BUSINESS COUNTERINTELLIGENCE AS A PROTECTION STRATEGY FOR SMES

Romel Ramón González-Díaz¹, Ángel Eduardo Acevedo-Duque², Santos Lucio Guanilo Gómez³, Elena Cachicatari Vargas⁴

¹Centro Internacional de Investigación y Desarrollo (CIID) Montería, Colombia
²Faculty of Business and Administration, Universidad Autónoma de Chile, Providencia - Santiago, Chile
³, ⁴Universidad Nacional Jorge Basadre Grohmann, Tacna, Peru

E-mails: director@ciid.com.co¹, angel.acevedo@uautonoma.cl², guanilog@unjbg.edu.pe³, ecachicatariv@unjbg.edu.pe⁴

Received 18 September 2020; accepted 22 January 2021; published 30 March 2021

Abstract. The objective of this research was to analyze the processes of business counterintelligence as a strategy to shield the SMEs from competitive intelligence services. It was framed in the convergence of research approaches given in 2 phases: quantitative phase (Likert type questionnaire applied to 385 Colombian businessmen), qualitative phase (semi-structured interview to 4 police officers with more than 25 years of experience in police counter-intelligence) and the conclusions are formulated taking into account the convergence of approaches by dimension/category. The significant findings allude to the existence of a perception on the part of the entrepreneurs about the counterintelligence systems implemented in the SMEs they manage. However, experts on the subject agree on the lack of knowledge of risk factors regarding information vulnerability and the lack of strategies to shield SMEs from competitive intelligence services.

Keywords: Business Counterintelligence; Business Intelligence Services; Counterintelligence Strategie; SMEs


JEL Classifications: E30, E32

* This research was supported by the project, which has received funding from research and innovation programme of the Centro Internacional de Investigación y Desarrollo (CIID) Montería, Colombia.
1. Introduction

Throughout history, military strategies have been associated with business strategies. This is because they share similar objectives in terms of achieving competitive advantage over the adversary. The study of strategic management has its origins in the military, terms such as objectives, mission, strengths and weaknesses were created to address problems on the battlefield. The academic literature records writings such as the book "The Art of War" related to military strategy that date back to around 500 BC. The phrase "If you use the enemy to defeat the enemy, you will be powerful everywhere you go" (Sun, 2016, p. 1) is a commonplace phrase in the literature, and it is only when you know every detail of the terrain that you can maneuver and fight" (Sun, 2016, p. 1). 78), alludes to the spying strategies used to destabilize the organization of an army, executing internal sabotage actions and collecting information on position, logistics and combat strength (Catoira, 2018; Jayaram, 2020; Khristoforov & Guseva, 2020; Teixeira Júnior & Da Silva, 2020).

The spying activities during the cold war (cases of KGB †آملاً bloc and CIA‡ capitalist) until today have multiplied the public cases as: Pentagon Papers (a classified Pentagon report on U.S. decision-making in relation to the Vietnam War), Watergate (extraction of documents on the harassment of activist groups and political figures that destroyed Richard Nixon's political career), Wikileaks (publication of documents on the dynamics and activities of the U.S. government abroad) and the case of Snowden (he warned about the massive programs of diplomatic surveillance and manipulation, economic espionage and social control by the U.S. government) (Cadiz, 2016; Crespo-Pazmiño, 2019; Olmedo & Gavilánez, 2018).

Undoubtedly, acts of espionage gain access to privileged information and generate competitive advantage in any public or private organization. In the business field there are also cases of theft of trade secrets that according to the consulting firm (PWC, 2018) companies in the world lose an estimated "3 billion euros, equivalent to 5% of world GDP" (p. 65). Most of this crime is associated with the theft of formulas and methods from development processes and systems as vital to the functioning of the organization. A recent case is the lawsuit filed by TESLA against RIVIAN for the alleged systematic theft of sensitive data and trade secrets from different projects, alleging the existence of a pattern of searching for TESLA personnel to consciously manipulate the illegal appropriation of TESLA trade secrets (Hipertextual, 2020; Pazmiño, 2020).

In Colombia, trade secrets are protected by Decision 486 of the (Andean Community, 2000). However, the violation of them is constantly evidenced in bidding processes, for example, recent disputes between Claro and Banco Agrario, where there is an alleged leakage of information in bidding processes to hire a provider of ICT services and computer security for the headquarters of the agrarian bank for contracts exceeding US$ 40 billion (Espectador, 2020; González-Diaz & Cruz-Ayala, 2020). In SMEs, the situation regarding theft of trade secrets has not been addressed. In fact, more than 96% of SMEs do not conduct risk assessments of vulnerability to cyber attacks, do not follow up on trusted employees and do not strategically plan for the protection of information assets (Griewatz et al., 2020; PWC, 2018; Riisager-Simonsen et al., 2020; Tejena-Macias, 2018).

† The KGB (Комитет Государственной Безопасности (Комитет Государственной Безопасности)) translated into Spanish as The Committee for State Security, was the name of the intelligence agency of the Soviet Union from March 13, 1954 to March 13, 1991.
‡ The CIA (Central Intelligence Agency), in Spanish: Central Intelligence Agency is a civilian foreign intelligence service of the United States federal government in charge of collecting, processing and analyzing national security information from around the world, mainly through the use of human intelligence.
1.1. Business Counterintelligence

There is no evidence in the scientific literature of studies on corporate counterintelligence, since it is a relatively new term that combines two words: "counter-intelligence" and "entrepreneurship". On the one hand, Gómez de la Torre Rotta and Medrano Carmona (2020); Mendoza Cortés (2020); Rodríguez (2017) agree that counterintelligence frames a set of activities aimed at detecting, preventing and eliminating the enemy's intelligence actions. As for business, reference is made to the company as an institution dedicated to activities or the pursuit of economic or commercial ends to satisfy the needs for goods or services of society (Cortiñas, 2019). In short, corporate counterintelligence refers to the set of coordinated activities to detect, prevent and eliminate intelligence services in their different forms, which are intended to alter the healthy internal and external development of the organization (Bohnsack et al., 2020). An economic entity must consider corporate counterintelligence as a measure to protect its tangible and intangible assets. This allows the creation of a space for sustainable development and secure information systems for economic activities. SMEs with good business counterintelligence systems guarantee information protection (Hernandez-Julio et al., 2020). Therefore, this research analyzes business counterintelligence processes as a strategy to shield SMEs from competitive intelligence services.

2. Methodology

In the present study we used the design of convergent mixed research, structured in 2 parallel sections (quantitative section and qualitative section). These research designs involve a confrontation of data from different angles (quantitative and qualitative), in order to merge them, confront them and generate a comprehensive interpretation with a holistic view of the object of study (Fetters et al., 2013; Guetterman et al., 2015; Kettles et al., 2011). Triangulation increases confidence, overcomes reductionism of approaches, and in case of congruency in the conclusions, confers reliability and validity of the results.

2.1. In the quantitative section

A survey was applied (questionnaire with 7 items with a Likert scale validated in the opinion of 3 experts with a Cronbach's Alpha coefficient of 0.91(Excellent) to a random sample with a margin of error of 5% with a confidence level of 95%, for a total of 385 SME entrepreneurs in Colombia. The data was analyzed with descriptive statistics to understand the behavior of the variables under study. SPSS25 was used as a tool for the analysis of quantitative data. The operationalization of the business counter-intelligence variable is shown in table 1.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Dimensions</th>
<th>Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUSINESS counterintelligence</td>
<td>Detect</td>
<td>Strategic diagnosis of SME information security vulnerabilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Organization of actions to detect intelligence operations of the competition against you</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Infiltration of employee-agents in charge of intelligence to the work team</td>
</tr>
<tr>
<td></td>
<td>To prevent</td>
<td>Execution of activities aimed at preventing competition intelligence activities against you</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information systems are monitored by a trusted work team</td>
</tr>
<tr>
<td></td>
<td>Remove</td>
<td>Application of rules and procedures to punish personnel involved in activities that violate the security of the information of the SME</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Implementation of strategies to obtain strategic information from the competition</td>
</tr>
</tbody>
</table>
For the interpretation of the data, the following interpretation criteria were considered according to the cut points, 4 cut-points were applied with a distance of 0.8 (see table 2).

<table>
<thead>
<tr>
<th>Cut points</th>
<th>Detect</th>
<th>To prevent</th>
<th>Remove</th>
<th>Counterintelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.00-1.80</td>
<td>Poor intelligence detection systems</td>
<td>Poor intelligence Prevention systems</td>
<td>Poor intelligence Elimination systems</td>
</tr>
<tr>
<td>2</td>
<td>1.81-2.60</td>
<td>Bad intelligence detection systems</td>
<td>Bad intelligence Prevention systems</td>
<td>Bad intelligence Elimination systems</td>
</tr>
<tr>
<td>3</td>
<td>2.61-3.40</td>
<td>Regular intelligence detection systems</td>
<td>Regular intelligence Prevention systems</td>
<td>Regular intelligence Elimination systems</td>
</tr>
<tr>
<td>4</td>
<td>3.41-4.20</td>
<td>Good intelligence detection systems</td>
<td>Good intelligence Prevention systems</td>
<td>Good intelligence Elimination systems</td>
</tr>
<tr>
<td>5</td>
<td>4.21-5.00</td>
<td>Excellent intelligence detection system</td>
<td>Excellent intelligence Prevention system</td>
<td>Excellent intelligence Elimination system</td>
</tr>
</tbody>
</table>

2.2. Qualitative section
In parallel, four police counter-intelligence experts were consulted on practical counter-intelligence procedures through a semi-structured interview with four questions related to the categories: Detect, Prevent and Eliminate. The selection criteria of the experts were: more than 25 years of service in the counterintelligence department of the Police, command of executive levels (sub-commissioner and commissioners) (González-Díaz & Polo, 2018). Subsequently, the opinions generated by the experts were subjected to a hermeneutic and interpretative analysis under the approaches of Martinez (2011) who proposes 4 steps: structuring, categorization, comparison and interpretation. Atlas.ti8 was used as a tool for the analysis of qualitative data.

3. Analysis and discussion of results
Once the information has been collected in parallel with each of the instruments, regardless of the research approach, the results are presented and discussed in two sections: Quantitative and Qualitative. Finally, a convergence of approaches is made to respond to the objective of this study.

3.1. Quantitative Section
In this section we used descriptive statistics in order to know the current situation of business counterintelligence in Colombian SMEs, which generated the following results (see table 3)

Table 3, shows a total of 385 managers surveyed with 0 missing values, with an average of 3.42 which according to table 2, is categorized as a good business counter-intelligence system. However, studies referring to the vulnerability assessment of information in SMEs published by Ocampo Giraldo (2019), Naughton et al. (2020),
Mabula et al. (2020) and Ageeva and Mishura (2019) do not agree with what is presented, in other words, those who manage SMEs are convinced that rudimentary procedures such as private surveillance are sufficient to safeguard the business operations of these entities. Therefore, a detailed analysis is made in figures (1, 2, 3 and 4).

In figure 1, the detection of competitive actions that violate the security of information and business secrets of SMEs is shown. The managers surveyed consider that the procedures assumed by the SME are good enough to detect competitive intelligence, consider that they have a good strategic diagnosis of the information security vulnerabilities of the SME, good organization of the actions to detect competitive intelligence operations against them and infiltration of employees-agents in charge of making intelligence to the work team as they propose (Laszka et al, 2014; Tariq et al., 2012; Wilson, 2014). These results do not coincide with those proposed by Gaitán Castro (2019) and Díaz Pérez (2020), who consider that SMEs lack the financial resources to implement a monitoring and information follow-up system to detect fraud with information management (González-Díaz & Ledesma, 2020).
In figure 2, the behavior of the surveyed managers’ answers regarding the prevention of intelligence actions by the competition can be seen. An average of 3.47 was obtained according to the data interpretation scale of table 2, which is considered as good systems for the prevention of enemy activity. Specifically, the managers consider to execute activities destined to prevent intelligence activities of the competition against them and their information systems are monitored by a trustworthy work team. These results contrast with those presented by Lara (2018) and Cevallos Villegas et al. (2018) who point to serious deficiencies in the detection systems of competitive intelligence services that may violate strategic trade secrets. Likewise, authors such as Al-Mohannadi et al. (2020) and Sari (2018) recommend an intensive process of social auditing of employees and direct competition using artificial intelligence-based web services to counter and report cyber threats.
Figure 3 shows the results of the surveyed managers regarding the systems of elimination of competitive intelligence actions in SMEs, who obtained an arithmetic average of 3.34, which implies that regular systems of elimination of enemy activity. It shows the impossibility of administrative and criminal processes for the application of rules and procedures to sanction staff involved in activities that violate the security of information of the SME and difficulty in implementing strategies to obtain strategic information from the competition. All of this is consistent with the studies by Díaz (2018), Muñoz-Gallego (2018) and Norberto et al. (2018) who state that although Colombia has made progress in legal matters regarding trade secrets, operational and procedural mechanisms are still required to sanction them (Sánchez et al., 2020).
Once the descriptive statistics of each dimension were analyzed, the arithmetic average of the business counterintelligence variable was calculated, which obtained an average of 3.42, which represents a good system of business counter-intelligence in Colombian SMEs in the scale of interpretation of the results described in table 3. However, these results contradict the cross-cutting approaches of Múnera Pavón (2019), Durst and Zieba (2020), Jalil and Hassan (2020), Knickmeier (2020), who indirectly believe that businessmen believe that their companies are protected from the leakage of strategic material by having a closed video camera monitoring system, leaving aside information traffic as a determining factor in the development of a company. Therefore, a reconceptualization of the concept of security and protection of assets is required, reflecting on the professional secrets that give life to the economic entity (Button, 2020; Jung & Jung, 2020; Konopatsch, 2020; Sailio et al., 2020).

3.2. Qualitative section
In this section we used hermeneutic interpretative analysis of key informants’ discourses through the following stages: structuring, categorization, contrasting, and interpretation. To this end, it was used as a tool for the analysis of qualitative data (Atlas.ti8), which allowed the generation of the following table 4 and the semantic network (figure 5).

<table>
<thead>
<tr>
<th>Table 4. Table Analysis keycode-informant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Informant 1</td>
</tr>
<tr>
<td>Absolute</td>
</tr>
<tr>
<td>Detect Gr = 22; GS = 10</td>
</tr>
<tr>
<td>Remove Gr = 19; GS = 6</td>
</tr>
<tr>
<td>Prevent Gr = 25; GS = 9</td>
</tr>
<tr>
<td>Totals</td>
</tr>
</tbody>
</table>
Table 4 shows the concurrence of the categories (Detect, Eliminate and Prevent) that respond to the guiding category of Business Counterintelligence. In this case, the interviewees are experts in the field of police counterintelligence and consider that it is necessary to be more consistent when elaborating planning processes to prevent enemy action with a frequency in codes of 46.67%, emphasizing the monitoring of human sources, infiltration of the environment, technological means, monitoring of social networks, vulnerability testing, psychological awareness, surveillance and home visits. As for the processes of eliminating enemy actions, experts consider that social engineering is required, legalizing sanctions and implementing security protocols, without neglecting the processes aimed at detecting enemy actions (González-Díaz, Acosta-Moltó, et al., 2020; González-Díaz, Becerra-Peréz, et al., 2020).

Figure 5 shows the hermeneutic framework of counterintelligence from police procedures through a semantic network that accounts for detection processes. These are focused on studies of the risk and threats that affect the security of the company's information. Likewise, a series of threat probability impact assessments must be carried out. Therefore, every organization must have a security protocol, both internal and external, that allows to know its vulnerabilities, weaknesses and also its strengths. In order to know the first ones, it is necessary to make a periodic control of its physical facilities as well as of its human component in order to establish possible information leaks and internal and external channels that allow it. Likewise, self-assessments, internal control audits, checklists, application of ISO 27001, Coso ERM 2013 and 2017 and ISO high level structure analysis, following each of the controls so as not to leave anything out in the analysis, as this is the only way to be rigorous and avoid overlooking possible vulnerabilities (Noroño Sánchez et al., 2020).

As for the prevention of competitive intelligence actions, physical vulnerability tests must be carried out on the facilities and personnel working in the company or institution. Likewise, security and reliability studies,
polygraph tests, home visits and accompaniment of personnel must be carried out. The continuous monitoring through surveillance, monitoring, extraction, interception of lines. Similarly, the activities to prevent contrary actions would be self-inflicted using an external element in order to know the weak part that allows its access, that is, if you want to know the vulnerabilities at the computer level, you can send a computer virus that can infiltrate the security system, if you want to know the physical vulnerabilities of the facilities to perform simulation activities that break with the security protocols and at the level of human component to perform control activities and monitoring of staff that is considered a threat.

In terms of eliminating the action of intelligence by the competition, you can run a good practice of intensive awareness at the beginning of the implementation of controls, which can be in 3 phases to ensure that the organization knows the rules and after this a stage of punishment with the application of exemplary attitudes, which should be visible to serve as a corrective measure but even more so pedagogical to the rest of people. In extreme cases, the formal mechanisms established in the Political Constitution of Colombia, Law on Intelligence and Counterintelligence 1621, Law 734 and 1015, Criminal Code, Law 1581 on Data Protection, may be used. Any person who violates the security of information has criminal and disciplinary reach.

4. Conclusions

Once both research approaches have been analyzed, a convergence is proposed based on the dimensions/categories: Detect, Eliminate and Prevent the action of competition. In this sense, the detection of competitive actions that violate the security of information and business secrets of SMEs is considered good, the experts recommend to maintain institutional stability by conducting a frequent study of the risks and threats that affect the security of information of the company or institution, if this is assumed as a frequent procedure, business sustainability is guaranteed, because organizational weaknesses can be addressed in time. Likewise, it is necessary to be rigorous in the access of external personnel to the SME. This requires investments in monitoring and follow-up systems to detect fraud with information management.

As for the processes of prevention of intelligence actions by the competition in SMEs, managers consider having good prevention systems. However, several studies described above contradict this position, so it is inferred levels of ignorance as to the scope of prevention of external intelligence attacks. Therefore, experts recommend testing the physical vulnerability of facilities and personnel working in the company and continuous monitoring through surveillance and follow-up. The systems of elimination of competitive intelligence actions in SMEs are regular due to the lack of knowledge about administrative and criminal processes for the application of rules and procedures to sanction personnel involved in activities that violate the security of the information of the SME. Therefore, it is recommended to implement awareness programs and reward the culture of information asset security, all of which will guarantee the sustainability of business counterintelligence.

Finally, the experts suggest implementing strategies to mitigate the processes of intelligence against SMEs, framed in creating false profiles in social networks, surveillance, monitoring, expansion. It is possible to resort to the service of hacker or cracker to obtain privileged information, processes of infiltration of their environment, monitoring of their social networks through social engineering, strategy of collection of human sources (cooperators, informants, single line of questioning) technical means, infiltration, counter-intelligence.


Díaz, R. R., & Ledesma, K. N. F. (2020). Riesgos del uso de dispositivos móviles en seguridad de la información de las PYMES (Risks of the use of mobile devices in information security of SMEs).


Acknowledgements

This research was supported by the project, which has received funding from research and innovation programme of the Centro Internacional de Investigación y Desarrollo (CIID) Monteria, Colombia.

Romel Ramón GONZÁLEZ-DIÁZ is the Professor of Business Enterprise and Innovation and Director of the CIID, Monerteria Colombia. ORCID ID: https://orcid.org/0000-0002-7529-8847

Ángel ACEVEDO-DUQUE. Faculty of Business and Administration, Universidad Autónoma de Chile, Providencia - Santiago, Chile. ORCID ID: https://orcid.org/0000-0002-8774-3282

Santos Lucio GUANILLO-GÓMEZ. Professor at the Universidad Nacional Jorge Basadre Grohmann, Tacna, Peru. ORCID ID: https://orcid.org/0000-0002-7611-937X

Elena CACHICATARI-VARGAS. Professor at the Universidad Nacional Jorge Basadre Grohmann, Tacna, Peru. ORCID ID: https://orcid.org/0000-0002-9843-432X

Copyright © 2021 by author(s) and VsI Entrepreneurship and Sustainability Center
This work is licensed under the Creative Commons Attribution International License (CC BY). http://creativecommons.org/licenses/by/4.0/