ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 8 Number 3 (March)
http://doi.org/10.9770/jesi.2021.8.3(21)

Publisher
http://jssidoi.org/esc/home

BUSINESS COUNTERINTELLIGENCE AS A PROTECTION STRATEGY FOR SMES*

Romel Ramón González-Díaz [1], Ángel Eduardo Acevedo-Duque [2], Santos Lucio Guanilo Gómez [3], Elena Cachicatari Vargas [4]

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

E-mails: director@ciid.com.co[1], angel.acevedo@uautonoma.cl[2], guanilog@unjbg.edu.pe[3] , ecachicatariv@unjbg.edu.pe[4]

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

Reference to this paper should be made as follows: González-Díaz, R.R., Acevedo-Duque, A.E., Gómez, S.L.G., Cachicatari Vargas, E. 2021. Business counterintelligence as a protection strategy for SMEs. *Entrepreneurship and Sustainability Issues*, 8(3), 340-352. http://doi.org/10.9770/jesi.2021.8.3(21)

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.*

ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 8 Number 3 (March)
http://doi.org/10.9770/jesi.2021.8.3(21)

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 [†]communist 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-Díaz & 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-Macías, 2018).

[†] The KGB (Komitet Gosudarstvennoy Bezopasnosti (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, 1954 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.

ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 8 Number 3 (March)
http://doi.org/10.9770/jesi.2021.8.3(21)

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 1. Operationalization of the business counterintelligence variable

Variable	Dimensions	Indicators
BUSINESS counterintelligence	**Detect**	Strategic diagnosis of SME information security vulnerabilities
		Organization of actions to detect intelligence operations of the competition against you
		Infiltration of employee-agents in charge of intelligence to the work team
	To prevent	Execution of activities aimed at preventing competition intelligence activities against you
		Information systems are monitored by a trusted work team
	Remove	Application of rules and procedures to punish personnel involved in activities that violate the security of the information of the SME
		Implementation of strategies to obtain strategic information from the competition

ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 8 Number 3 (March)
http://doi.org/10.9770/jesi.2021.8.3(21)

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 2. Criteria for Interpretation of dimensions and business counterintelligence variable

Cut points	Data range	Interpretation			
		Detect	**To prevent**	**Remove**	**Counterintelligence**
1	1.00-1.80	Poor intelligence detection systems	Poor intelligence Prevention systems	Poor intelligence Elimination systems	Poor business counterintelligence system
2	1.81-2.60	Bad intelligence detection systems	Bad intelligence Prevention systems	Bad intelligence Elimination systems	Bad business counterintelligence system
3	2.61-3.40	Regular intelligence detection systems	Regular intelligence Prevention systems	Regular intelligence Elimination systems	Regulate business counterintelligence system
4	3.41-4.20	Good intelligence detection systems	Good intelligence Prevention systems	Good intelligence Elimination systems	Good business counterintelligence system
5	4.21-5.00	Excellent intelligence detection system	Excellent intelligence Prevention system	Excellent intelligence Elimination system	Excellent business counterintelligence system

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. Summary of the descriptive statistics of the business counterintelligence

		Detect	To prevent	Remove	Business Counterintelligence
N	Valid	385	385	385	385
	Lost	0	0	0	0
Half		3.41	3.47	3.34	3.42
Dev . Deviation		1,363	1,335	1,442	1,365
Minimum		one	one	one	one
Maximum		5	5	5	5

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),

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 8 Number 3 (March)
http://doi.org/10.9770/jesi.2021.8.3(21)

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).

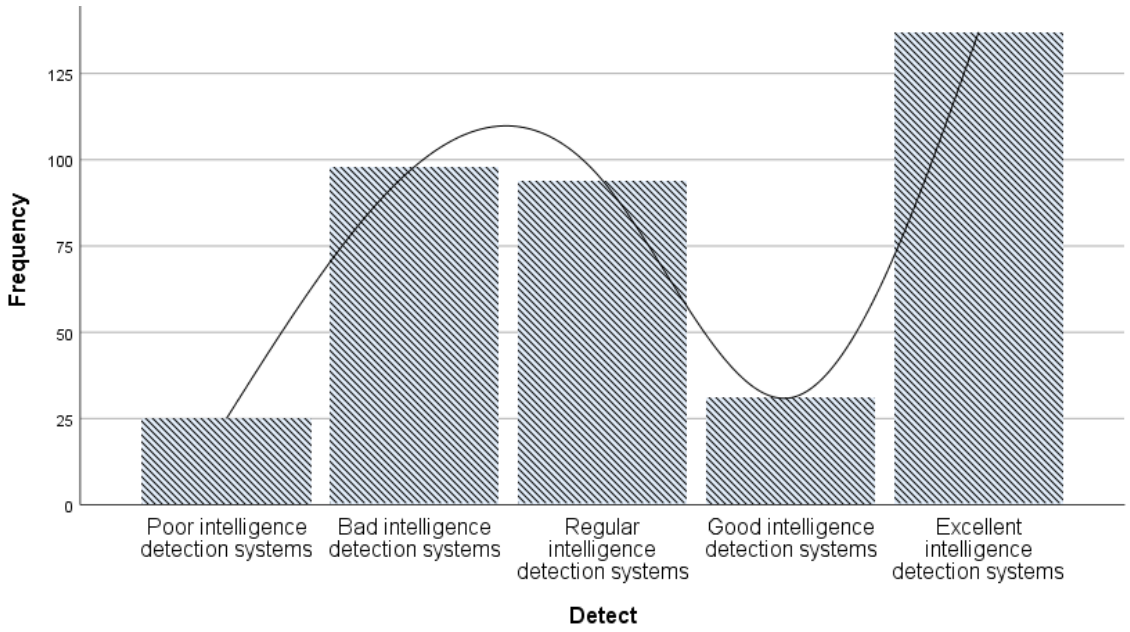

Figure 1. Detection of competitor intelligence actions

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).

ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 8 Number 3 (March)
http://doi.org/10.9770/jesi.2021.8.3(21)

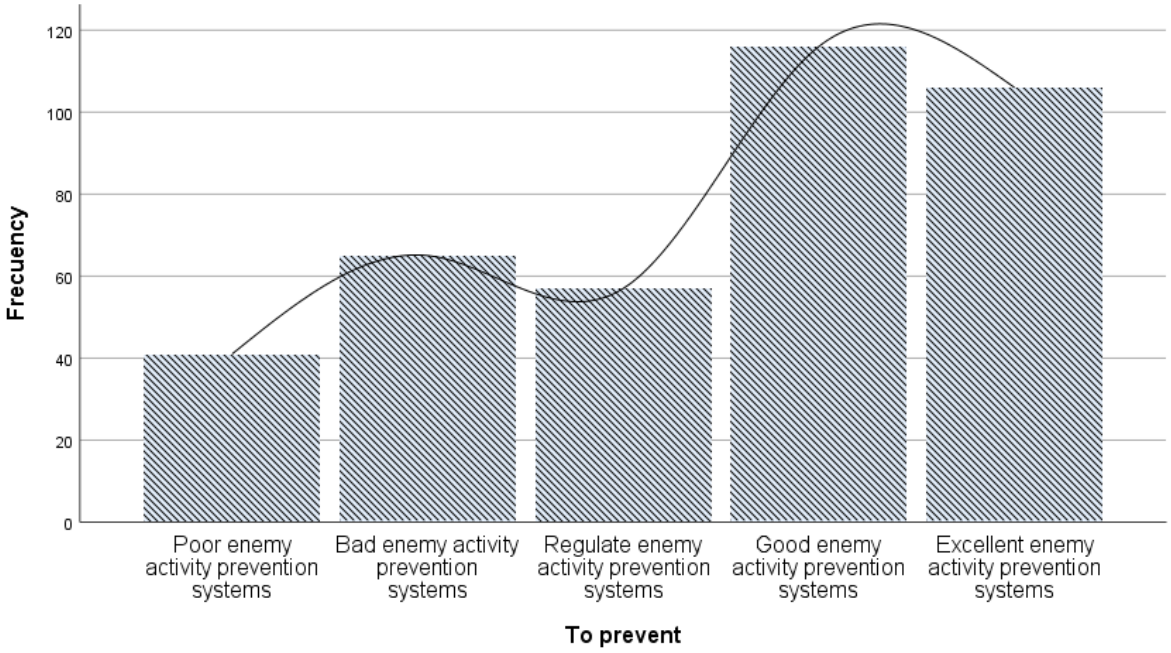

Figure 2. Prevention of competitor intelligence actions

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.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 8 Number 3 (March)
http://doi.org/10.9770/jesi.2021.8.3(21)

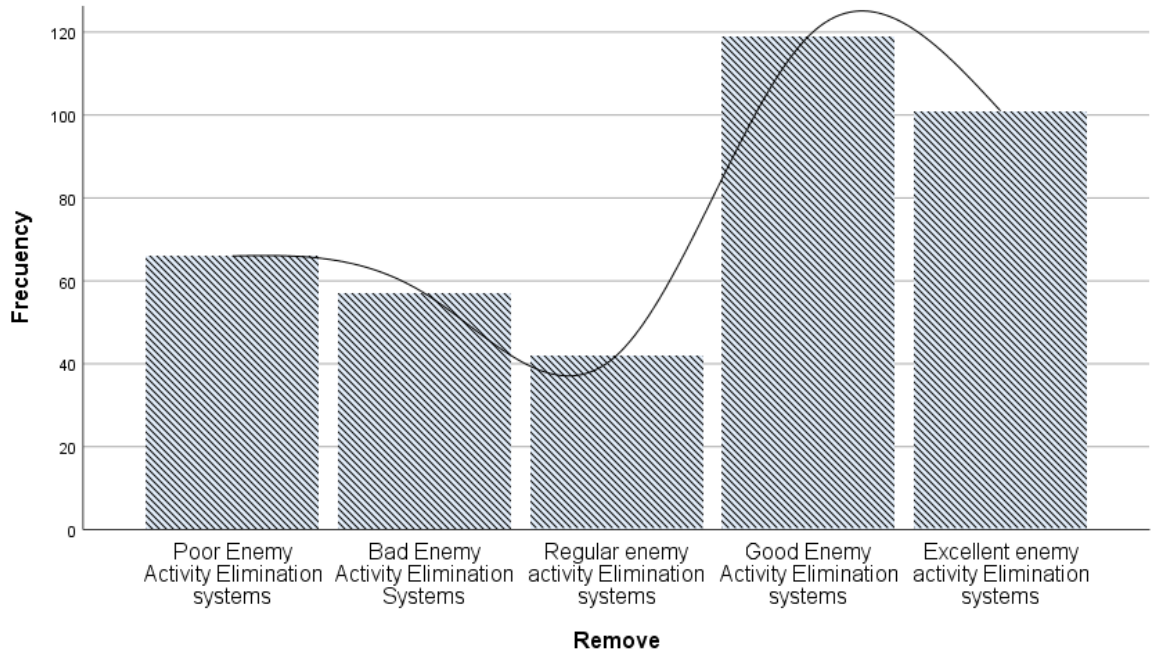

Figure 3. Elimination of actions competitive intelligence

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).

ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 8 Number 3 (March)
http://doi.org/10.9770/jesi.2021.8.3(21)

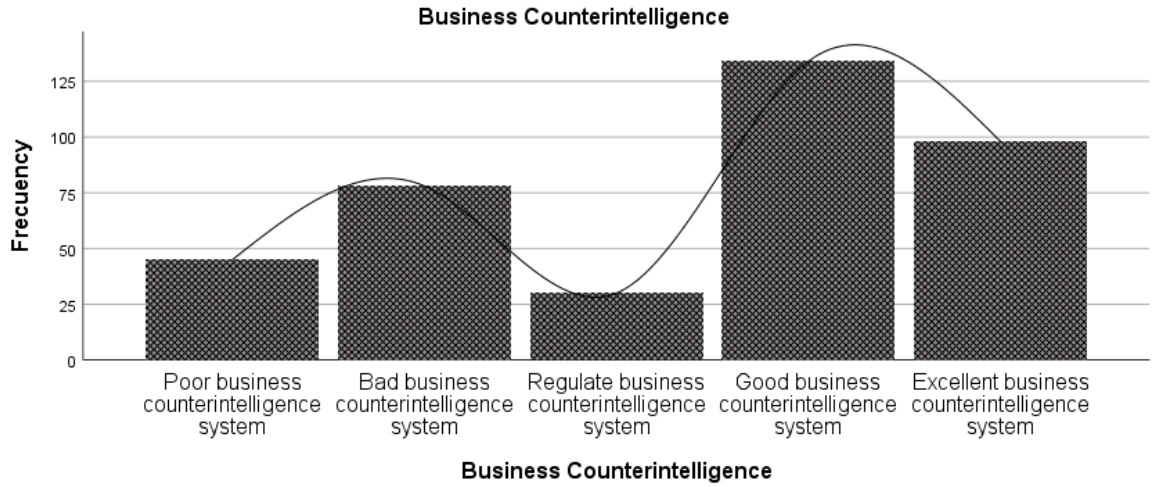

Figure 4. Business Counterintelligence in SMEs in Colombia

Once the descriptive statistics of each dimension were analyzed, the arithmetic average of the business counter-intelligence 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. Cualitative 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 4. Table Analysis keycode-informant

	Key Informant 1 Gr = 9		Key Informant 2 Gr = 6		Key Informant 3 Gr = 9		Key Informant 4 Gr = 16		Totals
	Absolute	Relative of the column	Absolute	Relative of the column	Absolute	Relative of the column	Absolute	Relative of the column	Absolute
Detect Gr = 22; GS = 10	5	45.45%	4	33.33%	4	30.77%	9	30.00%	22
Remove Gr = 19; GS = 6	4	36.36%	4	33.33%	4	30.77%	7	23.33%	19
Prevent Gr = 25; GS = 9	two	18.18%	4	33.33%	5	38.46%	14	46.67%	25
Totals	eleven	100.00%	12	100.00%	13	100.00%	30	100.00%	66

ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 8 Number 3 (March)
http://doi.org/10.9770/jesi.2021.8.3(21)

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 counter-intelligence 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).

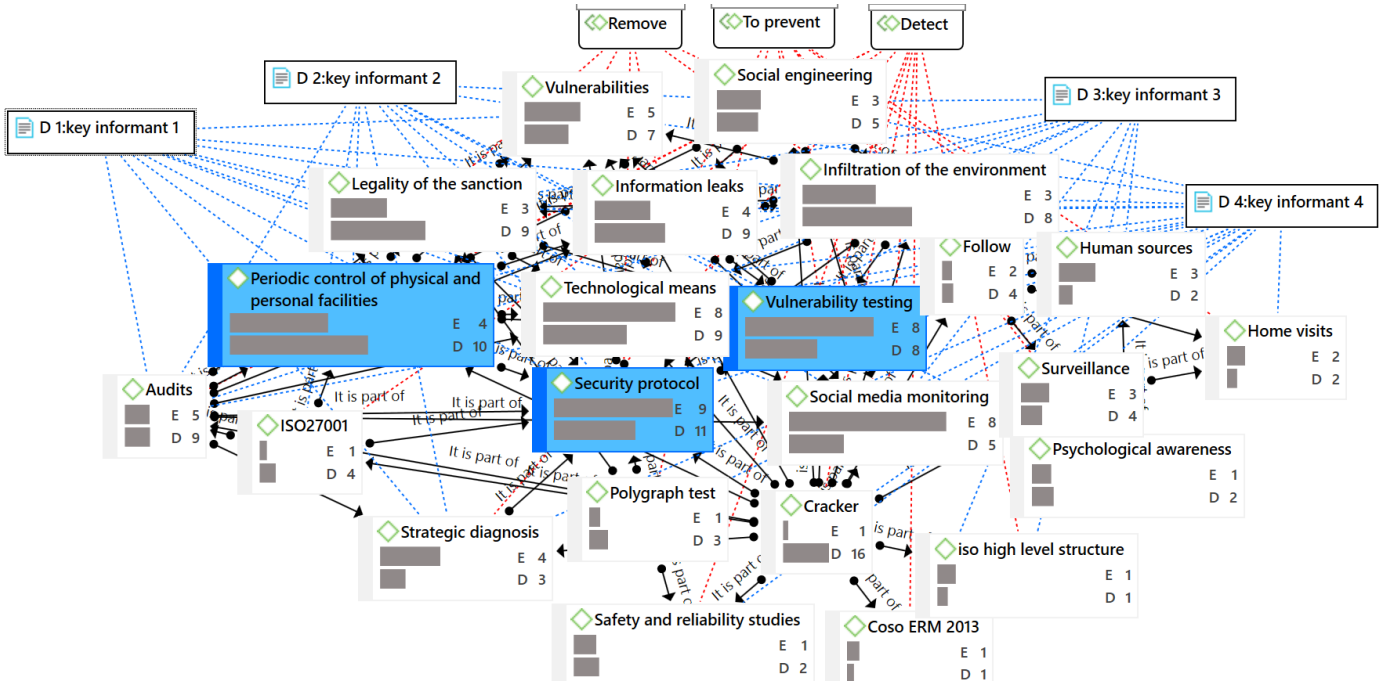

Figure 5. Hermeneutical framework about Police Counterintelligence

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 context 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,

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 8 Number 3 (March)
http://doi.org/10.9770/jesi.2021.8.3(21)

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.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 8 Number 3 (March)
http://doi.org/10.9770/jesi.2021.8.3(21)

References

Ageeva, S., & Mishura, A. (2019). Spatial aspects of the Russian banking system: Transformation and access to credit for small Russian firms. In Geofinance between Political and Financial Geographies: A Focus on the Semi-Periphery of the Global Financial System (pp. 120-137). Edward Elgar Publishing Ltd. https://doi.org/10.4337/9781789903850.00015

Al-Mohannadi, H., Awan, I., & Al Hamar, J. (2020). Analysis of adversary activities using cloud-based web services to enhance cyber threat intelligence [Article]. Service Oriented Computing and Applications, 14(3), 175-187. https://doi.org/10.1007/s11761-019-00285-7

Bohnsack, R., Kolk, A., Pinkse, J., & Bidmon, C. M. (2020). Driving the electric bandwagon: The dynamics of incumbents' sustainable innovation [Article]. Business Strategy and the Environment, 29(2), 727-743. https://doi.org/10.1002/bse.2430

Button, M. (2020). Editorial: economic and industrial espionage [Editorial]. Security Journal, 33(1). https://doi.org/10.1057/s41284-019-00195-5

Cádiz, G. M. P. (2016). Espionaje y contraespionaje en Puerto Rico durante la Segunda Guerra Mundial (Espionage and Counter-espionage in Puerto Rico during World War II). Cuaderno Internacional de Estudios Humanísticos y Literatura (CIEHL), (23), 20-32.

Catoira, A. A. E. (2018). Inteligencia corporativa y espionaje. http://hdl.handle.net/10469/13208

Cevallos Villegas, D. M., Moreno Rodríguez, C. J., & Chávez Garcés, Á. M. (2018). La auditoría interna como herramienta efectiva para la prevención de fraudes en las empresas familiares (Internal audit as an effective tool for fraud prevention in family businesses). Revista Universidad y Sociedad, 10(5), 15-20.

Comunidad-Andina. (2000). Decision 486: régimen común sobre propiedad industrial (Decision 486: common regime on industrial property) http://www.wipo.nt/wipolex/es/text.jsp

Cortiñas, J. (2019). Definición de empresa. Apuntes Gestión (Definition of company. Management Notes) https://www.apuntesgestion.com/b/definicion-deempresa/#comments

Crespo-Pazmiño, D. (2019). Ciberseguridad y Derechos Humanos: respuestas estatales e individuales a las revelaciones de espionaje de Snowden (Cybersecurity and Human Rights: State and Individual Responses to Snowden's Espionage Revelations). Comentario Internacional. Revista del Centro Andino de Estudios Internacionales (19), 77-98.

Díaz Pérez, J. S. (2020). Esquema Director de Seguridad para Empresas pymes del sector Construcción (Security Director Scheme for SMEs in the Construction sector). http://rua.ua.es/dspace/handle/10045/102087

Díaz, C. R. F. (2018). El delito de daños y el espionaje empresarial: dos ataques compatibles conta la información como bien inmaterial. InDret.

Durst, S., & Zieba, M. (2020). Knowledge risks inherent in business sustainability [Article]. Journal of Cleaner Production, 251, Article 119670. https://doi.org/10.1016/j.jclepro.2019.119670

Espectador, E. (2020). Claro rechaza declaraciones del Banco Agrario e insiste en que hubo filtración de datos (Claro rejects statements from the Agrarian Bank and insists that there was a data leak). https://www.elespectador.com/noticias/economia/claro-rechaza-declaraciones-del-banco-agrario-e-insiste-en-que-hubo-filtracion-de-datos/

Espionage and Competitiveness: The German Auto Industry in China's Modern Business Game). URVIO Revista Latinoamericana de Estudios de Seguridad (26), 93-103.

Fetters, M. D., Curry, L. A., & Creswell, J. W. (2013). Achieving integration in mixed methods designs - Principles and practices Health Services Research, 48(6 PART2), 2134-2156. https://doi.org/10.1111/1475-6773.12117

Gaitán Castro, S. (2019). 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). http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6472/Riesgos%20del%20uso%20de%20dispositivos%20m%C3%B3viles%20en%20seguridad%20de%20la%20informaci%C3%B3n%20de%20las%20PYMES.pdf?sequence=1&isAllowed=y

Gómez de la Torre Rotta, A., & Medrano Carmona, A. (2020). Orígenes yevolución de lasubversión y la contrainteligencia en el Perú, 1958-2015 (Origins and evolution of subversion and counterintelligence in Peru, 1958-2015). URVIO Revista Latinoamericana de Estudios de Seguridad (26), 57-71.

González-Díaz, R. R., & Cruz-Ayala, K. (2020). Contraloría financiera en la contratación pública. Una revisión de los contratos de obras públicas del estado venezolano (Financial Comptroller in Public Procurement. A review of the public works contracts of the Venezuelan state). Inquietud Empresarial, 20(1), 43-58.

González-Díaz, R. R., & Ledesma, K. N. F. (2020). Cultura organizacional y Sustentabilidad empresarial en las Pymes durante crisis periodos de confinamiento social (Organizational culture and business sustainability in SMEs during crisis periods of social confinement). CIID Journal, 1(1), 28-41.

González-Díaz, R. R., & Polo, E. A. S. (2018). Entrevistas Espontaneas Categoriales (EEC) para la construcción de categorías orientadoras en la investigación cualitativa (Spontaneous Categorical Interviews (EEC) for the construction of guiding categories in qualitative research). Journal Latin American Science, 1(2), 1-11.

González-Díaz, R. R., Acosta-Moltó, E., Flores-Ledesma, K., Vargas, E. C., & Menacho-Rivera, A. (2020). Marketing experience in non-profit organizations: A look at experience pro-viders [Article]. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, 2020(E36), 186-202.

González-Díaz, R. R., Becerra-Peréz, L. A., & Acevedo-Duque, A. E. (2020). Narco-marketing as a strategy for local tourism development [Article]. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, 2020(E36), 71-85. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85094645431&partnerID=40&md5=05aa102c97cbe24ef7e6480d83cbb588

Griewatz, J., Yousef, A., Rothdiener, M., Lammerding-Koeppel, M., Fritze, O., Dall'Acqua, A., Geißinger, M., Steffens, S., Steinweg, B., Borucki, K., Germanyuk, A., & Koenig, S. (2020). Are we preparing for collaboration, advocacy and leadership? Targeted multi-site analysis of collaborative intrinsic roles implementation in medical undergraduate curricula [Article]. BMC Medical Education, 20(1), Article 35. https://doi.org/10.1186/s12909-020-1940-0

Guetterman, T. C., Fetters, M. D., & Creswell, J. W. (2015). Integrating quantitative and qualitative results in health science mixed methods research through joint displays. Annals of Family Medicine, 13(6), 554-561. https://doi.org/10.1370/afm.1865

Hernández-Julio, Y. F., Meriño-Fuentes, I., González-Díaz, R. R., Guerrero-Avendaño, A., Toledo, L. V. O., & Bernal, W. N. (2020). Fuzzy knowledge discovery and decision-making through clustering and Dynamic tables: Application in Colombian business Finance. 2020 15th Iberian Conference on Information Systems and Technologies (CISTI). https://doi.org/10.23919/CISTI49556.2020.9141117

Hipertextual. (2020). Tesla contra Rivian: vuelve la obsesión por el robo de secretos comerciales (Tesla vs.Rivian: Trade Secret Theft Obsession Returns). https://hipertextual.com/2020/07/tesla-contra-rivian-robo-secretos-comerciales

Jalil, J. A., & Hassan, H. (2020). Protecting trade secret from theft and corporate espionage: Some legal and administrative measures. International Journal of Business and Society, 21(S1), 205-218. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85079684581&partnerID=40&md5=fc1e91b41abb8b9e5829bed4f17dcbdc

Jayaram, D. (2020). 'Climatizing' military strategy? A case study of the Indian armed forces. International Politics. https://doi.org/10.1057/s41311-020-00247-3

Jung, S. O., & Jung, C. H. (2020). Classification of industrial espionage cases and countermeasures. 2020 IEEE International Conference on Big Data and Smart Computing, BigComp 2020,

Kettles, A. M., Creswell, J. W., & Zhang, W. (2011). Mixed methods research in mental health nursing [Article]. Journal of Psychiatric and Mental Health Nursing, 18(6), 535-542. https://doi.org/10.1111/j.1365-2850.2011.01701.x

Khristoforov, V., & Guseva, Y. (2020). Soviet military strategy in Afghanistan: Errors in planning and public condemnation [Review]. Quaestio Rossica, 8(2), 382-398. https://doi.org/10.15826/qr.2020.2.469

Knickmeier, S. (2020). Spies without borders? The phenomena of economic and industrial espionage and the deterrence strategies of Germany and other selected European countries [Article]. Security Journal, 33(1), 6-26. https://doi.org/10.1057/s41284-019-00199-1

Konopatsch, C. (2020). Fighting industrial and economic espionage through criminal law: lessons to be learned from Austria and Switzerland. Security Journal, 33(1), 83-118. https://doi.org/10.1057/s41284-019-00200-x

Lara, J. E. Z. (2018). Médidas De Prevención Del Fraude De Las Empresas. In Médidas De Prevención Del Fraude De Las Empresas. Editorial Abya-Yala.

Laszka, A., Johnson, B., Schöttle, P., Grossklags, J., & Böhme, R. (2014). Secure team composition to thwart insider threats and cyber-espionage. ACM Transactions on Internet Technology, 14(2-3), Article 2663499. https://doi.org/10.1145/2663499

Mabula, J. B., Dongping, H., & Mwakapala, L. Y. (2020). SME's use of ICT and financial services on innovation performance: The mediating role of managers' experience [Article]. Human Systems Management, 39(3), 427-439. https://doi.org/10.3233/HSM-190790

Mendoza Cortés, P. (2020). Inteligencia y contrainteligencia militarfrente a fallos y desafíos. El caso de Culiacán, México (2019). URVIO Revista Latinoamericana de Estudios de Seguridad (26), 37-56.

Múnera Pavón, L. (2019). El espionaje en Colombia, 1919-1945: una mirada panorámica a través de los diarios El Tiempo (Espionage in Colombia, 1919-1945: a panoramic view through the newspapers El Tiempo), El Espectador y El Siglo.

Muñoz-Gallego, A. (2018). Retos y estrategias de ciberseguridad en la empresa. negocio Electrónico (Cybersecurity challenges and strategies in the company. Electronic business) https://riuma.uma.es/xmlui/handle/10630/16527

Naughton, S., Golgeci, I., & Arslan, A. (2020). Supply chain agility as an acclimatisation process to environmental uncertainty and organisational vulnerabilities: insights from British SMEs [Article]. Production Planning and Control, 31(14), 1164-1177. https://doi.org/10.1080/09537287.2019.1701130

Norberto, J., Gómez-Aller, J. D., Sánchez, J. A. L., & Martín, A. N. (2018). Derecho penal económico y de la empresa. Dykinson (Economic and corporate criminal law. Dykinson). file:///C:/Users/271/Downloads/derecho_penal_economico_2018.pdf

Noroño Sánchez, J. G., Nuñez Villavicencio, M., & González Díaz, R. R. (2020). Union ethics as a mechanism driving competitiveness in small and medium-sized enterprises [Article]. Utopia y Praxis Latinoamericana, 25(Extra3), 154-173. https://doi.org/10.5281/zenodo.3907063

Ocampo Giraldo, M. (2019). Artículo de revisión de Metodologías de Análisis de Riesgos de la Información, enfocado a Pymes Universidad Santiago de Cali].

Olmedo, J. I., & Gavilánez, F. L. (2018). Análisis de los ciberataques realizados en América Latina (Analysis of cyberattacks carried out in Latin America). INNOVA Research Journal, 3(9), 172-181.

Pazmiño, D. F. C. (2020). Espionaje y competitividad: la industria automotriz alemana en el juego comercial moderno de China

PWC. (2018). El fraude al descubierto (The fraud exposed). PWC. https://www.pwc.com/co/en/publications/technology/Fraude-al-descubierto.pdf

Riisager-Simonsen, C., Rendon, O., Galatius, A., Olsen, M. T., & Beaumont, N. (2020). Using ecosystem-services assessments to determine trade-offs in ecosystem-based management of marine mammals. Conservation Biology. https://doi.org/10.1111/cobi.13512

Rodríguez, J. V. (2017). La contrainteligencia en el sector de la industria (Counterintelligence in the industry sector). Economía industrial (405), 133-141.

Sailio, M., Latvala, O. M., & Szanto, A. (2020). Cyber threat actors for the factory of the future. Applied Sciences (Switzerland), 10(12), Article 4334. https://doi.org/10.3390/app10124334

Sánchez, J. G. N., Villavicencio, M. N., & Díaz, R. R. G. (2020). Ética sindical como mecanismo impulsor de competitividad en las pequeñas y medianas empresas (Trade union ethics as a competitiveness driver in small and medium-sized enterprises). Utopía y praxis latinoamericana: revista internacional de filosofía iberoamericana y teoría social (3), 154-173.

Sari, A. (2018). Context-aware intelligent systems for fog computing environments for cyber-threat intelligence. In Fog Computing: Concepts, Frameworks and Technologies (pp. 205-225). Springer International Publishing. https://doi.org/10.1007/978-3-319-94890-4_10

Sun, T. (2016). El arte de la guerra. Aegitas.

Tariq, M. A., Brynielsson, J., & Artman, H. (2012). Framing the attacker in organized cybercrime. 2012 European Intelligence and Security Informatics Conference, EISIC 2012, Odense.

Teixeira Júnior, A. W. M., & Da Silva, P. F. (2020). China in the contemporary world order: Grand strategy, military modernization, and balance of power [Article]. Sociedade e Cultura, 23, Article e59618. https://doi.org/10.5216/SEC.V23I.59618

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. Polo del conocimiento, 3(4), 230-244.

Wilson, C. (2014). Cyber threats to critical information infrastructure. In Cyberterrorism: Understanding, Assessment, and Response (Vol. 9781493909629, pp. 123-136). Springer New York. https://doi.org/10.1007/978-1-4939-0962-9_7

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) Montería, Colombia.

Romel Ramón GONZÁLEZ-DÍAZ is the Professor of Business Enterprise and Innovation and Director of the CIID, Montería 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 GUANILO-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