Denis Caleta[1], **Anita Peresin**[2]

STRATEGIC SECURITY DECISION-MAKING PROCESS IN CORPORATE ENVIRONMENT USING OPEN SOURCES INFORMATION

Globalization of the world and the globalization of security confront society with the dilemma how to continue development, based on the basic postulates of free movement of goods, services and people, mitigating threats and risks. We further define dilemmas and factors related to the role of supporting strategic decision-making process with the help of intelligence analysis based on the data and information derived from publicly available sources. The purpose of this paper is also to analyze the factors in the interaction between public and private environments, especially in terms of intelligence products use. We are located in a period where certain corporations have in the wind of globalization outgrown the exclusive influence of nation-states. Important information is becoming a tool for multinational corporations to achieve their strategic objectives. Corporate security environment aims at maximizing risks, which could adversely affect the continuity of business processes. Intelligence process, based primarily on the collection of information from publicly available sources, is becoming an effective tool in strategic management to promote the strategic interests of corporations.

Keywords: *corporate security; open sources information; intelligence analysis; security decision-making; public-private partnership.*

Деніс Калета, Аніта Перешин

ПРИЙНЯТТЯ РІШЕНЬ ЩОДО СТРАТЕГІЧНОЇ БЕЗПЕКИ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ З ВИКОРИСТАННЯМ ПУБЛІЧНОЇ ІНФОРМАЦІЇ

У статті показано, що глобалізація в цілому та глобалізація безпеки зокрема значно ускладнили подальший економічний розвиток, заснований на вільному русі товарів, послуг та людей. Виявлено дилему та чинники, що визначають роль процесів прийняття стратегічних рішень з використанням інтелектуального аналізу даних, доступних з публічних джерел. Окремо визначено чинники, що впливають на взаємодію державного та приватного середовища у контексті використання інтелектуального продукту. Акцент зроблено на тому, що ми живемо в час, коли інтереси корпорацій стали вищими за інтереси держав, а інформація є найважливішим інструментом досягнення стратегічних цілей підприємства. Зовнішнє середовище існування постійно максимізує ризики, які становлять загрозу для внутрішніх бізнес-процесів, і саме інтелектуальний аналіз публічної інформації може стати ефективним інструментом стратегічного менеджменту.

Ключові слова: *корпоративна безпека; джерела публічної інформації; інтелектуальний аналіз даних; прийняття рішень з безпеки; державно-приватне партнерство.*
Літ. 17.

Денис Калета, Анита Перешин

ПРИНЯТИЕ РЕШЕНИЙ ПО СТРАТЕГИЧЕСКОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНОЙ СРЕДЕ С ИСПОЛЬЗОВАНИЕ ПУБЛИЧНОЙ ИНФОРМАЦИИ

В статье показано, что глобализация в целом и глобализация безопасности в частности поставили под вопрос дальнейшее экономическое развитие, основанное на

[1] PhD, Assistant Professor, Faculty of State and European Studies, President of the Board, Institute for Corporative Security Studies, Slovenia.
[2] PhD, Faculty of Political Science, University of Zagreb, Croatia.

свободном передвижении товаров, услуг и людей. Выявлены дилеммы и факторы, определяющие роль процессов принятия стратегических решений с использованием интеллектуального анализа данных, доступных из публичных источников. Отдельно определены факторы, влияющие на взаимодействие государственной и частной среды в контексте использования интеллектуальных продуктов. Акцент сделан на том, что мы живём в то время, когда интересы корпораций стали выше интересов государств, а информация стала важнейшим инструментом достижения стратегических целей предприятий. Внешняя среда существования постоянно максимизирует риски, которые являются угрозой для внутренних бизнес-процессов, и именно интеллектуальный анализ публичной информации может стать эффективным инструментом стратегического менеджмента.

Ключевые слова: *корпоративная безопасность; источники публичной информации; интеллектуальный анализ данных; принятие решений по безопасности; государственно-частное партнёрство.*

1. Introduction

Success and quality of management are greatly measured by the capabilities of making high quality and due decisions that are important for strategic planning and the implementation of long-term goals necessary for the increase of effective businesses. Contemporary business environment, as a result of globalization, greatly changes the way of conduct and business activities of big corporations. In such circumstances companies have significantly changed their activities outside national borders, while new security challenges influenced their strategic management and planning. Current asymmetric threats do not represent solely threats to state structures but also a great threat to the economy, business and private sector. All of that requires a special type of adaptation for corporations. They need to create resiliency for business activities in the new security environment. Important segment of this process represents the development of corporative security measures that are able to encompass not only physical protection measures but the organization of the system for the collection and exchange of information, as well as establishing a system for policing and recovery in the case of breakdown or attack. Traditional security systems that are mostly fully established and counted on state capacities and abilities, proved insufficient under current conditions. New circumstances require new types of responses that countries alone are not able to achieve. One of these models is the development of public-private partnership in security, where it is necessary to encourage and develop wider cooperation with the aim of promoting partnership between public and private sector in the fight against new security threats and perils.

Traditional models of data collection important for due detection of security perils were mostly in the domain of state and its intelligence services (Podbregar, Ivanusa, 2010). At the same time, companies acting (because of their size, number of employees and the influence at the market) were observed through the prism of national interests from whence also came the interest of state to cede specific intelligence important for national companies. The structure of contemporary corporations with fully or partially foreign ownership, multinational structure in more than one national state, opens a number of questions related to the achievement of cooperation with national intelligence systems.

This paper proposes that for strategic decision-making in contemporary transnational business environment, collection and high-quality data analysis from open sources is the key aspect. Furthermore we examine the level of importance that strategic management in companies in Slovenia give to such collected and analyzed information in strategic decision-making. The Republic of Slovenia is chosen as a pilot project in our research, that will in the second phase include the region of South-Eastern Europe, in which we observe the attitudes on the development of public-private partnership models as a new instrument of enabling synergic acting of public and private sectors with the aim of perceiving and decreasing risks and perils the transitional societies are facing. The model of public-private partnership in security should allow bidirectional exchange of information necessary for the formation and protection of stable security environment which is in the interest of both public and private sectors.

2. Importance of relevant information for decision-making process

Decision-making is one of the most important aspects of modern management and its primary function, essential for planning, organizing, directing, controlling and staffing. In respect to volatile conditions and environments in which corporations operate, the capacity for timely gathering of accurate and useful information, as well as the quality of their analysis and processing, more than ever before becomes essential for strategic decision-making.

Therefore it is necessary to continuously work on the development of corporate strategy and other data gathering skills to enable effective business activities of companies in the complex and dynamic environment, as well as the development of knowledge of possible future security threats that could have a negative impact on businesses and how to respond to them rapidly and effectively. Due to the need for the development of more effective responses to new security challenges, Underwood (2002) believes that business intelligence should be replaced by corporate intelligence, to indicate the full width of the intelligence role and function within any organization or company. As the societies' disfunctionality increases, so does the violence in the working environment and the appearance of asymmetric threats. Underwood argues that they need to embrace corporate intelligence as the new foundation of corporation management.

For the purposes of strategic decision-making, intelligence, according to Underwood (2002) must focus on 5 areas: global, national, regional, corporate perimeter and corporate premises. This means that every company must develop response strategies against every potential threat, from global to the internal ones.

Corporate intelligence, in the businesses of the 21st century must be able to effectively deal with threats near and far, as well as inside and outside companies and state where they operate. A systematic approach to planning and preventing the impacts of asymmetric threats on companies is extremely important. Coleman (2006) defines 3 key areas that can help businesses lower their corporate risks: planning, education and compatibility. All 3 areas demand cooperation between public and private sectors. Furthermore, Coleman emphasizes the importance of information exchange between private and public sectors, joint and synchronized education and the necessity of all public and private security personnel, law enforcement officers to be properly trained and equipped to deal with foreseeable threats.

From the state and its intelligence services perspective, open source data named by Hulnick (2002) as "lifeblood of intelligence" have a great importance in the final quantity of all the collected data. That is also proven by the statistic data on the proportion of open source intelligence in the total quantity of the gathered intelligence data it is between 70–80%. In the private sector, the use of any information outside the open source domain, such as industrial espionage or electronic intercept, is a criminal act. This is why they are more focused on establishing analytical services for corporations, as well as on the development of data collecting instruments. Open source, on which the private sector intelligence analysts rely, as explained by Hulnick, could also include "grey intelligence".

3. Collection and analyses of open source information

Rapid development of technology has influenced the dynamics of state's responsibility in the area of security. Eijkman and Weggemans (2012) state the police, the intelligence and security agencies increasingly rely on the collection of data from open sources (Open Source Information – OSINF). OSINF as row data represents the database for Open Source Intelligence (OSINT) which is gathered through publicly available sources. Eijkman and Weggemans emphasize that as a result of rapid development of the Internet, such data have become widely available nowadays, and the new OSINT strategies use them evermore as the significant tool for timely prediction of threats to national security, especially asymmetric ones. Thus, new term has emerged – open source intelligence, defined as "intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement" (NDAA, 2006).

Nonetheless, users of OSINT are exposed to new challenges that spring from overwhelming amount of data that needs to be analyzed, sorted and linked. Dupont (2003) believes that fusing and integrating previously unlinked platforms, technologies and resources into holistic intelligence systems will be a defining trend of the next decade. Despite these challenges, Hulnick (2002) considers OSINT as the key factor of intelligence activities in the future, thus supporting Steels' (2000) statements that OSINT is an "intelligence multiplier" if used correctly.

There is no doubt that good open source intelligence can significantly improve prevention capabilities as a part of decision-making. Bean (2007) points to the problem of management and demarcation of OSINT from other types of intelligence and information inside intelligence agencies and between intelligence agencies and private sector contractors. In his research, Bean observed the striking disconnect between the discourse surrounding OSINT and its actual production, uses, and effects. According to this author, it is necessary to conduct a wider investigation on how the concept of OSINT functions as an organizational symbol and site of contestation in the intelligence reform. Stakeholders, including government officials, policymakers, and contractors, he explained, should be able to use certain strategies to construct and negotiate the concept of OSINT to meet particular goals and objectives.

OSINT also has its downsides: contingencies, including information glut, unreliability, misinformation and disinformation, translation requirements, and availability of information to adversaries that limit the utility of OSINT (Hulnick, 2003:565),

making Pringle (2003) conclude that "its inherent ambiguity diminishes its usefulness". Despite this, the OSINT industry has significantly increased during the last decade in Europe. Its users are increasingly becoming states, corporations, private companies and even the EU institutions (Hayes, 2010).

4. New paradigm in relations to public and private cooperation in sharing security relevant information

Expressed negative sides of open source information could be overcome in cooperation with the private sector (Hulnick, 2002), that develops techniques of sorting and delivery of raw data, to assist state intelligence analysts. That's how, for example, In-Q-Tel was created as "a private, non-profit, venture capital company set up and financed by the CIA in late 1999 to get a better bead on innovative technology the intelligence crowd might put to use" (Cortese, 2001). Additional initiatives, Cortese stresses, are designed for data mining and knowledge management to detect patterns or anomalies in the vast trims of raw data.

Some authors analyzed public services and private sector approach to OSINT. Harris (2005) believes that private sector should have a significant role in gathering, analyzing and distribution of OSINT. Bean (2007) talks of multimillion industries that employ thousands of analysts worldwide, but warns not to forget that government and industry have different paradigms of thought. Governments' goal is to centralize collection of OSINT in order to lower expenses, while private OSINT providers benefit from fragmented market as they can resell their products to multiple consumers. Final outcome also differs for governments and commercial users of private OSINT providers. Reliability of OSINT information could be inadequate for intelligence community. The best results could be expected when there is a partnership between analysts using classified intelligence and open source intelligence, thus avoiding the dilemma of information quality vs. information efficiency, as pointed by DeLone and McLean (2003). These authors explain that when security agencies order OSINT from private companies, their main goal is to achieve high level of information quality, what for them means information and conclusions based on unique, specialized and expert analysis, but also ability to track and check sources. On the other hand, private OSINT providers are preoccupied with information efficiency. Under the pressure to execute as many demands of multiple clients, source traceability is not of utmost importance as it takes too much of their time. Thus Bean (2007) concludes that this conceptual dilemma and economic imperatives separating the government and the industry make a smooth path to public-private partnership fraught with difficulty.

There are more and more initiatives to connect public and private sectors through OSINT. In 2006 in Belgium non-profit organization EUROSINT Forum was founded "dedicated to European cooperation and use of OSINT that prevent risks and threats to peace and security", backed by the European Commission's Justice, Liberty and Security Directorate. EUROSINT mission is "to create an European 'intelligence ecology' that is dedicated to provoking thought on (OSINT) and its use in the intelligence and security spheres by public and private sector organizations". Other goals include "giving voice to private sector actors dealing with security and intelligence issues and building a positive image for OSINT in the EU" and "the creation of partnerships between private companies and/or public

organisms, to create European consortiums that can bring forward new projects". Members of EUROSINT Forum include EU institutions, national defense, security and intelligence agencies, private sector providers of intelligence, technology developers, universities, think tanks and research institutes.

By analyzing the model of response to challenges developed by intelligence communities that forced governments to outsource part of their intelligence needs, Liaropoulos and Konstantopoulos (2013) state there are new dilemmas such models open: are governments turning national security into business and is the private sector in a position to penetrate intelligence community and thereby spin intelligence and downgrade the role of intelligence agencies.

5. Methodology and research findings

For direct assessment of the actual situation in strategic management decision-making based on the information gained through the process of gathering information through open sources, we decided to carry out a survey in which we have included companies operating in Slovenia. To investigate the issue, we used the basic research question: "Does strategic management of companies in the Republic of Slovenia adequately recognize the opportunities offered by the decision-making on the basis of data obtained from open sources?"

When considering various sources of information, we have systematically and progressively analyzed data essential for defining the problem and finding solutions. With the analysis and review of the current status and research in the study area, we tried to identify the most important findings, which would confirm or reject the formulated research question.

The analysis will require certain restrictions, since, due to its extensiveness, this is a rather complicated problem. Therefore, in the applicative part of contribution, we used structured interviews with selected speakers from 15 organizational environments that work on the surveyed area. With our contribution, we would particularly like to define certain new approaches to providing a high level of awareness of the need for decision-making on the basis of relevant information which can largely be obtained from open sources.

In examining the issue we have used a variety of research methods. The topic is interdisciplinary in nature, because organizational system in the general part draws from organizational, economic and business knowledge, while in the specific part, it relies on the legal and intelligence and security profession and standards. Thus, the methods employed in the process of developing the theoretical part included the processing of a problem in the direction from general to concrete (deduction), qualitative analysis of data, information and materials, analysis of business and decision-making processes, content analysis – review and study of domestic and foreign literature relating to organization of business systems within companies, and their impact on the provision of appropriate forms of decision-making, and synthesis of findings, insights and knowledge.

To achieve the theoretical knowledge and the subsequent testing of research questions, the empirical part of the paper presents the results of the interview. As already noted, the interview was conducted with the experts from 15 organizational environments. 9 of them come from big companies, 3 from the category of medium-sized and small companies and 3 from microentrepreneurial environment.

Organizations which the mentioned experts belong to have been chosen deliberately so as to include all 3 categories of economic organization in Slovenia, namely microenterprise environment, the category of small and medium-sized organizations and large corporations environment, which included home-based organizations in Slovenia and international foreign corporation with headquarters abroad.

The structured interview consisted of a questionnaire, which included open-ended questions. We decided to use open-ended questions mainly because organizations are characterised by significant features associated with the activity, operating environments, and of course organizational structure (size). Questions of this kind were necessary, for the interviewees to be able to explain in detail the circumstances relevant for understanding of the factors and measures for strategic decision-making. Consequently, the processing of collected data will not be analyze using mathematical and statistical methods, but quality (substantive) interpretation of findings, insights and knowledge. This is a multifaceted problem that cannot be seen from one angle; thus, it will be necessary to use an interdisciplinary approach.

The analysis of the responses shows that different organizations have different perceptions of the importance of comprehensive management of security risks and particular importance of taking strategic decisions on the basis of their relevant information. Due to their specific features, they thus tackle this issue very differently in their respective environments. In smaller organizations, one can detect problems with human and financial resources, especially from the perspective of a more organized approach to the creation of mechanisms in the structure of organization that would deal more systematically with gathering, analysis, and making appropriate strategic assessments based on the information obtained from public sources. In large organizations, especially those organizations that stand out which operate in a complex international environment and organizationally devote significant attention to strategic decisions on the basis of adequate previously collected information. In this context, they devote special attention to the security component with an emphasis on the protection of trade secrets, patents, and most important competitive advantages and thus the need for an appropriate level of safety culture employees. With large corporate organizational forms of business organizations the responses reflect different approaches in expected support from national safety authorities in exchanging specific information especially about markets which are not in close distance from Slovenia. Organizations with headquarters and major ownership in Slovenia direct their expectations toward the success of Slovenian economy being of national importance, thus expecting state institutions to provide support to those organizations with relevant information in the context of public-private partnership. This expectation is especially important in cases when businesses want to appear at the markets where they are not traditionally present and are located outside the Euro-Atlantic area. On the other hand, representatives of international corporations with headquarters outside Slovenia primarily emphasize the partnership between corporations and relevant authorities of the host country, especially in the direction of a more effective risk management for the smooth functioning of corporations on this territory. In information exchange they are willing to participate to such an extent that efficacy and safety of their manufacturing or other processes are provided. Specialty within this category of companies is also observed for those organizations that handle a specific

part of critical infrastructure of national or international perspective. Representatives of these organizations openly expect that one of the important tasks of national security bodies is to support them with all key information necessary for making strategic decisions that will ensure smooth operation of this critical infrastructure. Due to various factors, medium-sized and small businesses do not pay much attention to these processes of obtaining and structural processing the information needed for decision-making. Decision-making is carried out primarily at a more intuitive level and is based on the analyses carried out through regular operation processes. In the case of microenterprises this process is tackled rather unsystematically. The main reasons probably lie in the smaller scale of operation, lack of human and financial resources and especially in the absence of the awareness of possibilities provided by the process of gathering relevant information through public resources that through appropriate forms of analysis provide an effective foundation for making realistic decisions. In the case of regulating the market with adequate supply of these products and their affordability, they would be willing to transfer a part of these processes to outsourcing.

Furthermore, it should be noted that the above findings are also reflected at the organizational level, where at middle and lower organizational levels one does not know or has not established specific organizational groups that would deal with the areas of collection, analysis and evaluation of data and information obtained through public sources. The same findings arise from the use of specific IT tools enabling a more structured data capture, analysis, storage and preparation through a variety of products in terms of reports, assessments and notices for strategic management. In larger organizations one perceives increased importance of organizational approaches and deployment of new tools, especially with the focus on international environment and the impact of a dynamic competitive market in their performance. This is closely related to the quality of the products derived from information collection through open sources. Strategic managers particularly complain about the information being too general in some respects and given in a form that is non-transparent and takes too much time to seriously go into these products. In those organizational environments, especially in international corporation, this area is arranged in a systematic manner so that the efficiency of this process is, on the one hand, the responsibility of customers who must provide a properly defined user requirements, and, on the other hand, service or individual who is responsible for acquiring and analyzing data from public and other sources.

In international organization as well as in Slovenian organizations operating in international environment, safety culture and safety awareness are recognized and promoted as an important value. From this perspective, it could be perceived with the respondents that, in addition to information directly tied to economic factors markets where the company wants to expand to, safety factors are the ones that strategic management devotes extreme importance to. The assessment of these factors go towards a number of levels, from the strategic security analysis of critical safety factors affecting the performance of the key business processes, all the way to the safety of individual employees, who may be exposed to certain security risks because of specific characteristics of their work, importance of job and other factors. From this point of view it is important to make certain decisions or make an appropriate system of responding to the emergencies related to employees safety.

6. Conclusion

Through the analytical assessment of theoretical approaches of international environment and a specific analysis of the case of Slovenia, this paper provides certain findings that support the thesis on the necessity of finalizing a new paradigm of public-private partnership in the field of production and exchange of key economic data, which are, on the one hand, of utmost importance for the functioning of operators at national and international levels while, on the other hand, the effective economies are that basic foundation for proper development and functioning of the national and, consequently, international environment. Of course, this process opens some major dilemmas which will require similar basic research projects to find right answers, which will represent a proper balance of interests of public and private environments. This path must be primarily directed towards the effective operation of the economic system as a basic foundation of welfare of individual companies (Vadnjal, 2012). The proper definition of open dilemmas will also eliminate concerns about the commercially orientated intelligence security system of each country and on the other hand, constant allegations that state institutions are ineffective and inefficient in supporting national economy. The basic foundation problem still lies in the so-called "national interest" and its definition in relation to what are now businesses that can benefit from such national assistance. In a dynamic economic environment of globalization processes and mixed ownership, which is not confined within a single country the establishment of unified and clear levers will be an extremely challenging task. It will require an individual examination of each separate case where partnership will be built through approaches to participation of both organizational environments, public and private.

Special importance will have to be given to the education of strategic management and to raising its awareness of the opportunities and limitations offered by the area of obtaining information from open public sources. Today, it is necessary to take strategic decisions on the basis of appropriate assessments and analyses. However, there is a need for proper awareness that a dynamic economic and security environment constantly forces us to the ongoing implementation of the process of collecting, analyzing and evaluating this information. In the era of information society based on communication and information technology, in most cases we no longer face a lack of information, but we are seeing a huge amount of information and data, not necessarily accurate. Because of that it is necessary to adopt a structured approach to this process and ensure appropriate high qualified human potential for its implementation. The fact that cannot be avoided is constant weighting of the ratio between the size of organization, business processes and resources that we have available and of course the ambition of entering international markets. Due to aforementioned facts, it is likely that primarily smaller organizations wanting to base their decisions on adequate information and analysis will leave room for outsourced specialists who will perform these services for each client. Of course, certain dilemmas arise here regarding the protection of critical data of organization; however, open dilemmas can be resolved through appropriate partnership, further defined by a contract.

Finally, it should be noted that strategic leadership responsibility of each organization is basically to internally develop capabilities necessary to enable the provision of relevant information and analysis to take effective and timely decisions.

References:

Bean, H. (2007). The DNI's Open Source Center: An Organizational Communication Perspective. International Journal of Intelligence and CounterIntelligence, 20(2): 240–257.

Coleman, K. (March 22, 2006). Counter-terrorism for Corporations. Directions Magazine. Retrieved on December 19, 2012 from http://www.directionsmag.com/articles/counter-terrorism-for-corporations-part-ii/123182.

Cortese, A. (December 30, 2001). Suddenly, Uncle Sam Wants to Bankroll You. The New York Times. Retrieved on March 26, 2013 from http://www.nytimes.com/2001/12/30/business/suddenly-uncle-sam-wants-to-bankroll-you.html.

DeLone, D.W., McLean, R.E. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. Journal of Management Information Systems, 19(4): 9–30.

Dupont, A. (2003). Intelligence for the Twenty-First Century. Intelligence and National Security, 18(4): 15–39.

Eijkman, Q., Weggemans, D. (2012). Open source intelligence and privacy dilemmas: Is it time to reassess state accountability? Security and Human Rights, 4. Retrieved on June 3, 2013 from http://www.upeace.nl/cp/uploads/publications/03_Eijkman_Weggemans_v2[1]_1367418023.pdf.

Garicano, L., Posner, A.R. (2005). Intelligence Reform Since 9/11: An Organizational Economics Perspective. Journal of Economic Perspectives, 19(4): 151–170.

Hayes, B. (2010). Spyinf on a see through world: the "Open Source" intelligence industry. Statewatch Journal, 20(1).

Harris, S. (2005). Intelligence Incorporated. Government Executive Magazine, 15: 40–47.

Hulnick, S.A. (2002). The Downside of Open Source Intelligence. International Journal of Intelligence and CounterIntelligence, 15(4): 565–579.

Liaropoulos, A., Konstantopoulos, I. (2013). Privatization of Intelligence: Turning National Security into Business? Research Institute for European and American Studies. Retrieved on July 10, 2013 from http://www.rieas.gr/research-areas/global-issues/transatlantic-studies/1319-privatization-of-intelligence-turning-national-security-into-business-.html.

NDAA – 109th Congress National Defense Authorization Act For Fiscal Year 2006, Public Law 109–163, Section 931.

Podbregar, I., Ivanusa T. (2010). Public sources and analytic in intelligence processes. Revija za kriminalistiko in kriminologijo, 61/2 (apr.-jun. 2010): 191–198.

Pringle, W.R. (2003). The Limits of OSINT: Diagnosing the Soviet Media, 1985–1989. International Journal of Intelligence and CounterIntelligence, 16(4): 280–289.

Rathmell, A. (2002). The Privatization of Intelligence: A Way Forward for European Intelligence Cooperation – Towards a European Intelligence policy. In NATO Open Source Intelligence Reader.

Underwood, J. (2002). Corporate Counter-Terrorism, Intelligence, and Strategy. Competitive Intelligence Magazine, 5(6).

Vadnjal, J. (2012). Economic impact of the war again terrorism: the threats and opportunities for the global economy. Corporate security in dynamic global environment: challenges and risks, 155–162. ICS: Ljubljana.

Стаття надійшла до редакції 26.12.2013.