VARSTVOSLOVJE,
Journal of Criminal
Justice and Security,
year 21
no. 2
pp. 205–223

Corporate Intelligence as the New Reality: The Necessity of Corporate Security in Modern Global Business

Miha Dvojmoč

Purpose:

This paper seeks to address the necessity of corporate intelligence and its use in modern global business, as corporate security, to the wider expert community and academic community. The key concepts of corporate intelligence, competitive intelligence, sources and types of data collection, including phases of the competitive intelligence process are presented. The purpose of this paper is to define the key legal sources, relevant for corporate intelligence in the Republic of Slovenia, thereby establishing the normative framework for data collection in the Republic of Slovenia. The objective of this research is to define potential misuse that modern organisations must be aware of if they wish to successfully, and primarily safely, operate at the global level.

Design/Methods/Approach:

Literature review was conducted in order to achieve the articles purpose. In legal part of the paper, legal research methodology was implemented. The primary sources of law as cases, statutes etc. were analysed and law reviews, legal dictionaries and legal encyclopaedias for background information about a researched topic were added.

Findings:

Corporate intelligence, with an emphasis on competitive intelligence, and the mere awareness of the need for corporate security in the modern global business represent an inevitable step towards competitive and safe global business, with an awareness of external risks, exploiting their own advantages and knowledge of market characteristics.

Practical Implication:

Increased awareness in modern organisations that want to conduct their business safely, primarily from the perspective of global business. Present the risks on the market, as well as opportunities of their own competitive development. Offer a tool for managing challenges and upgrading business operations from the perspective of competitiveness and security on the market.

Originality/Value:

The article presents the concept of corporate intelligence with an upgrade to competitive intelligence, and represent corporate security as an unavoidable

and necessary tool for risk management, as well as achieving competitiveness and security in the global business. The findings are intended for all organisations, but primarily those that operate globally – or their managers, directors, owners, entrepreneurs and persons responsible for security systems in organisations. With regard to that, the article relates to these areas of practice, and is of use to scholars in assisting them to disentangle the various aspects of corporate intelligence, and also to managers who wish to gain an appreciation of the potential which competitive intelligence can bring to business success.

UDC: 005.934

Keywords: corporate intelligence, corporate security, business, globalisation

Korporativna obveščevalna dejavnost kot nova realnost: Nujnost korporativne varnosti v sodobnem globalnem podjetništvu

Namen prispevka:

V prispevku želi avtor širši strokovni javnosti in tudi akademski skupnosti predstaviti nujnost korporativne obveščevalne dejavnosti oz. njene uporabe v sodobnem globalnem podjetništvu v obliki korporativne varnosti. Predstaviti ključne koncepte korporativne obveščevalne dejavnosti, vključno s konkurenčno obveščevalno dejavnostjo ter vire in zvrsti pridobivanja podatkov, vključno s fazami procesa konkurenčne obveščevalne dejavnosti. Opredeliti ključne pravne vire, ki so relevantni za korporativno obveščevalno dejavnost v Republiki Sloveniji in s tem postaviti normativni okvir zbiranja podatkov v Republiki Sloveniji. Opredeliti možne zlorabe, ki se jih morajo zavedati sodobne organizacije, če želijo uspešno in predvsem varno poslovati na globalnem nivoju.

Metode:

Opravljen je bil pregled literature. V pravnem delu prispevka je avtor implementiral pravno raziskovalno metodologijo, analiziral primarne vire, kot so primeri pravne prakse in pravni akti, ter uporabil preglede pravnih virov, pravnih slovarjev in enciklopedij za vzpostavitev pravnih pojmov o raziskovani tematiki.

Ugotovitve:

Korporativna obveščevalna dejavnost s poudarkom na konkurenčni obveščevalni dejavnosti in samo zavedanje nujnosti korporativne varnosti v sodobnem globalnem podjetništvu predstavljajo neizogiben korak na poti h konkurenčnemu in varnemu globalnemu poslovanju, z zavedanjem zunanjih tveganj ter izkoriščanjem svojih prednosti in poznavanjem tržnih značilnosti.

Praktična uporabnost:

Dvig ozaveščenosti sodobnih organizacij, ki želijo poslovati varno, predvsem z vidika globalnega poslovanja. Predstaviti tveganja, ki jim na trgu pretijo, oziroma možnosti njihovega lastnega konkurenčnega razvoja. Ponuditi orodje obvladovanja izzivov in nadgradnje poslovanja z vidika konkurenčnosti in varnosti na trgu.

Izvirnost/pomembnost prispevka:

Prispevek predstavlja koncept korporativne obveščevalne dejavnosti z nadgradnjo v konkurenčno obveščevalno dejavnost in korporativno varnost kot tako prikazuje kot neizogibno potrebno orodje obvladovanja tveganj ter doseganja konkurenčnosti in varnosti v globalnem podjetništvu. Ugotovitve prispevka so namenjene vsem organizacijam, predvsem pa tistim, ki poslujejo globalno, oz. njihovim menedžerjem, direktorjem, lastnikom, podjetnikom in odgovornim za varnostne sisteme v organizaciji. Upoštevajoč navedene praktične sfere prispevek predstavlja uporabno orodje akademikom in raziskovalcem pri definiranju različnih vidikov korporativne obveščevalne dejavnosti ter menedžerjem, ki želijo s konkurenčno obveščevalno dejavnostjo uspešno poslovati.

UDK: 005.934

Ključne besede: korporativna obveščevalna dejavnost, korporativna varnost, podjetništvo, globalizacija

1 INTRODUCTION

Corporate security as a part of the comprehensive security in an organisation or enterprise revolves around various areas and aspects of activity, which indisputably includes the corporate intelligence, with economic or business intelligence and competitive intelligence as the dominant forms. In this regard, this article intends to present the corporate intelligence's necessity and its use in modern global business, as corporate security, to the wider expert community and academic community. Working through the key concepts of corporate intelligence, including competitive intelligence, sources and types of data collection, including phases of the competitive intelligence process, we define the key legal sources, relevant for corporate intelligence in the Republic of Slovenia, thereby establishing the normative framework for data collection in the Republic of Slovenia. On top of that and with the help of that, we define potential misuse that modern organisations must be aware of if they wish to successfully, and primarily safely, operate at the global level.

The corporate intelligence could represent a tool of increased awareness in modern organisations that want to conduct their business safely, primarily from the perspective of global business, taking into account the risks on the market, as well as opportunities of their own competitive development. As a tool for managing challenges and upgrading business operations from the perspective of competitiveness and security on the market, the mere awareness of the need for corporate security in the modern global business represent an inevitable step towards competitive and safe global business, with an awareness of external risks, exploiting their own advantages and knowledge of market characteristics.

The primary aim of the article is to present the concept of corporate intelligence with an upgrade to competitive intelligence, to reinforce the perception of the corporate security as an unavoidable and necessary tool for risk management, as well as for achieving competitiveness and security in the global business. The main aspect of the article is a review of key concepts - deriving from

(integral) corporate security, followed by corporate intelligence, with emphasis on economic or business intelligence and competitive intelligence as the dominant forms or corporate intelligence. Inevitably, we present the sources and types of data collection in competitive intelligence along with the stages of competitive intelligence process. The article also presents the normative framework for data collection in the Republic of Slovenia, and addresses the potential abuses.

In the paper, the literature review on corporate intelligence and similar concept is presented. Legal part of the study involves analysis of the primary sources of law as cases, statutes etc. to identify and retrieve information necessary to support legal decision-making. We also search secondary sources like law reviews, legal dictionaries and legal encyclopaedias for background information about the topic.

2 DEFINITIONS OF KEY CONCEPTS

2.1 (Integral) Corporate Security

Integral (corporate) security is a relatively new concept in the corporate governance and is dealing with those undesirable outcomes that might endanger resilience and survival of the organization. Rising number of threats that might have a negative impact on the business has resulted in creation of Chief Security Officer (CSO) (Aksentijevic Forensic and Consulting, n. d.). As part of the comprehensive security in an organisation or enterprise, corporate security involves adopting and implementing a corporate security policy, and includes numerous areas of activity, among them (Dvojmoč, 2019):

- ensuring legal and uninterrupted business operations;
- protection against risks and threats (by assessing risks and threats specific for the critical infrastructure, organisation, assessment, protection and detection of unlawful actions within the organisation, deceit and fraud to the detriment of the organisation, and, in this regard, implementation of intelligence and counter-intelligence measures within the organisation);
- legal protection of information system technologies (IT security);
- corporate protection of real rights and intellectual property rights (including corporate protection of property rights and other real rights of the organisation, protection of patents, brands, models, original of products, and protection of organisation's material copyrights);
- providing physical and technical security (which includes corporate arrangement for protecting organisation's property, supervision over security tasks of internal or external services, and security planning and risk assessment);
- ensuring a safe work environment by protecting people and personal data, legal arrangement of safe environment, and legal arrangement of health and safety at work;
- corporate human resources management and administration.

As such, the concept is relevant for all organisations, primarily those that operate globally, for their managers, directors, owners, entrepreneurs and persons

responsible for security systems in organisations. Disentangling the various aspects of corporate intelligence, and gaining an appreciation of the potential which competitive intelligence can bring to business success, is necessary to achieve the above-mentioned goals, as presented below.

2.2 Corporate Intelligence

Within the concept of corporate security, we can discuss a narrower concept, corporate intelligence, which includes economic or business intelligence and corporate or competitive intelligence as hyponyms of corporate intelligence.

Etymologically, the word *intelligence* is derived from Latin *intelligere* (*intellego, intellegis, intellegere, intellexi, intellectum*), which can mean to detect, notice, realise, comprehend, understand, to be skilled, think, consider, imagine.

Intelligence is a very wide concept, which Richelson (in Purg, 1995) defined as "the results of collecting, analysing, combining and interpreting all available data that concern one or more aspects of a foreign country or operating area, which is directly or potentially significant for planning." Müller-Wille (2004) has a similar definition, but differentiates between different types of intelligence based on their function (military intelligence, which collects and studies information on current and potential activities of foreign armed forced inside and outside the national territory; security intelligence, which collects and studies threats to the constitutional arrangement; criminal intelligence, which conducts activities of fighting organised crime; and external intelligence, which focuses on activities abroad, and its purpose is to provide support for foreign political decision-making and situation assessment of security, defence, external and security policies). The development of traditional intelligence services is heading towards "privatisation" of intelligence, with the aim of forming and developing a new discipline, i.e. economic inquiry or competitive intelligence, which can be used in another (corporate or business) world.

2.3 Economic and Competitive Intelligence as the Dominant Forms or Corporate Intelligence

In the field of economy, we encounter several conceptual definitions of corporate intelligence. The most prevalent concepts are economic or business intelligence and corporate or competitive intelligence. In the Slovenian setting, we encounter concepts such as business intelligence, business information and economic inquiry (Ulcej, Britovšek, & Sotlar, 2011).

The term economic intelligence is used to describe the collection of business-relevant economic information, including technological data, financial, commercial proprietary and government information, whose acquisition by foreign interested parties either directly or indirectly contributes to a relative increase of productivity or improved competitive economic position of the country, in which the organisation or enterprise acquiring such information is located (Porteous in Potter, 1998). In the framework of economic intelligence,

Henri Martre (in Potter, 1998) distinguishes between primary and secondary, and tactical and covert economic intelligence. Primary and secondary economic intelligence represent the collection of publicly available information from open sources (the difference is only in the level of difficulty to obtain information); in tactical economic intelligence, information originates from more difficult to access, privileged sources (e.g. consumer research, personal contacts, etc., and includes, for example, internal information on an enterprise, cost and sales analyses, information on studies, development, key projects, etc.); in the case of covert economic intelligence, information is obtained illegally, is confidential and, as such, legally protected.

Economic Intelligence aims to take advantage of this opportunity to develop better methods for the identification of relevant sources of information, the analysis of the collected information and its manipulation to provide what the user needs for decision making. Focused mostly on information available outside the organisation, the scope of Economic Intelligence covers wide fields ranging from technology to market or legal topics and is closely linked to other information management approaches such as Knowledge Management or Business Intelligence (Economic intelligence, 2002). Economic Intelligence concerns the set of concepts, methods and tools which unify all the co-ordinated actions of research, acquisition, treatment, storage and diffusion of information, relevant to individual or clustered enterprises and organisations in the framework of a strategy (Bellinger in Economic intelligence, 2002).

Competitive intelligence is a concept, first used in the 1980s, and developed at Motorola – Jan Herring, an associate expert was the first to use the term *competitive intelligence* in English (Galvin, 1997).

Competitive intelligence is a systematic and ethical programme for collecting, analysing and managing information that can potentially affect plans, decisions and operations of an enterprise. Considering the purposes and goals, competitive intelligence is a process of increasing competitiveness on the market by improving the understanding of enterprise's competitors and its competitive environment. Information can be collected from publicly available sources, and is focused on the competition – its purposes, goals, marketing, etc. Based on this information, the enterprise can adapt its strategy, thus successfully defending against competitor's attempt to reduce its market share or to completely push it out of a specific market. It is also often used to collect and analyse data for proving unfair competition.

Havenga and Botha (2003) define competitive intelligence as an internationally recognised tool that allows organisation to maintain their competitiveness on the global level. Its purpose is therefore to provide support and consultancy to enterprises, which are reflected in management decision making and activities.

As stated by Lönnqvist and Pirttimäki (2006), most European academics define business intelligence as a wide concept that represent management and transformation of business information into intelligence products, with the purpose of providing support in decision making, thus achieving the goals of the organisation. The latter definition thus also includes competitive intelligence, which, according to the definition by the Society of Competitive Intelligence Professionals (SCIP), encompasses monitoring of the competitive environment

and internal activity through an analysis of findings, with the purpose of providing support for the decision-making process. This helps management in enterprises form better decision-making strategies, primarily in marketing, development and investments. In this respect, legality and ethics of collecting information and controlled distribution of intelligence to decision makers is often emphasised. Competitive intelligence is thus defined as a way to provide competitive advantage or facilitate decision making through collecting, analysing and managing information related to the business environment in which an enterprise operates (SCIP, n. d.).

As the widest concept, most Slovenian authors use the term of economic inquiry, which is then further divided into several stages, specifically: business intelligence, competitive intelligence, industry intelligence, due diligence of a good manager, marketing intelligence, social inquiry and defensive economic inquiry (Dvoršak, 2003; Gjerek, 2009; Žaže, 2007).

Dvoršak (2003) defines business intelligence as collecting, organising and utilising data, primarily by management, with the purpose of good decision making, specifically in an ethical and lawful manner.

In light of the above, we can say that definitions of key concepts of corporate security and corporate intelligence represent a certain challenge – or in other words, concepts that must be introduced, presented and established as necessary in organisation, particularly in the time of globalisation and IT development. For this purpose, we describe various aspects of operation, usability and indispensability of these presented concepts, as well as their advantages and potential disadvantages, by presenting the regulatory and legal framework and misuse in light of the discussed subject.

3 ECONOMY AND COMPETITIVE INTELLIGENCE AS A PART OF A BUSINESS PROCESS

Economic activity is any activity that is carried out against payment on the market (Zakon o preprečevanju omejevanja konkurence, 2008). As stated by Črnčec (2008), it is necessary to understand the distinction of intelligence based on the entity conducting such activities. If these activities are carried out by a national intelligence service in the economic field, this represents an economic intelligence. If such activities are carried out by enterprises, this represents competitive intelligence, which is the focus of this article.

The goal of forming a successful strategy in an organisation is to primarily create and maintain a competitive advantage over one's competition. In this way, competitive intelligence represents a source of a more permanent competitive advantage. It is necessary to make sure that it contributes prompt, relevant and analysed products that, together with the know-how of experts in the field of competitive intelligence, help form and manage the organisation's strategy (Hughes, 2005).

Organisations of all types and sizes have always faced the need for information management. Globalisation, the spread of information and communication technologies, the construction of formal and informal networks, the acceleration

of economic change, the evolution of relationships between the makers of finished products and their suppliers, the introduction of customer relationship management, and the shortening of product life cycles, among other things, has led to permanent changes in the day-to-day management of the enterprises (Economic intelligence, 2002).

Facing a growing quantity of data, it is necessary to adopt a pragmatic and primarily effective method for reviewing and managing data and information, which will help decision making in organisations. Today, an entrepreneur without a strategy can obtain a vast quantity of information, which is meaningless if he does not know how it can be used or exploited. Therefore, a good strategy – the result of a dialectic process between the internal situation and external environment – must be adopted. It is also important that all enterprise sectors are included in the needs analysis. The plan for collecting information must be focused on what is most important for the organisation in terms of ensuring competitiveness. The goal of the organisation is to maintain its position on the market or to increase its market share. For this purpose, it is necessary to monitor external factors, primarily legislation and regulation, social and political trends, economic movements, intellectual property and patents, clients, technological development and the global market (Economic intelligence, 2002).

The process of competitive intelligence in organisations must include not only collecting internal and external information from competitors, but also from clients, suppliers, technology, environment, and potential business relationships. In such cases, the process of competitive intelligence provides an early warning system and helps predict activities by competitors, clients and governments (Gilad in Calof & Wright, 2008).

Management of small and medium-sized enterprises must thus face external and internal information. This process – which we can call a comparative analysis – includes primarily three phases, specifically: confrontation, comparison and calibration (Economic intelligence, 2002). In the following chapters, we give a detailed presentation of the types of data collection and the stages of the competitive intelligence process.

3.1 Sources and Types of Data Collection in Competitive Intelligence

The need for an improved information delivery process has become widely accepted over the past decade. For this reason, a growing number of enterprises is considering the options for developing and conducting competitive intelligence processes. They are aware of the value and the applicability of investments into new, modern competences, which are reflected in investment into competitive intelligence programmes (Gračanin, Kalac, & Jovanović, 2015).

Consistent collection of the right information at the right time is based on a continuous process of information and policy established at the level of the European Union (Economic intelligence, 2002).

There are many sources of information on competitors that can be used in the competitive intelligence process. Employees who are in direct contact with clients represent the most important source of information. Competitors have

established extensive communication with their suppliers, clients, distributers, shareholders and levels of government. Contact with these sources can provide plenty high-quality and useful information to an enterprise. Another good source of information is following trade magazines, fairs, advertising, websites, annual reports, etc. In this regard, a careful selection of data sources, data reliability and timely acquisition of information are very important. In most cases, enterprises list the Internet, personal contact, employees, published information and external distribution channels as the most important information sources (Gračanin et al., 2015).

Software providers have developed special software for the competitive intelligence process, which supports the data collection process on competitors, simplifies procedures for data mining and analysis, and supports decision making based on systematic databases. Thus, decision makers can simplify the information collection process and become more effective in competitive intelligence (Gračanin et al., 2015).

Enterprises have two options regarding the agents for the competitive intelligence process, specifically: internal or external providers of competitive intelligence. Enterprises can decide to establish their own departments in charge of systematic data monitoring and analysis, and submission of such data to persons responsible. The latter is primarily suitable for large enterprises and organisations with sufficient human and financial resources available to implement an internal competitive intelligence system. On the other hand, enterprises can hire an external competitive intelligence provider, who will provide the required intelligence products to management. Here, we should emphasise certain advantages of an external system, such as investigators' experience, production of more concrete recommendations and, primarily, time savings (Vrenko Peruško, 2004).

3.2 Stages of Competitive Intelligence Process

In different literature, we can find quite a few versions of the intelligence cycle, which are quite similar. Liebowitz (2006) thus divides the intelligence cycle of competitive intelligence into four stages, specifically: collection, synthesis, analysis, and strategy development. The author emphasises that data and information collection is the most important initial step in competitive intelligence. According to Kahaner (in Anžič, 2010), this step represents the collection of raw data and information from various sources for the purpose of forming the final product. He points out that creative individuals can obtain such information and data legally and ethically. The nest stage – the synthesis stage – represents refining of collected information into meaningful segments and summaries, followed by the analysis stage (Liebowitz, 2006), which is a more productive and future-oriented stage than the synthesis stage. According to Kahaner (in Anžič, 2010), the analysis is the most complex stage of the intelligence cycle. It requires exceptional decisiveness, resourcefulness and analytical expertise, as it needs to find patterns and obtain information, and finally meaningfully shape said information and form well-founded conclusions about the results. Thus, the purpose of the analysis is to generate intelligence products that help an organisation strategically improve

decision making. In the competition and environment analysis stage, enterprises have to focus only on specific information. The latter is essential for the general success and effectiveness of an enterprise, as managers cannot use all acquired information at every moment (Gračanin et al., 2015). The last stage of the process is called strategy development, which includes both short-term and long-term development of a business strategy in an enterprise. Along with strategy development, new needs are arising for information and data for the purposes of adapting the strategy of the organisation, which results in a new competitive intelligence cycle (Liebowitz, 2006).

The review of literature has shown that different authors list different variations of intelligence cycle, which have four to eight separate stages or phases on average. These differences are mostly different names of individual stages and different breakdowns of the cycle; however, individual stages are very similar in terms of content.

In all organisations, the intelligence cycle of competitive intelligence starts on the basis of the same needs. Once demand and goals for information are determined in an enterprise, the process of collection, storage and analysis of available information is implemented, focusing on obtaining answers required for easier decision making and action. Throughout the data collection process, feedback is very important, ensuring that the intelligence process can be adapted, as it has to be constantly adapted to new changes in the world (Economic intelligence, 2002).

Another version of the intelligence cycle includes multiple stages, and on every individual step, the consequences have to be resolved (Economic intelligence, 2002). Objective represents a starting point, from which we progress to data collection. Process data results in storing of data, and with dissemination the analysis is performed. The next step is action, which proceeds again to the objective, although if during analysis the additional information is required, we must return to data collection. Moreover, if the redefinition is needed, the action phase is skipped, and we continue with setting the objective.

The intelligence cycle is a transformation of a mass of data, available in various forms, first into information, then into knowledge, and ultimately into 'intelligence' or intelligence product (Economic intelligence, 2002).

3.3 Open Source Intelligence (OSINT) as Data Collection Method in the Corporate Intelligence

As also recognized by Britovšek, Tičar and Sotlar (2017), the data collection as one of the fundamental elements of intelligence can be categorized according to different intelligence disciplines, among which collecting from publically available sources in the form of the open source intelligence (OSINT), along with human intelligence, signals intelligence and imagery intelligence, represents one of key processes of identifying and retrieving information necessary to support legal decision-making. Britovšek et al. (2017) point out OSINT as crucial in collecting and analysing the data in the private sector, where private citizens are limited mainly to open source collection. Other entities or rather subjects of public

and private security sector have broader range or certain legal entitlements that enable them to collect beyond OSINT, still open source intelligence remains one of the most recognized aspect of data collection as found in their study - 86 % of respondents who perceive their work as private intelligence or counterintelligence uses OSINT (Britovšek et al., 2017).

OSINT as one of the stages of competitive process. The intelligence community has been involved in OSINT for a better half of century, and is defined as "intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement" (Williams & Blum, 2018). If anything, OSINT has become more complex in terms of sources and methods with the evolution of internet and the rise of social media. As such its crucial aspect is and will be a legal point of view in gathering the information, even if from open sources. Protecting the individuals, managing massive quantities of data, leveraging private sector tools and entities to the fullest possible extent, are only a few of possible problematic areas of OSINT use. Exploitation of open source intelligence brings with a wide variety of legal dilemmas, which connect to the privacy and data protection, primarily (but not exclusive to) the collection and retention of information in regard to social media data and in accordance to the Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). The dynamics of social media - in comparison with news media and legally attainable literature, where these (and other) aspects are less present or even non-existent - carry with a huge responsibility for the intelligence collectors and analysts. Besides privacy and data protection, Cuijpers (2013) argues the domain of intellectual property rights as another legal point of view, which should also be acknowledged when dealing with OSINT as corporate intelligence. Those issues alone argue the importance and dependence on national legislation.

The technology holds various and broad aspects of intelligence operations, arising new questions about ethics and legal challenges for the intelligence community. Eijkman and Weggemans (2013) argue even the OSINT's increased use of open source information needs to be balanced for safety and security purposes by assessing what accountability in a digital world should entail (in regard to state security entities). Taking that to the private sphere and using it in the corporate world, takes it up a notch, as we point out in the next chapter on normative framework for data collection.

4 NORMATIVE FRAMEWORK FOR DATA COLLECTION IN THE REPUBLIC OF SLOVENIA

Private intelligence companies are limited to publicly available data in data collection and acquisition. The latter is defined in provisions of certain laws listed below.

The Companies Act (Zakon o gospodarskih družbah [ZGD-1], 2006) defines the concept of trade secret, with the enterprise setting the way such trade secret is protected and the responsibility of persons obligated to protect it. Any actions, whereby persons outside the enterprise try to obtain data considered a trade secret, is prohibited, if such actions violate the law and enterprise's intention.

Since April 2019, the Trade Secrets Act (Zakon o poslovni skrivnosti [ZPosS], 2019) is also in effect, which transposes into the Slovenian legal framework the EU directive aiming to standardise the concept of trade secrets within the EU and to provide adequate and harmonious levels of modern protection. Consequently, a new law would introduce increased transparency and raise the level of protection for trade secrets, thereby indirectly affecting the protection of knowledge, experience and business information of enterprises, their competitiveness and performance.

Article 1 of ZPosS (2019) states that the act "regulates the area of trade secrets, rules for determining and protecting trade secrets against their unlawful acquisition, use and disclosure," thus defining right at the start the three most common risks threating trade secrets. ZPosS (2019) provides a new definition of trade secret as follows: "A trade secret includes undisclosed know-how and business information that meet the following requirements: – is a secret that is not generally known or easily accessible to persons in circles groups that normally handle such type of information; – has a market value; – the holder of trade secret has taken reasonable actions to keep it secret in given circumstances."

ZPosS (2019) defines a lawful acquisition, use and disclosure of trade secret, as well as unlawful acquisition, use and disclosure of trade secret. The acquisition of trade secret is considered lawful "if it is obtained by independent discovery or creation; observation, study, dismantling into components or testing of product or object that was made available to the public or is legally owned by the acquirer who is under no applicable legal obligation restricting acquisition of trade secret; exercising a right of workers or worker representatives to information and consultation in accordance with applicable regulation, when such a disclosure is required for that purpose; any other action considered in compliance with fair business practices under the given circumstances, or exercising a right to access public information". Furthermore, a trade secret is acquired lawfully if the acquisition, use or disclosure of trade secret is defined by another law or EU regulation, if the party is ordered to do so by a final and enforceable court decision, or if the party is required to do so for the purposes of an investigation by the inquiry commission of the National Assembly of the Republic of Slovenia.

Article 5 of ZPosS (2019) defines unlawful acquisition of trade secret as an acquisition "carried out by direct unauthorised access, theft or copying of documents, objects, material, content or electronic files that contain a trade secret or could help discover a trade secret, or by any other action that is considered in violation of fair business practices", or "if obtained from a person who used or disclosed a trade secret unlawfully, and the acquirer was aware or should have been aware of this at the time". In Article 5, ZPosS (2019) defines unlawful use and disclosure of trade secret as use or disclose by third party that meets one of the following conditions: (1) the trade secret was acquired unlawfully; (2) the person

violates a confidentiality agreement or other obligation of non-disclosure in relation to the trade secret; (3) the person violates a contractual or other obligation to restrict use of the trade secret; (4) at the time of use or disclosure, the person was aware or should have been aware that the trade secret acquired from another person was used or disclosed unlawfully. Furthermore, unlawful use of trade secret includes "producing, offering or making available on the market of any goods that is the subject of a violation, or importing, exporting or warehousing for these purposes, when the person that is carrying out any of these activities was aware or should have been aware under the given circumstances that the trade secret was used unlawfully".

Additionally, Article 8 of the Industrial Property Act (Zakon o industrijski lastnini [ZIL-1], 2001) defines the official confidentiality of records regarding a patent application and model application in the official newsletter of the industrial property office.

The Obligations code (Obligacijski zakonik [OZ], 2001) also defines the observance of the principals of good faith and fair dealing in concluding contractual obligations, exercising rights, and performance of duties on the basis of such obligations. In their transactions, parties with contractual obligations must act according to the principle of good business practices.

Ultimately, the two most important laws in this regard are the Classified Information Act (Zakon o tajnih podatkih [ZTP], 2001), which, amongst other things, provides specifics on the handling of classified information for all persons that were given access or became aware of such information, and the Criminal Code (Kazenski zakonik [KZ-1], 2008), which defines criminal offences and relevant criminal sanctions.

An enterprise is allowed to acquire and analyse data from publicly available sources, but has no right to encroach on an individual's right to privacy (Britovšek, 2017). The Private Detective Services Act (Zakon o detektivski dejavnosti [ZDD-1], 2011) gives special status to detectives, who are allowed under certain circumstances to use specific methods for collecting data. Here we should point out the following entitlements of detectives, as listed in Article 27 of ZDD-1 (2011):

- collection of data from persons or publicly available sources
- acquisition of data from licences
- acquisition of data based on personal perception
- use of technical means for data acquisition

As part of collection of data from persons or publicly available sources, a detective may collect information directly from persons to which such data refers to, as well as from persons who have such data at their disposal if it is submitted voluntarily, and from publicly available sources. Furthermore, per written authorisation of a client, a detective may acquire data from certain records (records of registered vehicles, records of permanent residency and central population register, records of insured persons, aircraft register and the Slovenian register of ships). A detective may also access court and administrative files, and copy data from such files when the party that authorised the detective is entitled to do so (ZDD-1, 2011).

A detective may obtain information by direct personal perception in public places or from public places, publicly accessible closed and open spaces, and places and spaces visible from publicly accessible places and spaces. Doing so, a detective may not encroach on private closed spaces and private spaces that an individual has separated from public spaces by erecting any type of fence, obstacle or visible marking or warning, thus clearly indicating the presence of a private space. As part of their duties arising from the authorisation, a detective employing personal perception may use image-recording devices, but only when necessary for the preservation of evidence. A detective may also use audio-recording devices or other tools for the preservation of evidence and leads. A detective may use audio-recording devices exclusively on the basis of a clearly demonstrated written or recorded verbal approval by the person against whom such a device will be used (ZDD-1, 2011).

4.1 Risks Arising from Data Abuse

As defined by the Prevention of Restriction of Competition Act (Zakon o preprečevanju omejevanja konkurence, 2008), unfair competition represents actions by an enterprise on the market that violate good business practices, thereby causing or potentially causing damage to other enterprises. Actions of unfair competition in terms of data acquisition include primarily submission of data on another enterprise, if such data harms the reputation and business of another enterprise, and unlawful acquisition of another enterprise's trade secret or unjustified exploitation of confidential trade secret of another enterprise.

Based on EU rules on the protection of free competition, certain practices are especially forbidden. Sanctions for abuse may be fines (up to 10% of their annual turnover) or imprisonment, with special attention being paid to enterprise directors who have violated regulations. All EU members must apply and observe the competition rules, with courts having competence over supervision and compliance with rules. The rules apply to all enterprises as well as organisations whose main activity is of an economic nature (European Union, Your Europe, 2018).

Within the competition rules, we should point out unlawful contacts and agreements between enterprises or organisations, referred to as "cartels", which limit competition. The most common examples of such agreements are production limits, pricing, market division, allocation of clients, and distribution agreements between suppliers and sellers. All exchanges of information and agreements between enterprises and their competitors are considered anti-competitive practice, reducing the strategic uncertainty on the market. Disclosure of such information via telephone, e-mail, or in meeting can represent a violation of the rules. It is therefore best for enterprises not to limit production, not to exchange strategic information regarding the enterprise, not to set conditions of operations and prices, and not to share their markets. When agreements benefit the economy and consumers (listed in the Decree on block exemptions), they are not prohibited. If an enterprise has a dominant position on the market because of its large market share, it has no ensure price regulation. This means that the enterprise may not

charge unreasonably low prices that would restrict the business of other competing enterprises. Furthermore, an enterprise may not charge too high prices, set special business conditions for business partners, or cause discrimination among consumers (European Union, Your Europe, 2018).

Restrictions on competitive conduct are also set by the prohibition on competition and the non-compete clause. The prohibition of competition binds a worker in an employment relationship to be loyal to the enterprise, while the non-compete clause refers to the period after employment, when the worker no longer has a contractual relationship with the enterprise. During the employment relationship, the worker is obliged to refrain from all actions that would harm the enterprise, which means the prohibition of competitive activity. The worker must not carry out any activity or conclude transactions for non-commercial or commercial activity for their own account or account of others, worker's activity must not include activities carried out by the employer and which could represent competition to the employer, except with the approval of the employer. If the worker violates this obligation, the worker is liable for damages and subject to disciplinary action, which can result in termination of the employment contract. After the employment contract is terminated, the worker is bound by the non-compete clause, which is admissible only if the worker obtained specific knowledge and contacts that could be used to compete with the former employer. Its effect is therefore time-limited (Senčur Petek, 2016).

Enterprises and organisations often face issues of protection of trade secrets. "Any data determined as such by the enterprise management with a written decision is considered a trade secret. Company members, workers, members of corporate governance bodies and other persons obligated to protect a trade secret must be notified of such a decision. Even if data is not defined as a trade secret by a decision from the previous paragraph, data that would obviously cause significant damage if disclosed to an unauthorised person is also considered a trade secret. Company members, workers, members of corporate governance bodies and other persons are liable for disclosure of trade secret if they were aware or should have been aware of the nature of such data." (ZGD-1, 2006, Article 39)

A trade secret data has two main characteristics. The data is confidential and known to a certain group of persons; therefore, it should only be known to this pre-determined group of persons, who are not allowed to submit this data or disclose it to third parties or use it in any other way. The reason for confidentiality of trade secret must have a market value (TehnoCenter of the University of Maribor, n. d.). When a trade secret is determined by a written decision, it is necessary to precisely specify the group of persons who are aware of this secret, their responsibilities and method of protecting the trade secret. In this case, the law defines three categories of persons who are obligated to protect the trade secret: persons within the enterprise (employees, company members, etc.), persons who work for the enterprise on the basis of civil-law contracts, and persons outside the enterprise who are aware of the specific trade secret (Šutanovac, 2017).

5 CONCLUSION

From its humble beginnings, where is primarily existed within the sphere of private security (in detective and private security enterprises), the use of intelligence in western enterprises managed to developed into a unique market tool, which provides the highest benefit to global multinational corporations. State borders do not represent an obstacle to the use of intelligence, and such efforts to obtain competitive advantages and to identify potential risks today benefit not only enterprises but also states. In accordance with the legislation and considering the normative and legal framework, organisation utilise corporate intelligence both for protecting their know-how, interests and secrets, and to manage risks related to information leaks or thefts (Britovšek et al., 2017).

Considering the nature of information that is the subject of intelligence, methods of acquisition and the transfer of tools from the above-mentioned sphere of private security and originally regulated intelligence services as part of national (counter) intelligence entities, we must highlight the potential shortcomings arising from the transfer of such activities to the private sphere. The need for information and their significance can potentially lead to pressure on an enterprise, which, in the process of acquiring the best or most reliable information, can get dangerously close to the line between acceptable and not-acceptable, or endangering the rights and freedoms such as privacy.

Findings by the Global Intelligence Alliance have shown that most enterprises face the need for better understanding of the complexity of external environment, and integration of such understanding into strategically planned projects (Calof & Wright, 2008). It was found that most enterprises have a need for more formal intelligence. The study had also shown that almost two-thirds of respondents in the last five years were subject to at least three large competitive events. As many as 97% of respondents replied that their enterprise has a too weak early warning system (Gilad in Calof & Wright, 2008).

The first positive effect of the electronic age is undoubtedly the availability of information. Most required information is easily accessible and often without additional expenses (Gračanin et al., 2015). As a result, commercial and other organisations that face the need for acquiring information and data are have a major advantage. However, it is up to them how, in what way and particularly to what extent they intend to focus their attention on (competitive) intelligence. According to Britovšek et al. (2017): "With the pursuit of profit in the private sphere, there is often increased willingness to abuse information and the information acquisition technology; consequently, laws are violated, and basic human rights such as the right to privacy are threatened." Private enterprises that conduct such activities are not subject to supervision that applied, or applies, to intelligence and security services of democratic states, whose supervision is clearly defined and activities strongly regulated. Organisations can defend against competitive intelligence with private counter-intelligence, which represents the same risks, as it includes strong protective measures (Britovšek et al., 2017).

In organisations that participated in the study by the Competitive Intelligence Foundation, the competitive intelligence process was directed towards the following goals: new or increased revenue, new product or service, cost reduction or avoidance, time savings, increased profit, and achieving financial goals.

They focused primarily on key intelligence subjects, such as enterprise profiles, comparative analysis of enterprises, early warning system, industry trends, buyer and supplier profiles, technology assessment, economic or political analysis, and profile implementation. The latter led to very good results in the following areas: development of entrepreneurial or business strategy, sales or business development, market entry decisions, product development, research and development decisions, merger and acquisition decisions, joint venture decisions, and legislative responses (Competitive Intelligence Foundation, 2006).

We can surmise that competitive intelligence affects a wide range of decision making and is an indispensable in developing short-term and long-term business strategy in an organisation or enterprise, particularly if we consider the global operations of organisations and IT development, which opens up organisations to new possibilities and, ultimately, threats. The success of business operations is inevitably linked to the acquisition, collection and analysis of information from legally obtained sources using business and competitive intelligence, as the selection between relevant and irrelevant information enables decision-makers to effectively make their presence in global markets. Corporate intelligence thus represent a necessary security element in every organisation, and particularly those that are globally oriented. As such, corporate intelligence is a vital and indispensable part of the modern global business world and represents its new reality.

REFERENCES

Aksentijevic Forensic and Consulting. (n. d.). *Integral security (CSO)*. Retrieved from http://www.ict-forensics-consulting.com/management-consulting/integral-security-cso/

Anžič, M. (2010). *Konkurenčna obveščevalna dejavnost gospodarskih družb* (Magistrsko delo) [Competitive intelligence in companies (Master's thesis)]. Ljubljana: Fakulteta za družbene vede.

Britovšek, J. (2017). *Zasebna obveščevalna dejavnost v Republiki Sloveniji – Teoretični, pravni in praktični vidiki* (Doktorska disertacija) [Private intelligence in the Republic of Slovenia – A theoretical, legal and practical perspectives (Doctoral disseration)]. Ljubljana: Fakulteta za varnostne vede.

Britovšek, J., Tičar, B., & Sotlar, A. (2017). Private intelligence in the Republic of Slovenia: Theoretical, legal, and practical aspects. *Security Journal*, *31*(2), 410–427.

Calof, J. L., & Wright, S. (2008). Competitive intelligence: A practitioner, academic and inter-disciplinary perspective. *European Journal of Marketing*, *42*(7/8), 717–730.

Competitive Intelligence Foundation. (2006). Competitive intelligence: A competitive intelligence foundation research report, 2005–2006. *Review of Innovation and Competitiveness, 1*(1), 25–44.

Črnčec, D. (2008). *Obveščevalna dejavnost v javnem in zasebnem sektorju (Gospodarska vs. konkurenčna obveščevalna dejavnost)* (Doktorska disertacija) [Intelligence in the public and private sector (Business vs. competitive intelligence (Doctoral disseration)]. Ljubljana: Fakulteta za družbene vede.

Cuijpers, C. M. K. C. (2013). Legal aspects of open source intelligence: Results of the VIRTUOSO project. *Computer Law and Security Review*, *29*(3), 642–653.

Dvojmoč, M. (2019). Integralna korporativna varnost [Integral corporate security]. *Varstvoslovje*, *19*(3), 252–272.

Dvoršak, A. (2003). Zbiranje relevantnih podatkov o proizvodnji, konkurenci in poslovanju: Industrial intelligence & competitive intelligence & business intelligence [Gathering relevant data on production, competition, and operations: Industrial intelligence & competitive intelligence & business intelligence]. In M. Pagon (Ed.), *4. Slovenski dnevi varstvoslovja* (p. 144). Ljubljana: Visoka policijsko-varnostna šola.

Eijkman, Q. A. M., & Weggemans, D. (2013). Open source intelligence and privacy dilemmas: Is it time to reassess state accountability? *Security and Human Rights*, *23*(4), 287–296.

Economic intelligence: A guide for beginners and practitioners. (2002). CETISME. Retrieved from https://www.madrimasd.org/uploads/CETISME-ETI-guide-english.pdf

European Union, Your Europe. (2018). *Competition rules in the EU.* Retrieved from https://europa.eu/youreurope/business/selling-in-eu/competition-between-businesses/competition-rules-eu/index_en.htm

Galvin, R. W. (1997). Competitive intelligence at Motorola. *Competitive Intelligence Review, 8*(1), 3–6.

Gjerek, B. (2009). *Taktika in metodika dela gospodarskih poizvedovalcev* (Specialistična naloga) [Work tactics and methodology of economic inquirers (Specialist thesis)]. Ljubljana: Fakulteta za varnostne vede.

Gračanin, Š., Kalac, E., & Jovanović, D. (2015). Competitive intelligence: Importance and application in practice. *Review of Innovation and Competitiveness, 1*(1), 25–44.

Havenga, J., & Botha, D. (2003). *Developing competitive intelligence in the knowledge-based organisation*. Retrieved from https://pdfs.semanticscholar.org/586a/8f6d76390e17f75ec9bc8ebe6a28cd66ffef.pdf

Hughes, S. (2005). Competitive intelligence as competitive advantage: The theoretical link between competitive intelligence, strategy and firm performance. *Journal of Competitive Intelligence and Management*, *3*(2), 3–18.

Kazenski zakonik (KZ-1) [Criminal Code]. (2008, 2009, 2011, 2012, 2015, 2016, 2017). *Uradni list RS*, (55/08, 66/08, 39/09, 91/11, 50/12, 54/15, 6/16, 38/16, 27/17).

Liebowitz, J. (2006). *Strategic intelligence: Business intelligence, competitive intelligence and knowledge management*. Boca Raton: Auerbach Publications.

Lönnqvist, A., & Pirttimäki, V. (2006). Measurement of business intelligence. *Information Systems Management*, *23*(1), 32–40.

Müller-Wille, B. (2004). *For our eyes only? Shaping an intelligence community within EU* (EU-ISS Occasional paper, no. 50). Paris: European Union Institute for Security Studies.

Obligacijski zakonik (OZ) [Obligations Code]. (2001, 2004, 2007, 2016, 2018). *Uradni list RS*, (38/01, 32/04, 40/07, 64/16, 20/18).

Potter, E. H. (1998). *Economic intelligence and national security*. Ottawa: Carleton University Press.

Purg, A. (1995). *Obveščevalne službe: Povezave med obveščevalnimi sistemi in državno suverenostjo v luči modela sodobnega iskanja obveščevalnega sistema Republike Slovenije* [Intelligence services: Connections between intelligence systems and

national sovereignty in light of the modern search model for an intelligence system of the Republic of Slovenia]. Ljubljana: Enotnost.

Senčur Petek, D. (2016). Konkurenčna prepoved in konkurenčna klavzula [Prohibition on competition and non-compete clause]. *Anali PAZU HD, 2*(1), 27-43.

Society of Competitive Intelligence Professionals (SCIP). (n. d.). *Integrated strategic competitive intelligence best practices*. Retrieved from https://www.scip.org/page/AssessmentGuidebook

Šutanovac, L. (January 18, 2017). *Odgovor strokovnjaka: Poslovna skrivnost* [Expert's reply: Trade secret]. Ljubljana: Zavod mladi podjetnik. Retrieved from https://mladipodjetnik.si/novice-in-dogodki/novice/odgovor-strokovnjaka-poslovna-skrivnost

TehnoCenter of the University of Maribor. (n. d.). *Trade secret.* Retrieved from http://www.intelektualna-lastnina.si/druge-pravice/poslovna-skrivnost

Ulcej, D., Britovšek, J., & Sotlar, A. (2011). Obveščevalna dejavnost v gospodarstvu: Pojmovne opredelitve [Economic intelligence: Definitions]. In T. Pavšič Mrevlje (Ed.), *11. Slovenski dnevi varstvoslovja*. Ljubljana: Fakulteta za varnostne vede. Retrieved from https://www.fvv.um.si/dv2010/zbornik/nacionalna_varnost/britovsek_ulcej_sotlar.pdf

Vrenko Peruško, I. (2004). *Business intelligence: Oči in ušesa uspešnih podjetij* [Business intelligence: Eyes and ears of successful enterprises]. Retrieved from http://www.gfk.si/4_2_lclank.php?cid=2010

Williams, H. J., & Blum, I. (2018). *Defining second generation open source intelligence (OSINT) for the defense enterprise*. Santa Monica: RAND. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf

Zakon o detektivski dejavnosti (ZDD-1) [Private Detective Services Act]. (2011). *Uradni list RS*, (17/11).

Zakon o gospodarskih družbah (ZGD-1) [Companies Act]. (2006, 2008, 2009, 2011, 2012, 2013, 2015, 2017, 2019). *Uradni list RS*, (42/06, 60/06, 10/08, 68/08, 42/09, 33/11, 91/11, 32/12, 57/12, 82/13, 55/15, 15/17, 22/19).

Zakon o industrijski lastnini (ZIL-1) [Industrial Property Act]. (2001, 2002, 2004, 2006, 2013). *Uradni list RS*, (45/01, 96/02, 37/04, 20/06, 100/13).

Zakon o poslovni skrivnosti (ZPosS) [Trade Secrets Act]. (2019). *Uradni list RS*, (22/19).

Zakon o preprečevanju omejevanja konkurence [Prevention of Restriction of Competition Act]. (2008, 2009, 2011, 2012, 2014, 2015). *Uradni list RS,* (36/08, 40/09, 26/2011, 87/11, 57/12, 33/14, 76/15).

Zakon o tajnih podatkih (ZTP) [Classified Information Act]. (2001, 2003, 2006, 2010, 2011). *Uradni list RS,* (87/01, 101/03, 28/06, 9/10, 60/11).

Žaže, S. (2007). *Meje dovoljenosti gospodarskega poizvedovanja* (Specialistična naloga) [Boundaries of Permissibility of Economic Inquiry (Specialist thesis)]. Ljubljana: Faculty of Criminal Justice and Security.

About the Author:

Miha Dvojmoč, PhD, Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: miha.dvojmoc@fvv.uni-mb.si