidze 2015), particular studies conducted by Glitz

and Myersson (2017) and Lyakhovich (2019) within the scope of historical background are quite remarkable. Besides, the implementation methods of corporate espionage with the support of modern technology (for instance; unmanned aerial vehicles) have also been very popular, and the concept of espionage has undergone a structural transformation in recent years (Scott, 2021).

In a study conducted by Sandberg (2015) the human factor (inside or outside the company) was investigated within the scope of information security systems in corporate espionage attacks, and it was concluded that traditional security systems were inadequate in line with the developing technology and must have been focused especially on internal human resources. In a similar study, the phenomenon of trust between employee and employer was examined regarding the increasing number of corporate espionages in the workplace (Chan, 2003). However, not surprisingly, the findings were concentrated on that the potential risks strengthened internal control mechanisms but also damaged the environment of mutual trust in the workplace.

Apart from the majority of research, investigating the precautions to be taken against corporate espionage attacks (Brown 2011; Budiono and Sawitri 2017; Podszywalow 2012; Schafer and Karlins 2021; Bressler and Bressler 2015), Fitzpatrick et al. (2004) examined the legal rights and remedies that companies have to protect against trade secret piracy from their own personnel or business partners.

The majority of international espionage activities after World War II focused especially on economic and technological issues, due to the commercialization process of technology observed in the last quarter century. The strong correlation between countries' economic welfare and technological development ability has also led to similar results for commercial legal entities. It has been observed that global companies that do not bring adequate importance to innovation and R&D lose their production capabilities and commercial sustainability in the long run. However, some global companies that are aware of these challenges may choose different (sometimes illegal, sometimes unethical) methods in order to avoid their inadequacies and achieve their commercial goals faster and with a lower cost.

According to US defense industry reports, espionage attacks carried out by corporations or individuals to obtain data/information about target institutions constitute approximately 60% of the total suspicious activities among all espionage attempts. Besides, opponent state-sponsored espionage attacks, including military or intelligence agency activities, account for

only 21% of suspicious activities. Finally, espionage activities indirectly carried out by public organizations, including institutes, laboratories or universities, constitute the remaining 19% (Office of the National Counterintelligence Executive, 2001). As can be clearly seen from the statistical distribution above, the size and content of competition between global companies has evolved into a different appearance in the last quarter century. Moreover, the absolute necessity for strategic intelligence against rival companies at international competition, the unprecedented situation has created some new employment opportunities for intelligence officers who are experts on espionage (especially Eastern bloc career officers who left the labor market following the end of Cold War).

In another recently experienced incident, the conflict between two global giants in mobile communications (Samsung and Apple) caused confidential issues to become publicly discussing and subsequently the process to be referred to the court. The accusation in the documents submitted by Apple lawyers to the California District Court focus on Samsung officials gaining unauthorized access to the text of trade secret agreement between Apple and Nokia. The emergence of corporate espionage is as interesting as the incident itself; The words expressed by a Samsung official (Dr. Seungho Ahn) perhaps unintentionally, in a meeting with Nokia executives led to the outbreak of the scandal: "We know the details of licensing agreement you made with Apple" (Eaton, 2013). No one has yet provided a satisfactory explanation about how Samsung officials obtained this top-secret information.

The high-quality data and knowledge that emerge within the scope of companies' 'new product' research naturally cause them to be exposed to corporate espionage attacks. Such kind of espionage attacks may come from commercial/technological competitors or companies with strategic cooperation, or even from subsidiaries. Since intelligence practices that can be described as corporate espionage activities are generally carried out within legal limits, so there is no criminal sanction for the organizing party.

The methodology of corporate espionage activities (Altıntaş and Asal, 2021, p. 156) first begins with 'Open-Source Intelligence' studies. The process, which begins with the compilation of publicly available information (reports, fairs, social media, written and visual media, photographs, internet, etc.), offers the opportunity to collect low-cost and quite extensive data and information. Individuals of all ages and commercial legal entities in today's world, who tend to use all the opportunities of IT world, have transferred every moment of their lives and mostly their official information to virtual environment and share them in interaction with the

society. This provides an opportunity to access data/information far beyond what is thought, without incurring any costs, especially for malicious parties.

As seen in Figure 1 below, the second stage of the corporate espionage methodology is the immediate ‘Transfer of Executives’ of rival companies after they leave their workplaces. Ensuring an effective and fair competitive environment in global markets creates a situation that will be beneficial in the medium and long term for all parties involved, especially for customers. However, the intensive pressure of international competition on companies, the irresistibility of know-how accumulated by rival companies over the years, or the instinct to access confidential information about competitors' trade secrets can sometimes lead companies to prefer faster and more effective methods. Employing senior managers of competing companies operating in the same industry, while remaining within legal limits, appears to be an extremely valid method for corporations. Although it is not an illegal alternative, unfortunately global companies often resort to this method, in which moral rules are disregarded and conflict of interest between institutions becomes inevitable. Long-term job experience in the sector and comprehensive knowledge of operations of the company naturally increases the attractiveness of these types of managers. In recent years, global companies have generally made their senior managers sign a 'Non-Compete Agreement', so that the resigned manager cannot establish a rival company or get a job in a competitor corporation, or legally prevented from entering into any relationship with rival companies. The fact that employees who were in possession of customer network or production/trade secrets during their employment, 'changing side' for various reasons reveals perhaps one of the easiest but most effective methods of corporate espionage.

"Persuading" a senior manager working in a small technology-based company to leave the job and take all the company's know-how with him when transferring to a rival company is a standard type of corporate espionage that is often observed. In 1993, GM-Opel manager (Ignasio Lopez) transferred to VW company with a group of friends, but in the meantime, he took some confidential trade secrets (data/information regarding with the automotive design) with him. Thereafter, when VW realized the negative tendency of multibillion-dollar compensation lawsuits filed against him, VW agreed to pay GM-Opel $100 million and order spare parts worth $1 billion. Besides, in 2010, the US-based hotel giant Starwood accused Hilton, one of its most important competitors in the sector, of stealing documents containing sensitive information about the luxury segment (Worldwide) hotel concept. When the former Starwood senior manager (Ron Klein) hired by Hilton, took with him a storehouse of trade

secrets (more than 100.000 electronic files), he could not avoid being accused of unfair competition by Starwood.

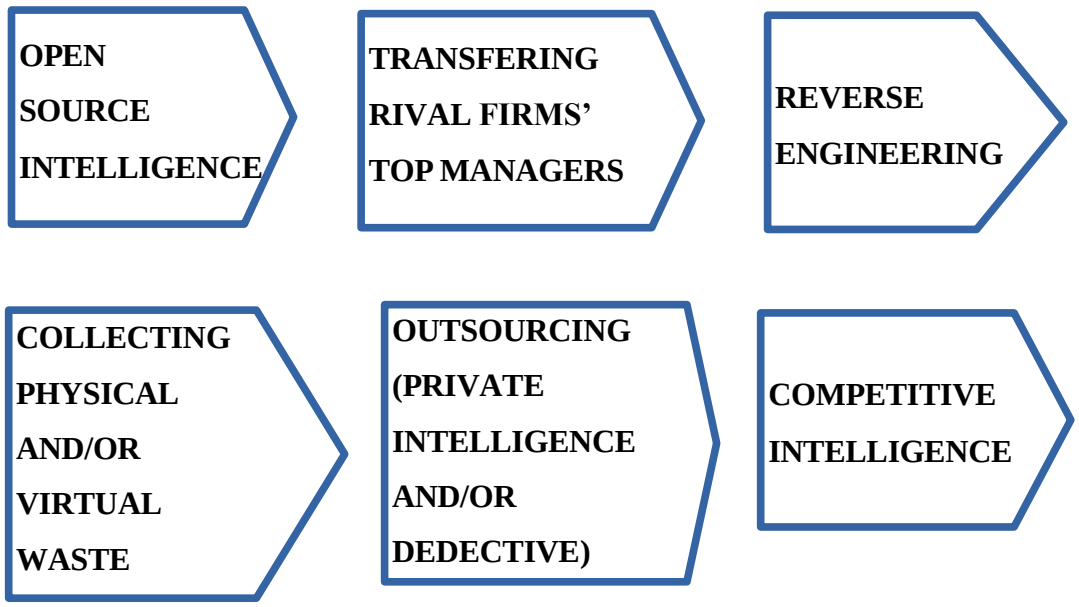

Figure 1: The Fundamentals of Corporate Espionage Methodology

The third stage of the corporate espionage methodology involves a method simply referred to as 'Reverse Engineering'. Reverse engineering refers to the technical decomposition of products, which are generally accepted by consumers, into sub-units by companies whose technological competence is not developed, and re-updating them with different methods. In this method, by going backwards in the production process, the process is completely analyzed, rival companies' popular products are deciphered and can be re-introduced to the market by making minor changes or by creating different brand names. Reverse engineering research can enable companies to achieve a certain sales success in the short and medium term, without great effort and without significant R&D expenditure, with limited similarity in terms of quality to the copied product, but within the framework of a low-sales price policy. For instance, it is claimed that Chinese Chengdu J-20 fighter jet was developed in light of data and information obtained through 'Reverse Engineering' from US F-117 Nighthawk stealth, which was shot down in Serbia in 1999 (Vashist and Kumar, 2013, p. 1).

The fourth stage of the corporate espionage methodology is the 'Collection of Virtual and Physical Waste' of rival companies in order to conduct comprehensive analysis. The content of these method is the secret collection of wastes/garbage that have been put out of use by employees of rival companies, but whose physical integrity or quality has not been lost, for the

purpose of comprehensive analysis. This method can provide extremely useful findings in terms of determining the present activities, strategies or current situations of rival companies. Examples of these wastes/garbage are pieces of paper whose integrity is intact or partially damaged, post-its, CDs, USBs, documents that may contain critical data/information, notebooks, prototypes, undestroyed drawings, samples, plans, aircraft tickets, appointment books etc. In addition, for example, during a business trip to a rival company, inferring various meanings from some physical objects within the facility or analysis of hierarchical relationships/communication between employees may obtain valuable inputs for decision makers. Besides, the widespread usage of mobile communication devices as well as portable computers/tablets in daily human life creates precious opportunities for corporate espionage attacks. For instance; decisions such as donating outdated computers to switch them with new ones or replacing broken mobile phones with new ones, even delivering these types of electronic tools to mechanic store for repairment, can create serious security vulnerabilities and may give direct access to virtual waste of used devices.

In 1978, a competitor of Tennant Co. namely Advances Machine Company, located in Oakland-California, seized carbon papers thrown into a trash bin in the office environment by the secretaries of Tennant company. The carbon papers placed between the typed papers contained information about the product sales prices that would be offered to prospective customers of Tennant Co. The fact that carbon papers can be easily read by holding them up to light has provided a significant competitive advantage to the rival company. But Tennant Co. won the lawsuit it filed against its rival and the court ruled that Advances Machine Company to pay $500.000 (Altintas, 2021, p. 896).

The fifth stage of the corporate espionage methodology involves purchasing services from a ‘Private Intelligence/Detective Agency’ in order to obtain strategic data and information regarding the operation of target companies with the help of 'Outsourcing'. Private intelligence/detective agencies that work in line with the principles of confidentiality and security generally provide monitoring and surveillance services for rival companies or their employees within the framework of principle of collecting legal evidence. Global corporations often prefer outsourcing in activities that require special expertise, such as collecting data and information about rival companies or their employees. This is because, corporations want to give the impression that they are acting within legal limits, as well as they may not want to use their official personnel with existing employment contracts in such operations. Moreover, since it is an activity that requires professionalism (espionage), private intelligence/detective agencies

rented for a certain fee can also provide two-way services. In other words, the relevant agencies provide monitoring and surveillance services for rival companies, as well as the protection of the existing company against industrial/corporate espionage attacks that may come from competitors.

The disclosure that Oracle-CEO (Larry Ellison) paid money to a detective company (Investigative Group International) to obtain the office garbage and virtual waste of Microsoft employees in 2000 is another true-life example of this issue (Miller et al., 2000). Such initiatives taken by the majority of global companies to gain competitive advantage, especially in production and sales development activities can easily reveal the strengths or weaknesses of rival companies at their business operations. Besides, the corporate espionage crisis between Japanese electrical giant Hitachi and US-based IBM began in 1981, when Hitachi senior executives (Kenji Hayashi and Isao Ohnishi) paid $648.000 to an intermediary (actually a spy of a Private Intelligence/Detective Agency) to steal technical data/information from their computers and some other documents. During the case that was brought to court, completely by chance, it was revealed that Mitsubishi Electric was also conducting research on IBM for similar purposes, and the relevant company was also included in the ongoing legal investigation process.

The sixth and final stage of the corporate espionage methodology, which we can briefly summarize as 'Competitive Intelligence', consists of compiling and then analyzing all information in open sources belonging to the competitor/target company. Commercial legal entities are often instinctively curious about the confidential information and documents of rival/target organizations and naturally want to seize them. In as much as having the confidential commercial or technological information of rival organizations means rising to a superior position in national/international competition. Finally, we can briefly define competitive intelligence as ‘the comprehensive analysis resulting from all kinds of raw data, information and documents collected from open sources regarding rival companies that provided within ethical rules and legal limits. In order to increase the efficiency in strategic decision-making processes, transforming data and information as an input to intelligence product after final analysis is an extremely useful strategy and/or policy determination tool for the senior management.

Competitive intelligence traces back to the 1600s. Working as an agent of the British East India Company, RL Wickham was sent to China to gather intelligence. He researched the local importance and potential of the tea plant. Aiming to contribute to the British economy,

Wickham analyzed China's tea production for ten years and later, the foundations of a tea industry were laid in England (Breed, 1999). The data-information-intelligence process is thought to be a step-by-step process, but this does not always mean that these steps must be followed. For example, a 15% tax imposed by the USA on "bakery products" to European Union is an unconnected piece of data, but with a simple interpretation it turns into operational which is intelligence information. For Turkish manufacturers producing this product, this "simple information" is the key to entering the US bakery market; because there is no tax imposed by the US on the same product to Türkiye and Turkish products have gained a great competitive advantage in terms of price against EU products. As can be seen, this “simple information” that has a specific importance can be interpreted as “operational information”. This is intelligence (Koc, 2014, p. 23).

In the last half century, when 'Technological Cold War' is still intensely experienced, corporate/industrial espionage attacks that cause illegal technology transfer are becoming increasingly widespread, and it is generally not possible to compensate for damages caused. There is no doubt that private-looking companies that appear to be private enterprises but are affiliated with Chinese government behind the scenes are at least as active and dangerous as Chinese government. The political and military competition of Cold War between east and west has evolved into commercial and technological competition between their global companies today. Both the financial losses caused by corporate espionage attacks on global companies and the economic damages resulting from workforce decrease promote global companies, especially those engaged in high-tech production in developing countries, to take comprehensive precautions in line with the principles of CI.

Conclusion

For both developing and developed countries, commercial legal entities are institutions that are of vital importance for the macroeconomic welfare and socioeconomic development of countries. Nowadays, the technological and commercial know-how that companies have acquired by spending significant time, effort and money are frequently exposed to corporate espionage attacks from rival companies. The negative pressure that such kind of espionage attacks create on the commercial performance of global companies generally come up within the form of serious financial losses or economic damages due to workforce loss. This situation forces global companies, especially those engaged in high-technology-oriented production, to take strategic precautions to protect their technological know-how. Therefore, nowadays, private/public enterprises are obliged to protect their sensitive and unique data/information

against unauthorized access, with respect to the basic principles of CI. The precautions to be taken are the most strategic requirement of companies' commercial and financial sustainability and the core guarantee of their economic security.

As has been illustrated in detail before, not only companies from Western and economically prosperous countries (US or Western Europe) with advanced technology, but also companies from developing countries (Taiwan, Türkiye, etc.) that engage in high-technology-oriented production can also be exposed to corporate espionage attacks. For this reason, the organizational structures of all companies, without exception, that engage in technology-oriented production should be reconstructed parallel with Corporate-CI principles and the basics of CI philosophy should be integrated into the company cultures. Moreover, this strategic approach should cover not only large companies operating on a global scale, but also SMEs with growth potential.

The first stage of the model developed regarding the fundamental methodology of corporate espionage attacks carried out completely within legal limits is the production of Open Source Intelligence. In the second stage of the model, the Recruitment (Transferring) of Rival Company Executives after their employment contracts is terminated, and in the third stage, Reverse Engineering studies take place. In the fourth stage of the model, there is the Collection of Physical and Virtual Waste of rival companies, and in the fifth stage, there are corporate espionage attacks carried out by purchasing Outsourcing services with the help of private intelligence/detective agencies. Finally, in the sixth and final stage, Competitive Intelligence production takes place comprehensively.

The extent to the information and communication technologies have reached today has turned individual to a dependent of virtual world, and social media platforms have further promoted the flow of this tendency. This new situation for individuals has not made any difference for companies; even data and information that can be considered confidential for companies have been shared in detail in the cyber world in order to reach a wider customer community. In this process, open source intelligence production for rival companies and various markets has reached such levels that it has almost overshadowed corporate espionage activities. For this reason, global companies should act more 'sensitive and discreet' about the data and information they share in the virtual environment, thus they prevent from the possible manipulations and avoid from the formation of various intelligence vulnerabilities. Operations Security, a prediction tool that allows to estimate the rival companies’ tactical policies and strategic plans, if is not taken into account sufficiently, companies' commercial performances

and financial returns are negatively affected certainly. When the 'bits of data and information' shared with the public without carefully contemplated or aware of details even in good faith are brought together as a result of patient analysis, the 'big picture' clearly emerges and a proactive defense or attack strategy can be developed by rival companies easily. Such kind of operations, which create a very useful basis for corporate espionage attacks, can only be eliminated by informing and raising the awareness of companies and their personnel.

Strategically important corporate espionage attacks are a serious source of threat, especially for companies operating on a global scale, but these initiatives also contain serious opportunities. Therefore, the ideal strategy for companies is, on the one hand, to protect their technological know-how against corporate espionage attacks in line with the CI principles, and on the other hand, not to ignore the extraordinary gains of corporate espionage by remaining within legal limits.

REFERENCES

Almeling, D. (2012). Seven reasons why trade secrets are increasingly important. Berkeley Technology Law Journal, 27(2), 1091–1118.

Almeling, D. S., W. Snyder, D., Sapoznikow, M., E. McCollum, W., & Weader, J. (2010). A statistical analysis of trade secret litigation in state courts. Gonzaga Law Review, 46(1), 57–101.

Altıntaş, K. M. (2021). İstihbarata karşı koyma prensipleri bakımından atik istihbaratının stratejik önemi ve karşılaştırmalı analizi. Uluslararası Kriz Ve Siyaset Araştırmaları Dergisi, 5(2), 879–914.

Altıntaş, K. M. ve Asal, S. 2021. Ekonomik İstihbarat Kapsamında Endüstriyel Casusluk. ISBN 978-625-400-286-1, Nobel Academic Publishing. 5th. Edition. Ankara.

Baker McKenzie. (2017). The Board Ultimatum: Protect and Preserve (The Rising Importance of Safeguarding Trade Secrets). https://www.bakermckenzie.com/-/media/files/insight/publications/2017/trade-secrets

Barnes, J. E. (2001, September 7). P.& G. Said to Agree to Pay Unilever $10 Million in Spying Case. The New York Times. https://www.nytimes.com/2001/09/07/business/p-g-said-to-agree-to-pay-unilever-10-million-in-spying-case.html

Billand, P., Bravard, C., Chakrabarti, S., & Sarangi, S. (2009). Corporate Espionage (SSRN Scholarly Paper 1430908). https://doi.org/10.2139/ssrn.1430908

Bless, C., Higson-Smith, C., & Sithole, S. L. (2013). Fundamentals of social research Methods.

Breed, T. 1999. Tea consumers, tea trade, and colonial cultivation. Accessed 10 November, 2023, https://vdocuments.mx/tea-consumers-tea-trade-and-colonial-cultivation-consumers-tea-tradetea-consumers.html?page=1.

Bressler, M. S., & Bressler, L. (2015). Protecting your company's intellectual property assets from cyber-espionage. Journal of Legal, Ethical and Regulatory Issues, 18(1).

Brown, A., & Brown, D. O. H. P. A. (2011). The Grey line: Modern Corporate Espionage & Counter Intelligence. Createspace Independent Publishing Platform.

Budiono, G. L., & Sawitri, N. N. (2017). Strategic Business Espionage: an ethics and business practices to gain opportunity or community problems. Studies in Business and Economics, 12(1), 29–39. https://doi.org/10.1515/sbe-2017-0003

Burgess, C., & Power, R. (2008). Secrets stolen, fortunes lost: Preventing intellectual property theft and economic espionage in the 21st (1st ed.). Syngress.

Chan, M. (2003). Corporate espionage and workplace trust/distrust. Journal of Business Ethics, 42(1), 45–58.

European Commission 2013. "Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade

secrets) against their unlawful acquisition". Accessed 29 August, 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0471.

Eaton, K. (2013). Samsung, Did You Have to Spy on Apple and Nokia's Licensing Deal? https://www.fastcompany.com/3019303/samsung-did-you-have-to-spy-on-apple-and-nokias-licensing-deal

Fink, S. (2002). Sticky fingers: Managing the Global Risk of Economic Espionage. Dearborn Trade.

Fitzpatrick, W. M., DiLullo, S. A., & Burke, D. R. (2004). Trade secret piracy and protection: Corporate espionage, corporate security and the law. Advances in Competitiveness Research, 12(1), 57–72.

Glitz, A., & Meyersson, E. (2017). Industrial espionage and productivity. Social Science Research Network. https://doi.org/10.2139/ssrn.3003864.

Gönültaş, B. (2018). Internet espionage cost German companies $50.5 billion. Anadolu Agency. Accessed 21 July, 2023. https://www.aa.com.tr/tr/dunya/internet-casuslugualman sirketlerine -50-5-milyar-dolara-mal-oldu-/1253821.

Javers, E. (2011). Secrets and Lies: The Rise of Corporate Espionage in a Global Economy. Georgetown Journal of International Affairs, 12(1), 53–60.

Kellett, A. (2015). Trends and Future Directions in Data Security. Vormetric Insider Threat Technical Report. Vormetric Data Security.

Koc, Yaman. 2014. Dış Ticaret İstihbarat Kanalları. İstanbul Sanayi Odası. Yayın No 6.

Lippoldt, D. C., & Schultz, M. F. (2010) Uncovering Trade Secrets—An Empirical Assessment of Economic Implications of Protection for Undisclosed Data (OECD Trade Policy Papers 167; OECD Trade Policy Papers, Vol. 167). (2014). https://doi.org/10.1787/5jxzl5w3j3s6-en

Lyakhovich, E. V. (2019). Chinese porcelain interpretation in Europe: History of Chinese and European porcelain cultures relationships. Proceedings of the 3rd International Conference on Art Studies: Science, Experience, Education (ICASSEE 2019). https://doi.org/10.2991/icassee-19.2019.10

Mashingaidze, S. (2015). Corporate espionage masquerading as business intelligence in local banks: A descriptive cross-sectional research. Corporate Ownership and Control, 12(4), 653–659. https://doi.org/10.22495/cocv12i4c6p5

Dunn, G. M. A., & Jr, J. S. (2000, June 29). Oracle Defends Its Spying on Microsoft as "Public Service." Los Angeles Times. https://www.latimes.com/archives/la-xpm-2000-jun-29-fi-45932-story.html

Miller, S. (2018, January 17). 2017 U.S. State of Cybercrime Highlights. Retrieved December 7, 2023, from https://insights.sei.cmu.edu/blog/2017-us-state-of-cybercrime-highlights/.

Office of the National Counterintelligence Executive. (2001). "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage". Accessed 13 September, 2023, https://irp.fas.org/ops/ci/docs/fy01.pdf.

PricewaterhouseCoopers. 2014. "Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats". The Center for Responsible Enterprise and Trade. February. Accessed August, 14, 2023. https://www.innovation-asset.com/hubfs/blog-files/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf.

PricewaterhouseCoopers. (2016). Global economic crime survey 2016: Adjusting the lens on economic crime preparation brings opportunity back into focus. In PWC. PwC Group. Accessed December 1, 2023, from https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

Podszywalow, M. (2012). Risk Management Magazine—Preventing Corporate Espionage. Magazine. https://www.rmmagazine.com/articles/article/2012/03/01/-Preventing-Corporate-Espionage-

Rothke, B. (2001). Corporate espionage and what can be done to prevent it. Informtion Systems Security, 10(5), 1–7. https://doi.org/10.1201/1086/43315.10.5.20011101/31716.3

Rodgers G. Marrs S. D. (2004). Trade Secrets and Corporate Espionage: Protecting Your Company's Crown Jewels, Acc Docket. Apr., 60-62.

Salaria, N. (2009). Meaning of the term-descriptive survey research method. International Journal of Transformations in Business Management, 2(2).

Sandberg, J. (2015). Human Element of Corporate Espionage Risk Management – Literature Review on Assessment and Control of Outsider and Insider Threats [Master Thesis]. University of Tampere.

Schafer, J., & Karlins, M. (2021). Hacked by Bits and Pieces: What Can We Learn from an Example of Corporate Espionage? Journal of Information Security, 12(03), 224–231. https://doi.org/10.4236/jis.2021.123012

Schumpeter, Joseph. (1970). Das wesen des geldes. Neuauflage, Göttingen, Germany: Vandenhoeck & Ruprecht.

Scott, C. (2021). Corporate Espionage by Drone: Why corporations need better physical and legal protections. Social Science Research Network. https://doi.org/10.2139/ssrn.3772434

Trzeciak, R. F. (2017). "SEI Cyber Minute: Insider Threats". Accessed 16 August, 2023. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=496626.

Vashisth, A., & Kumar, A. (2013). Corporate Espionage. Business Information Review, 30(2), 83–90. https://doi.org/10.1177/0266382113491816

Winkler, I. (1999). Corporate Espionage: What it Is, why it is Happening in Your Company, what You Must Do about it. Prima Lifestyles.

World Association of Intellectual Property-WIPO (2018). "What Qualifies as a Trade Secret". Accessed 28 August, 2023. https://www.wipo.int/tradesecrets/en.