Comparative Analysis of Strategic Relationship between Industrial versus Corporate Espionage within the Framework of Implementation Methods

Kadir Murat Altintas

Abstract

In the last 30 years, widespread illegal science and technology transfer, physical or cyberattacks on companies' trade secrets and intellectual property can cause serious damage to corporations. The effectiveness of precaution to be taken largely depends on accurate perception of these attacks and deciphering the sources of their motivation. The aim of this study is to comparatively analyse and model the relationship between industrial versus corporate espionage attempts for the purpose of legal/illegal technology transfer in terms of structural differences and implementation methods. Related concepts are explained through "Industrial-Corporate Espionage Pyramid" which is defined by Altintas, as well as evaluating alternative implementation methods of espionage activities. The choice that companies initially need to make is whether to carry out espionage activities within legal boundaries or not. Companies have to decide whether they will outsource espionage activities or will be carried out by using in-house sources.

Keywords: intelligence, industrial espionage, corporate espionage, corporate spying, cyberattack

Análisis comparativo de la relación estratégica entre el espionaje industrial versus el espionaje corporativo en el marco de los métodos de implementación

Resumen

En los últimos 30 años, la transferencia ilegal generalizada de ciencia y tecnología, los ataques físicos o cibernéticos a los secretos comerciales y la propiedad intelectual de las empresas pueden causar graves daños a las empresas. La eficacia de las precauciones a tomar depende en gran medida de la percepción precisa de estos ataques y de descifrar las fuentes de su motivación. El objetivo de este estudio es analizar y modelar comparativamente la relación entre los

 doi: 10.18278/gsis.6.1.5

intentos de espionaje industrial versus empresarial con el propósito de transferencia de tecnología legal / ilegal en términos de diferencias estructurales y métodos de implementación. Los conceptos relacionados se explican a través de la "Pirámide de Espionaje Industrial-Corporativo" que define Altintas, así como también se evalúan los métodos alternativos de implementación de las actividades de espionaje. La elección que las empresas deben tomar inicialmente es si realizar actividades de espionaje dentro de los límites legales o no. Las empresas deben decidir si subcontratarán las actividades de espionaje o se llevarán a cabo utilizando fuentes internas.

Palabras clave: inteligencia, espionaje industrial, espionaje corporativo, espionaje corporativo, ciberataque

执行方法框架下商业和企业间谍活动之间的战略关系比较分析

摘要

过去30年里，广泛的非法科学转移和技术转移、公司贸易机密和知识产权遭受的物理攻击或网络攻击，能对企业造成严重损失。预防措施的有效性很大程度上取决于对这些攻击的准确感知和破解攻击动机的来源。本研究旨在从结构差异和执行手段两方面比较分析商业间谍活动和企业间谍活动（这些间谍活动企图完成合法/非法技术转移）之间的关系，并对该关系进行建模。通过由学者Altintas定义的 “商业-企业间谍活动金字塔”，并评价间谍活动的替代性执行方法，对相关概念加以解释。是否在法律限制内开展间谍活动，这是公司最初需要做的选择。公司须决定其是否将间谍活动外包，或者用公司内部来源开展间谍活动。

关键词：情报，商业间谍活动，企业间谍活动，企业间谍行为，网络攻击

Introduction

Since the early 1970s, technology-based globalization movements in the world have gained spectacular momentum and the period of commercialization of technology, which means the transformation of information into technology and then commercial products or export commodities, has started. In this period, transforming innovative ideas and competitive meth-

ods into a commercial value belongs to countries and companies that can allocate their vast amount of resources into Research and Development (R&D) programs.

The accelerating effect of information technologies on economic globalization has contributed to the digital revolution and technological innovations that create the information age are generally produced by multinational companies in developed economies. However, information technology systems and infrastructures created by private companies have been exposed to threats, such as highly effective data/information theft of technological accumulation in the past few decades. At this point, a new strategic concept appeared on the agenda of relevant literature: Technology and Information Security.

Particularly, large-scale global companies in the last two decades are exposed to industrial and corporate espionage attacks (by targeting confidential data and information or by stealing intellectual property) from rival firms with the occasional help of government support. According to European Union Commission (2016), every year industrial and corporate espionage attacks can cause billions of euros in losses to companies. Moreover, public intelligence authorities have evolved into invisible stakeholders of national companies and have started working in cooperation and coordination towards their common goal of national and economic security in recent years. Large scale companies operating on a global environment have also started to outsource espionage services to private intelligence companies.

The aim of this study is to comparatively analyse and model the relationship between industrial versus corporate espionage attempts for the purpose of legal/illegal science and technology transfer in terms of structural differences and implementation processes. Theoretical and functional scope of related concepts is explained through "Industrial-Corporate Espionage Pyramid," which is defined by Altintas and also called "Altintas Pyramid," as well as comparatively evaluating alternative implementation methods of industrial and corporate espionage attempts. Another important purpose of this study is to contribute to the awareness of corporate top management about cyber and physical industrial/corporate espionage attacks.

The Importance of Industrial versus Corporate Espionage within the Conceptual Framework

Since the first half of 1980s, neoliberal economic model and deregulation policies were widely accepted by most of the economies and financial markets. The subsequent dissolution of the Union of Soviet Socialist Republics and the termination of Cold War caused concepts such as investment and privatization to become more popular. In addition, the widespread usage of mobile communication devices as well as portable computers and tablets, intelligence activities among countries

and companies increased exponentially all around the world. As a result, security has become the major issue of both individuals and institutions that have innovative skills and technological knowledge within this framework of espionage attacks together with covert economic operations.

However, information technology systems and infrastructures invented by corporations have been exposed to threats (such as trade secret theft together with intellectual property stealing). For this reason, large-scale global companies had to protect all digitalized assets and know-how accumulation produced as a result of enormous R&D activities and expenses. At this point, a new strategic concept appeared on the literature: Technology and Information Security.

Every year, high-quality industrial data and information as well as confidential documents are stolen by rival firms, through industrial espionage or corporate spying attacks organized by competitors, intelligence agencies of competitor states, disgruntled employees or shareholders. Technical infrastructures related to R&D and new product technologies as well as engineering processes of large-scale global companies are under serious threat.

Misappropriation or theft of trade secrets and corporate espionage threaten innovation, growth development and investment of business entities and national economy globally (OECD, 2016). Trade secret theft is one of the main factors that cause billions of dollars in annual losses to business entities and the national economy (PricewaterhouseCoopers, 2014). Trade secret is a gold nugget that determines the success and survival of a business entity. It provides a business entity with a competitive advantage over its rival. However protecting a trade secret is not an easy task especially from current and former employees as well as from competitors. The task is made difficult with the availability of technological devises that can be used to steal the information from inside and outside of the business organization (Jalil and Hassan 2020, 205).

The content of industrial and corporate espionage activities carried out in recent years has focused largely on economic and financial issues. At this point, it is more favourable to explain conceptual differences between industrial and corporate espionage by clarifying the juridical boundaries and the distinction between implementation procedures. Though are quite similar definitions between these two concepts, it is possible to describe industrial espionage as the activity of acquiring trade secrets or intellectual property through illegal attempts. Corporate espionage generally considered to be within legal limits (yet unethical), will provide economic and financial advantages to private enterprises in market competition.

Industrial espionage is carried out in a veiled and deceptive manner by private companies acting on their behalf. Obtaining economic intelligence using secret and illegal tools by the private sector is called industrial espionage (Porteus 1994, 737). It does

not cover the activities of private entities without the involvement of foreign governments, nor does it relate to legal efforts to obtain commercially useful information from internet. Some open source gathering efforts are not covered by industrial espionage, although they may be a precursor to future covert activities. Some countries have a long history of ties between government and industry. However, it is often difficult to ascertain whether espionage has been committed under foreign government sponsorship (Nasheri 2005, 13). In 2020, large-scale global companies due to fierce commercial and technological competition, it appears to bring corporations closer to the *sweet poison* of industrial espionage unfortunately. The goals and expectations of companies from espionage attempts are to:

1) Gain competitive advantage and prestige in their respective industries,

2) Save costs, particularly from R&D expenses,

3) Decrease the credibility of competitors in the industry,

4) Increase the efficiency of intercompany decision-making processes.

Finally, industrial espionage is an illegal initiative and process that is carried out to obtain confidential data and information as well as commercial/technological secrets related to rival firms or their employees which cannot be obtained by open source intelligence in order to gain absolute advantage.

However, corporate espionage (spying), defined as outsiders penetrating corporate offices or networks, and can be very damaging (Horan 2000, 29-30). These types of attacks could be described as illegal and unethical activities undertaken by organizations to systematically gather, analyse and manage information on competitors with the purpose of gaining a competitive edge in the market (Vashisth and Kumar 2013, 83), in other words it may arise due to unfair competition among firms (Vimmer 2015, 26). Corporate espionage sometimes referred to as industrial espionage, corporate spying, or economic espionage, has become a multibillion dollar industry. The exact dollar figure on the costs of corporate espionage is difficult to determine and many thefts of proprietary information go undetected and unreported. Even when espionage is discovered by an employer, the scale and impact of the breach often cannot be determined. Government studies have estimated the annual loss to businesses due to corporate espionage to be as much as hundreds billions of dollars (Koen and London 2019, 331). Corporate espionage is also used to examine products or ingredients for perceived or actual risks, to time markets, and to establish pricing. All too commonly, companies find themselves the targets of such activity without the knowledge or methodology to effectively counter it (Rothke 2001, 1). In case of evidence of an existence of foreign government or involvement of a hostile spying, companies involved in such illegal activities are subject to legal prosecution. Factors that determine the legal limits of corpo-

rate espionage attempts are also closely related with the degree of economic damage sustained to the owner of trade secrets or intellectual property and the deterrent potential of the prosecution.

The cases involving trade secret theft from Lucent Technologies, IDEXX and Avery Dennison demonstrate (1) how devious employees can use the naiveté of other personnel and the firm's computer infrastructure to support their corporate espionage activities; and (2) that corporate recognition of these security breaches occurred only after their technologies had been transferred to competitors (Fitzpatrick 2004, 66). The strategic importance of industrial espionage initiatives carried out for corporations operating on a global scale is becoming more and more remarkable in recent years. Moreover, within this phase, public intelligence authorities have transformed into invisible stakeholders of their national companies and have started to work in cooperation/coordination towards mutual economic security objectives.

Corporate and industrial espionage might occur at corporations as soon as other actors have competing interests. This makes everyone with competing interests a potential spy. However, if a corporation wishes to limit the possible impact of espionage, relatively simple mitigating measures might help. The first step is acknowledging that espionage might happen and that the corporation is a potential target. The second step is a risk analysis which identifies critical means and processes and their vulnerabilities. Based upon this awareness and risk analysis, the corporation can develop policies for whom to allow access to confidential corporate information. Restraint in allowing access is in place here. Authorization to access confidential information should only be granted after no restrictions were found during a screening process. Still, theft of confidential corporate information cannot be fully excluded. Therefore, also a need exists to prepare for situations in which espionage actually has occurred. In order to create resilience after espionage, corporations need to develop contingency plans in advance, and conduct damage assessments and improve mitigating measures to avoid future espionage afterwards (Ijzerman and Berge 2019, 1).

As a result, there is a strategic relationship between industrial and corporate espionage initiative in terms of implementation procedures. The linkage between industrial and corporate espionage is closely related with the strategic decisions (conducting espionage activities within the boundaries of the legislations or not) to be made by the company's senior management. Corporate espionage attempts may fall within legal limits compared to illegal (sometimes publicly sponsored) industrial espionage attacks. However, espionage attacks carried out to obtain confidential data and information against competitors or their employees are considered as criminal offense when they go beyond the legal boundaries.

The Anatomy of Industrial and Corporate Espionage Attacks

The source of threat from espionage attacks can be evaluated under two main headings:

A. Internal Threat: In brief, the insider includes current or former employee, business partner or contractor. The information age makes it possible for all level of employees including business partners to gain access to volumes of data and pose a significant security risk. The case of Edward Snowden provides a good example of insider threat. According to Software Engineering Institute at Carniege Melon University, insiders can pose a considerable threat to the organization. This is because the insiders know and are aware of the organization's policies, procedures and technology and they also know the vulnerabilities of the organization. They can bypass the security measures using their knowledge and access to the company's proprietary systems. In this regard, insiders have a significant advantage over outsiders or external attackers. Such threat from insiders is therefore real and could be substantial. Thus to prevent harm to the company or organization assets, focus should not only be made to external-facing security mechanisms, such as firewalls, intrusion detection systems, and electronic building access systems, but also to include insiders as potential threats (Jalil and Hassan 2020, 208).

In 2016, a survey conducted by the U.S. State of Cybercrime found that 27% of electronic crimes were suspected or known to be caused by insiders and the insider attacks caused more severe damage than caused by outsider attacks (U.S. of Cybercrime, 2016). According to a Statistical Analysis of Trade Secret Litigation in the U.S. Federal Courts, 85% of the trade secret lawsuits in the state and federal courts of the U.S. found that the alleged misappropriator was either an employee or a business partner (Almeling et al., 2010, 59). In 2016, a survey conducted by IBM estimated that employees and other malicious or careless insiders accounted for 60% of cyber-attacks from unauthorized access, viruses or other malicious code, "phishing" attempts and other means (IBM X-Force Research, 2016).

The nature of insider threats is different from other cybersecurity challenges; these threats require a different strategy for preventing and addressing them. An insider threat is anonymous and difficult to identify but a clue could be derived from the definition of malicious insider threat. Such threat refers to "a current or former employee, contractor or other business partner who has or had authorized access to an organization's network, system or data and intentionally misused that access in a manner that negatively affected the confidentiality, integrity or availability of the organization's information or information systems." In addition, insider threats can also be unintentional (non-malicious) (The CERT Division Insider Threat Centre 2016, 2-3).

B. External Threat: This category includes competitor, hacktivist, foreign government and organized crime. The

act of these threat actors could also be associated with data breach and data leakage through computer system, intrusion of detection system and electronic building access system. According to Almeling (2010), there are increased threats from foreign individuals, companies and government due to three factors namely internationalization of business, access to technology that allows hackers to access trade secrets from anywhere in the world and that some countries viewed stealing of trade secrets as an aid to development (Almeling et al., 2010, 62).

Attacks on trade secrets and intellectual property, which are strategically important assets of companies, are usually caused by spies of hostile intelligence services, retired spies hired by competitors, private intelligence companies, unless they are caused by internal threats. Moreover, a rival company owned by a foreign government is also a significant threat in an industry segment. This method is generally applied by Chinese government that the rival company looks like a private company, but implicitly belongs to the government.

The need to access confidential data and information regarding trade secrets or intellectual property of competitors and the necessity to protect national companies against foreign industrial espionage and corporate spying attacks, without exception, increase the awareness of top management of corporations about intelligence gathering operations.

Some of the Sample Cases of Industrial versus Corporate Espionage Attacks

In recent years, espionage attacks have been frequently observed in uncontrolled areas such as commercial (technological) fairs, international airway travels, airport lounge or hotel accommodations-abroad. We should exemplify these attempts that intend to obtain confidential data and information of competitors as follows:

A copy of the German Transrapid train developed by engineers of Siemens and Thyssen-Krupp companies started operating in China under the name of CM1-Dolphin before the train started operating in Germany. Chinese intelligence acquired the technical characteristics of the train at the Shanghai Technology Fair in 2004. Additionally, American businessmen traveling to Europe for trade negotiations were cautioned in 1992 for travelling with French Airlines. Because the French Intelligence Service placed listening devices on the aircraft seats, and this was detected by CIA agents. Besides, hotel rooms with electronic cards are an extremely risky area as an uncontrolled zone. According to a news article titled "Hackers Lock Romantik Seehotel Jaegerwirt's Guests out of Their Rooms, Demand Bitcoin Ransom," in thebitcoinnews.com website published at January 30, 2017:

Hackers attacking critical IT infrastructure for Bitcoin ransom is not a new thing. It has been happening on a regular basis in the past couple of years. But attacking a hotel and locking

hundreds of guests out of their rooms probably never happened before last week. According to reports, one of the top European hotels, Romantik Seehotel Jaegerwirt in Austria became the target of cybercriminals. They managed to hack into the luxurious 4-star hotel's electronic key system, rendering it useless. While the hotel guests were unable to move in and out of their hotel rooms, the hackers demanded a ransom of over EUR 1500 in Bitcoin from hotel authorities. (Bilefsky 2017)

Apart from this, methodology of corporate espionage activities depend mostly on obtaining confidential data and information that belongs to rival firms within the legal limits. For instance, obtaining information from the executives of competitors under job interviews, hiring detective to spy on and evaluate the selling process of rival companies, eavesdrop on communication at rival companies' facility trips, b2b cooperation meetings, at a commercial fair organizations, recruitment of rival company employees together with confidential documents after resigning or employing a detective to obtain the password of target computer by shoulder surfing or by pretexting. Some of experienced corporate espionage examples from bloomberg.com website recently:

Hewlett-Packard's board became ensnared in a scandal in 2006 after the company spied on its directors, reporters, and employees in a probe to ferret out the source of boardroom news leaks. Investigators hired by the company obtained personal phone records by posing as reporters and company directors. They also trawled through garbage and followed reporters. As a result, then-Chairman Patricia Dunn, who approved the spying, was fired. HP also agreed to pay $14.5 million to settle an investigation by California's attorney general, $6.3 million to settle shareholder lawsuits, and an undisclosed amount to settle a case filed by journalists at *The New York Times* and *Business Week*.

In April 2009, Starwood Hotels & Resorts Worldwide sued Hilton Hotels over trade secrets. Starwood had claimed two former Starwood executives hired by Hilton stole information about Starwood's W hotel brand to develop the Denizen line of properties. Ross Klein and Amar Lalvani were involved in developing Starwood's lifestyle and luxury hotels, including the St. Regis, W, and Luxury Collection brands, and downloaded confidential Starwood information to use later at Hilton, according to the complaint. In 2010, Starwood settled its case and said Hilton was ordered to make sure "the conduct that occurred does not occur again" (Beasley 2009).

Strategic relationship between industrial versus corporate espionage: Industrial-Corporate Espionage Pyramid

It is useful to classify industrial and corporate espionage implementation methods in two main categories. The main reason for this classification emerges from determining the

juridical boundaries of industrial and corporate espionage attacks. That is to say, the distinction is based on whether espionage attempts preferred by large-scale global companies will continue their covert operations within legal limits or to stray outside of legal boundaries. Confidential data and information gathering activities, that can be described as corporate espionage initiatives are generally carried out within legal limits, and commercial entities are not subject to any criminal sanctions about these types of attempts.

However, since industrial espionage attempts carried out against competitors beyond the legal boundaries, they usually involve activities that require experienced personnel. At that point, these types of attempts have to be executed either by recruiting expert personnel or purchasing outsourcing services. It is possible to elaborate general implementation procedures and preferences regarding industrial and corporate espionage activities through the Industrial-Corporate Espionage Pyramid defined firstly by Altintas, also called as Altintas Pyramid, (Figure 1).

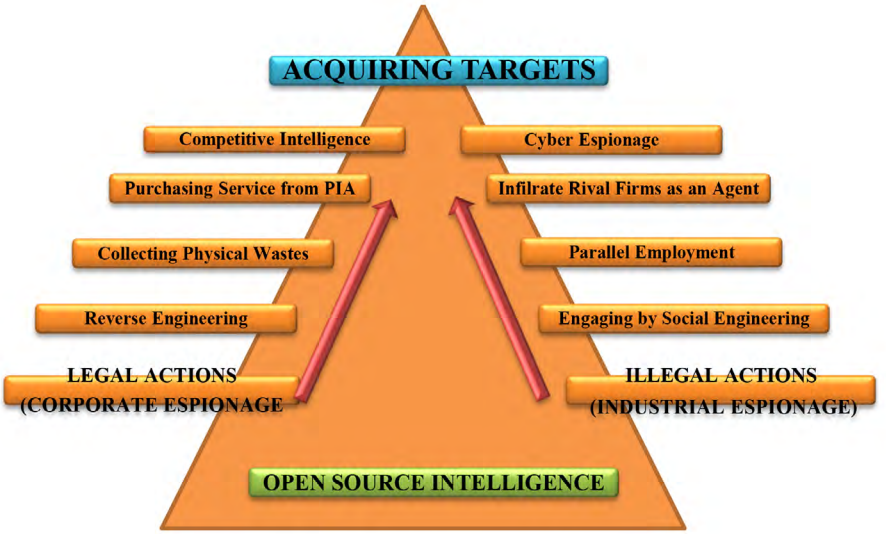

Figure 1: Industrial-Corporate Espionage Pyramid, also called as "Altintas Pyramid"

At the lowest stage of the Industrial-Corporate Espionage Pyramid, within the framework of **Open Source Intelligence** activities start with the priority to collect and analyse public information (reports, fairs, social media, print-visual media, photographs, internet, etc.). The next stages are determined by companies' strategic preference between industrial and corporate espionage attempts, in other words, companies should decide whether to stay within the legal boundaries or not.

In order to gain superiority over their rivals while staying within the legal boundaries, companies, as part of corporate espionage, may refer to a method called **Reverse Engineering.** Re-

verse engineering is the re-adaptation of products and is generally preferred by companies that do not have adequate technological competence. It involves disassembling competitors' product into detailed sub-units. In this method, by going backwards in the production process based on an existing product, the process is completely resolved, popular products of rivals are deciphered and easily can be re-introduced to the market with small differences and diversified brand names. Although there is limited resemblance to the original product in terms of quality, with little effort and without making significant R&D expenses, companies may reverse engineer a competitor's product and achieve certain sales advantage.

For instance—BGM-71 TOW missile (in May 1975), negotiations between Iran and Hughes Missile Systems on co-production of the TOW and Maverick missiles stalled over disagreements in the pricing structure, the subsequent 1979 revolution ending all plans for such co-production. Iran was later successful in reverse-engineering the missile and now produces its own copy, the Toophan. In other words, Toophan is an Iranian SACLOS anti-tank guided missile reverse-engineered from the American BGM-71 TOW missile. Moreover, Toophan 1, an unlicensed copy of the BGM-71A TOW missile, began mass production in 1988 (Defence Intelligence Agency, 1988).

Another way of obtaining confidential data and information about competitors is to **Collect Physical Wastes** for analysis**,** within the legal limits. The amount of physical waste, which has been left out of use by the rival employees', but whose physical integrity or quality has not been damaged, can be analysed and bring out extremely useful clues in terms of current activities, strategies and current situations of competitors. Examples of these wastes are; untainted or partially damaged pieces of paper, post-its, CDs, USBs, documents that may contain critical data and information, notebooks, prototypes, undestroyed drawings, samples, plans, plane tickets, appointment books, etc.

The surveillance and covert searches began a year ago, after officials at software giant Oracle Corp. became outraged that some industry groups were aggressively supporting its rival Microsoft Corp. in that firm's federal antitrust fight with the Justice Department. Oracle hired Washington-based Investigative Group International and told its private detectives to find documents that might be embarrassing to Microsoft. It was corporate hardball, and it was all supposed to remain secret. But yesterday, after a series of revelations about individuals' rifling through trash and offering cash to janitors, Oracle chief executive Larry Ellison publicly acknowledged that his company paid the detectives to prove the three groups were public relations fronts for his company's biggest competitor (*The Washington Post*, 2000).

Private Intelligence Agencies-PIA, working in line with the principles of confidentiality and trust, provide monitoring and surveillance services for competing companies within the framework of collecting evidence in

accordance with the law. In this sense, companies may prefer the method of outsourcing that require special expertise, such as collecting confidential data and information about competitors or their employees. Because companies generally want to pretend to be acting within legal limits, they may not want to use their official personnel in such espionage attempts. Private intelligence agencies that are hired for a certain fee can also provide double-sided service. That is, the relevant offices of companies not only provide tracking and surveillance services to companies, but also protect company against industrial and corporate espionage attacks from competitors.

Some private intelligence agencies use online perception management, social media influencing/manipulation campaigns, strategic disinformation (such as fake news production/propaganda production, opposition research and political campaigns using social media and artificial intelligence. Former anti-corruption prosecutor Aaron Sayne said private intelligence is "an industry that's largely undocumented and has very flexible ethical norms" as agencies collect and use sensitive information "for one purpose on day one and some completely contradictory purpose on day two" (Burgis 2017). The private intelligence industry has boomed due to shifts in how the U.S. government is conducting espionage in the War on Terror. Some $56 billion (USD) or 70% of the $80 billion national intelligence budget of the United States was in 2013 earmarked for the private sector according to *The New York Times*' Tim Shorrock. Functions previously performed by the CIA, NSA, and other intelligence agencies are now outsourced to private intelligence corporations (Abbot, 2013).

Besides, corporations generally want to obtain confidential data and information about competitors in order to be one step ahead at the international competition. In other words, they are always curious about competitors' customers, suppliers, personnel, organizational structure, environmental awareness, technical knowledge, stakeholders, status of their partners, legal relations and similar high quality data and information. Provided that it is completely within the ethical rules and legal limits, raw data and information about competitors are collected from public sources. It is also analysed for the senior management which is used as input at the strategic decision making processes, called **Competitive Intelligence.**

The airline industry is a great example of how competitive intelligence is being used in practice. Every day, airline companies are changing their flight ticket prices based on several pieces of external information. For instance, if all competitors increase their price for a certain route, a flight provider would quickly follow suit to secure higher margins. In addition, customer information is frequently used for pricing adjustments. By identifying and tracking specific users, flight companies can spot when a potential customer is repeatedly searching for the same flight details and increase the prices over time, since they

can be sure that they really want to fly on these dates (Kompyte, 2018).

Conversely, within the scope of illegal industrial espionage activities, such operations require a more qualified knowledge and ability. At that point, engaging competitor firms' employees through **Social Engineering** requires sufficient knowledge and experience, especially in the areas of intelligence and espionage. The concept of social engineering is expressed as the art of human deception, and can also be defined as obtaining unauthorized access to competitor systems by detecting the weak chain among their employees. Actually, social engineering is the activity of manipulating human inadequacies and emotions, using various methods of persuasion and deception against rival employees. In other words, social engineering operations that force rival company employees to make mistakes through the exploitation of human emotions such as fear, excitement, joy, loss of reputation and trust in the eyes of customers and society, make rival systems completely unusable. Large-scale global companies may sometimes turn to illegal ways to obtain confidential data and information as well as commercial/technological secrets related to competitors. In addition, misleading claims against competitors try to weaken the commercial success of competitors, especially in the virtual climate of social media where there is limited or even uncontrolled environment.

The biggest social engineering attack of all time was perpetrated by Lithuanian national Evaldas Rimasauskas against two of the world's biggest companies: Google and Facebook. Rimasauskas and his team set up a fake company, pretending to be a computer manufacturer that worked with Google and Facebook. Rimsauskas also set up bank accounts in the company's name. The scammers then sent phishing emails to specific Google and Facebook employees, invoicing them for goods and services that the manufacturer had genuinely provided—but directing them to deposit money into their fraudulent accounts. Between 2013 and 2015, Rimasauskas and his associates cheated the two tech giants out of over $100 million. Moreover, in March 2019, the CEO of a UK energy provider received a phone call from someone who sounded exactly like his boss. The call was so convincing that the CEO ended up transferring $243,000 to a Hungarian supplier—a bank accounts that actually belonged to a scammer (tessian.com Website).

Engaging rival companies' employees with criminal methods such as threat, wiretapping, blackmail, provocation, honey trap, in other words transforming them almost actual agents, are one of the most remarkable industrial espionage methods. In the organizations of large-scale companies, it is possible to employ retired members of armed forces or intelligence officers to engage rival employees working at critical position of competitor firms. The method that can be preferred for industrial espionage initiatives is to try to obtain confidential data and information from rival firms' employee by a certain fee or criminal procedures-also called as **Parallel Employment.** This method

aims to discover rival employees who have weaknesses particularly in fiscal matters, since money is the most important source of motivation for many people. It is an extremely easy and prevailing method. The initiation of an illegal financial relationship in terms of rival firms' employee means that he/she is going to be hired as a dual employer.

Pin Yen Yang and his daughter Hwei Chen Yang were arrested in Cleveland on September 5, 1997, and charged with mail fraud, wire fraud, money laundering, receipt of stolen property, and theft of trade secrets from Avery Dennison Corp. Avery Dennison is one of the largest U.S. manufacturers of adhesive products, including adhesives for such things as postage stamps, labels, and diaper tape. Pin Yen Yang is the President of Four Pillars Enterprise Company of Taiwan, which manufactures and sells pressure-sensitive products mainly in Taiwan, Malaysia, Singapore, People's Republic of China, and the United States. The company has more than 900 employees and annual revenues of more than $150 million. His daughter has a Ph.D. in analytical chemistry from New Mexico State University, was employed most recently by Four Pillars as an Applied Research Group Leader, and may hold dual citizenship in the U.S. and Taiwan. The Yangs were convicted in April 1999 of having paid an Avery Dennison employee in Ohio, Dr. Ten Hong Lee, between $150,000 and $160,000 for highly sensitive and valuable proprietary manufacturing information and research data over a period of approximately eight years from 1989 to 1997. Payments were reportedly made through Lee family members in Taiwan. Avery Dennison estimates that its direct costs for developing the stolen technology were in the tens of millions of dollars (U.S. Department of Commerce).

Agents (who have adequate intelligence expertise and professional knowledge) **Infiltrate or Pose Rival Companies** under different pretences. Technology transfers or intellectual property theft by covert economic operations that was performed by agents as a hidden "payroll employee" of competitor firms are the most effective and at the same time the most damaging method of industrial espionage. In addition, self-employed agents (usually people who have criminal background) can also be hired by companies to obtain confidential data and information on their own initiative and sell them to companies offering the highest amount of money.

Yanqing Ye, 29, a Chinese national, was charged in an indictment today with one count each of visa fraud, making false statements, acting as an agent of a foreign government and conspiracy. Ye is currently in China. According to the indictment, Ye is a Lieutenant of the People's Liberation Army (PLA), the armed forces of the People's Republic of China and member of the Chinese Communist Party (CCP). On her J-1 visa application, Ye falsely identified herself as a student and lied about her ongoing military service at the National University of Defence Technology (NUDT), a top military academy directed by the CCP. It is further alleged that while studying at

Boston University's (BU) Department of Physics, Chemistry and Biomedical Engineering from October 2017 to April 2019, Ye continued to work as a PLA Lieutenant completing numerous assignments from PLA officers such as conducting research, assessing U.S. military websites and sending U.S. documents and information to China. According to court documents, on April 20, 2019, federal officers interviewed Ye at Boston's Logan International Airport. During the interview, it is alleged that Ye falsely claimed that she had minimal contact with two NUDT professors who were high-ranking PLA officers. However, a search of Ye's electronic devices demonstrated that at the direction of one NUDT professor, who was a PLA Colonel, Ye had accessed U.S. military websites, researched U.S. military projects, and compiled information for the PLA on two U.S. scientists with expertise in robotics and computer science (U.S. Department of Justice).

Cyber Espionage, which has become a nightmare of companies in recent years, is now the most preferred method among espionage activities against large-scale, innovative, technology-based public/private enterprises. With almost zero cost, the intranet/internet infrastructure of the target company is affected from far away distances, and furthermore, the damages it causes can reach incredible dimensions compared to its cost. Cyber espionage is defined as the secret seizure of e-mail traffic, messages or all kinds of electronic communication facilities of competitors in order to collect confidential data and information.

Computer attacks on Google that the search giant said originated in China were part of a concerted political and corporate espionage effort that exploited security flaws in e-mail attachments to sneak into the networks of major financial, defence, and technology companies and research institutions in the United States, security experts said. At least 34 companies, including Yahoo, Symantec, Adobe, Northrop Grumman and Dow Chemical, were attacked, according to congressional and industry sources (Cha and Nakashima, 2010). Additionally, Google has discovered that the accounts of dozens of U.S. China and Europe-based Gmail users who are advocates of human rights in China appear to have been routinely accessed by third parties. These accounts have not been accessed through any security breach at Google, but most likely via phishing scams or malware placed on the users' computers (Google Official Blog, 2010). Internet giant Google has said it may end its operations in China following a "sophisticated and targeted" cyber-attack originating from the country. Although Google did not accuse Beijing directly, but said it was no longer willing to censor its Chinese search engine - google.cn. This could result in closing the site, and its Chinese offices, Google said (BBC News, 2010).

Conclusion

In recent years, attacks on companies' technological knowledge and experience, such as trade secrets or intellectual property, have been increasing. At the same time, these types of at-

tacks can cause serious damage to the economies of companies. The effectiveness of precautions taken in this regard largely depends on accurate perception of the content of these attacks and deciphering the sources of their motivation.

However, detailed analysis of structural differences and implementation methods among these types of attacks will also increase the awareness of senior management of corporations on defending valuable assets. Industrial and corporate espionage attempts should actually be evaluated from two perspectives; espionage attacks and counterintelligence. In other words, the strategies that companies choose to capture the desired confidential data and information will also increase the effectiveness of precautions that can be taken against such attacks.

Industrial-Corporate Espionage Pyramid models alternative implementation procedures of industrial and corporate espionage attacks as a whole. In this context, companies should make a strategic decision whether to stay within the legal limits or not. However, in all cases, companies must acquire the basic data and information with open source intelligence. Collecting physical wastes of competitors is another remarkable activity that requires proficiency. Reverse engineering and/or competitive intelligence activities are inter-company solutions for acquiring targets. Besides, companies that prefer to step outside of legal boundaries need expert contribution and sometimes require governmental assistance. Because illegal activities must necessitate adequate expertise on espionage, companies which do not prefer to outsource may opt for recruiting retired intelligence and/or military persons that have enough experience on engaging rival employees by social engineering. Moreover, engaging rival employees for parallel employment and infiltrating rival companies as an agents are extremely dangerous and illegal activities which could be accepted as serious crimes across multiple jurisdictions. Besides, cyber espionage attacks to rival firms also require adequate expertise; hence, they are generally outsourced to freelance hacker groups.

Companies can also choose to achieve their desired goals by outsourcing. This is an optimal decision in terms of performing a specialized activity for companies that do not want to be associated with such activities in front of public. Outsourcing these types of activities to a third party has some advantages together with serious disadvantages. Although inter-company labour sources are more reliable and manageable compared to outsourcing, due to superior expertise requirements, companies generally hire external actors for these types of activities.

Finally, the preference that companies initially face with is to carry out espionage activities within legal boundaries or not. In addition, companies have to answer the strategic question of whether espionage activities against competitors will be carried out by outsourcing or by making use of inter-company labour resources. In other words, these are the preliminary stages

that companies should answer in the process of acquiring targeted data and information within the framework of industrial versus corporate espionage activities.

Kadir Murat Altintas holds a PhD in Economics-Finance and an MS in Industrial Engineering. His primary area of research includes industrial espionage within the framework of economic intelligence as well as Chinese espionage system as part of their security infrastructure. Dr. Altintas's latest book is on "Industrial Espionage within the scope of Economic Intelligence: The Strategic Importance of Industrial Espionage for Commercial Entities" has been established at September 2020. He welcomes opportunities for continued research and collaboration.

References

Abbot, Sebastian. "The Outsourcing of U.S. Intelligence Analysis." *A Journalism Initiative of the Carnegie and Knight Foundations.* News 21 Project. Accessed January 28, 2021, from http://newsinitiative.org/story/2006/07/28/the_outsourcing_of_u_s_intelligence.

Almeling, David S., Darin W. Snyder, Michael Sapoznikow, Whitney E. McCollum, and Jill Weader. (2010). "A Statistical Analysis of Trade Secret Litigation in State Courts." *Gonzaga Law Review.* 46, 57-80, Accessed November 24, 2020. http://blogs.gonzaga.edu/gulawreview/files/2011/01/AlmelingSnyderSapoznikowMcCollumWeader.pdf.

BBC News. (2010). "Google 'may pull out of China after Gmail cyber-attack'." January 13 2010. Accessed January 28, 2021. http://news.bbc.co.uk/2/hi/business/8455712.stm.

Beasley, Deena. (2009). "Starwood sues Hilton, alleges corporate espionage." *Reuters*, 17 April 2009, https://www.reuters.com/article/us-starwood-hilton-idINTRE53G00220090417.

Bilefsky, Dan. (2017). "Hackers Use New Tactic at Austrian Hotel: Locking the Doors." *The New York Times,* 30 January 2017. https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html.

Bloomberg. (2011). "Famous Cases of Corporate Espionage." Accessed November 22, 2020. https://www.bloomberg.com/news/photo-essays/2011-09-20/famous-cases-of-corporate-espionage.

Budiono Gatut L. and Ni Nyoman Sawitri. 2017. "Strategic Business Espionage: An Ethics and Business Practices to Gain Opportunity or Community Problems." *Studies in Business and Economic.* Volume 12: Issue 1, 29-39. http://doi.org/10.1515/sbe-2017-0003.

Burgis, Tom. (2017). "Dossier affair shines light on shadowy private intelligence work: In the corporate sphere paymasters sometimes have ulterior motives." *Financial Times*. January 14, 2017.

Carnegie Mellon University. (2017). "CERT Division Insider Threat Center." Software Engineering Institute. 2017 CERT Insider Threat Center Catalogue. Accessed October 26, 2020. https://resources.sei.cmu.edu/asset_files/Brochure/2017_015_001_452233.pdf.

Cha Ariana Eunjung and Ellen Nakashima. (2010). "Google China cyberattack parts of vast espionage campaign, experts say." *Washington Post,* January 14, 2010.

Defence Intelligence Agency. (1988). Department of Defense-24.02.1988. Accessed January 28, 2021 https://www.dia.mil/FOIA/FOIA-Electronic-Reading-Room/FOIA-Reading-Room-Iran/FileId/89383/

European Union Commission Report. (2016). "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry." Brussels, 5.7.2016 COM(2016) 410 final. Accessed January 28, 2021 https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52016DC0410&from=en

Fitzpatrick, W. M., Samuel A. DiLullo, and Donald R. Burke. (2004). "Trade Secret Piracy and Protection: Corporate Espionage, Corporate Security and the Law." *Advances in Competitiveness Research*, Vol. 12, No. 1, 57-71.

Google Official Blog. (2010). "A new approach to China." January 12, 2010. Accessed January 28, 2021. https://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

Horan, Sheila. (2000). "Corporate and Industrial Espionage and Their Effect on American Competitiveness - A statement before the House Subcommittee on International Economic Policy and Trade." IO6 Congress. Serial No: 106-180. September 13, 2000. Washington, D.C.

IBM X-Force Research. (2016). "Cyber Security Intelligence Index: A Survey of the Cyber Security Landscape." Accessed October 21, 2020. http://www-03.ibm.

com/security/data-breach/cyber-securityindex.html.

Ijzermans, Maarten and Wietse Van den Berge. (2019). "Resilience after Corporate or Industrial Espionage." The BCI Netherlands & Belgium Conference, Utrecht, Netherlands.

Jalil, Jüriah and Halyani Hassan. (2020). "Protecting Trade Secret from Theft and Corporate Espionage: Some Legal and Administrative Measures." *International Journal of Business and Society*, Vol. 21 S1, (2020):205-218, ISSN: 15116670.

Koen, Clifford and Brian London. (2019). "To Catch a Thief: Protecting Proprietary Information Including Trade Secrets from Corporate Espionage." *The Health Care Manager*, Oct/Dec 2019; 38 (4):331-342, DOI: 10.1097/HCM.0000000000000283.

Kompyte. (2018). "Competitive Intelligence Examples from the Real World." Accessed October 12, 2020. https://www.kompyte.com/blog/competitive-intelligence-examples/

Nasheri Hediah. (2015). *Economic Espionage and Industrial Spying*. London: Cambridge University Press.

Organisation for Economic Co-operation and Development. (2016). "Enquiries into Intellectual Property Economic Impact: Approaches to the Protection of Trade Secrets." Brian Mitchell. "Corporate Cyberespionage: Identification and Prevention." Published online: 30 Sep 2020.

Porteus, Samuel. (1994). "Economic Espionage: Issue Rising from Increased Governmental Involvement with Private Sector." *Intelligence and National Security*, Volume 9, October 1994, No 4, 737, DOI: 10.1080/02684527.2020.1771934.

PricewaterhouseCoopers. (2014). "Economic Impact of Trade Secret Theft: A framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats." Centre for Responsible Enterprise and Trade. Accessed September 1, 2020. https://www.innovation-asset.com/hubfs/blog-files/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf.

Rothke, Ben. (2001). "Corporate Espionage and What Can Be Done to Prevent It." *Information Systems Security*. 10:5, p. 1-7. Accessed November 2, 2020 DOI: 10.1201/1086/43315.10.5.20011101/31716.3 https://www.researchgate.net/publication/220450115_Corporate_Espionage_and_What_Can_Be_Done_to_Prevent_It.

Tessian. (2020). "Spear Phishing: Real-World Examples of Social Engineering At-

tacks." Accessed November 1, 2020. https://www.tessian.com/blog/examples-of-social-engineering-attacks/

O'Harrow, Robert Jr. "Oracle Admits To Probe." *The Washington Post*, June 29, 2000.

U.S. Department of Commerce. (2020). "Notable Industrial Espionage Cases." Accessed November 7, 2020. https://www.wrc.noaa.gov/wrso/security_guide/industry.htm.

U.S. Department of Justice (2020). "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases." Accessed September 29, 2020. https://www.justice.gov/usao-ma/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china.

U.S. State of Cybercrime Report. (2016). "Software Engineering Institute, U.S. State of Cybercrime Survey." Publisher RSA. White Paper. May 2016. Accessed November 19, 2020. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=499782.

Vashisth, Akanksha and Avinash Kumar. (2013). "Corporate espionage: The insider threat." *Business Information Review.* 30(2) 83–90, DOI: 10.1177/0266382113491816.

Wimmer, Bruce. (2015). *Business Espionage Risk, Threats and Countermeasures.* 1st edition, eBook ISBN: 9780124200548. Butterworth-Heinemann.