UDK 351.746.3:334.758(497.7)

THE NEED FOR AN INTEGRATED APPROACH IN THE OPERATION OF PRIVATE SECURITY COMPANIES

Oliver Bakreski[45]

Ss. Cyril and Methodius University, Faculty of Philosophy, Institute for Security, Defence and Peace

Leta M. Bardjieva[46]

PhD Candidate, Faculty of Philosophy, Institute for Security, Defence and Peace

Abstract: Current security tendencies and trends, as well as the complex security requirements of clients counterpoise a real call for companies to offer protection at all levels in response to current security threats and challenges. In accordance with the principle of supply and demand, as well as in context of the factors that condition and determine the dynamics of current security challenges, security companies need to provide and maintain an integrated approach to operations, in order to ensure competitiveness and continuity of business.
Hence, the basic hypothesis of this paper refers to the thesis that through the integrated approach, security companies will provide a wide range of services in their operations adequate to the needs and requirements, as well as the optimal level of quality, thus ensuring the competitiveness of legal entities that offer services and professionalism and readiness of the staff in this profession.
The methodology for preparing this paper consists of empirical and theoretical research on the specific topic and includes the application of qualitative analysis of relevant primary and secondary sources, comparative analysis, case study and processing and interpretation of quantitative data.

Keywords: security, security company, services, integrated approach, competitiveness.

Introduction

When it comes to private security companies and their evolution in the 21st century, the transformation and adaptation that has occurred in this sector is evident. Namely, after the controversial start in the middle east and near east conflicts and the synonymization of private security and military companies with modern mercenaries, extortionists; groups that violate international law and standards, customary law in conducting military and security operations; already in the third decade of the new millennium, private security subjects have a completely different position, which is strictly regulated at the national and international level; they work in conjunction with the police forces and local communities and impose standards and innovations in security operations in the various domains where they offer their services and products (Bakreski, 2018:96).

[45] Contact address: oliverbakreski@yahoo.com

[46] Contact address: lbardjieva@gmail.com

In this context, it is significant to emphasize that in recent decades, a substantial change is occurring in the security services market. Namely, state institutions from service providers, became consumers of such services for actions that until recently were exclusively under the competence of the state security apparatus (Bakreski, 2018:99). Thus, private security in cooperation with the police plays a key role in joint efforts to ensure the safety and protection of citizens, public interests and private property. In addition to these segments, it should be noted that corporations are also focusing on building an independent security umbrella that should be the result of the security threats that companies face, as well as the integration of services and technology in security companies which is a product of the response to changes in demand, demographics and technology (International Code of Conduct Association, 2022:45). Nevertheless, it is important to point out that this transformation of the security companies is the result of continuous and proactive engagement of the subjects from the private security sector and the relevant state institutions in the domain of legal prescription and regulation of the private security business, which in contemporary context, among other things, is a complementary element in the overall security system of the society and an activity of public interest. It is also the result of the constant adaptation and response to the needs and demands of the end recipients for the services and products of the private security industry, which in contemporary context imply protection on several types, levels and domains and which are listed at the highest positions in profit making on a global level. The integration of different levels and types of security allows comprehensive analysis of vulnerabilities and comprehensive protection against various threats (National Cyber Security Strategy, 2018-2022:12).

All these statements highlight the importance of ensuring an integrated approach to security (OSCE, 2015:19). The integrated approach should be developed in several domains. *First*, in the context of strategic management, which implies normative solutions defined by legal provisions, regulations, instructions and other acts and the creation of strategies at the executive level. *Second*, in the context of the systemic approach, which implies integrating the activities and harmonizing the work of several heterogeneous institutions and their units, which are defined as elements of the overall system for providing and maintaining national security. *Third*, from an operational perspective, separate domains of security must be implemented together: such as locks in the physical environment and security software in the virtual environment. Integrated security in this context also requires systems and devices to be compatible and interoperable, with the ability to clearly overview the security environment and potential vulnerabilities or shortfalls (Campbell and Hall, 1987:26). *Fourth*, in the context of the domain of technical security, integrated, or in accordance with the related terminology, holistic security should integrate all elements designed to protect the client (the legal or natural person receiving services), considering them as a complex and interconnected system. The ultimate goal of integrated security is continuous protection of all attack surfaces: the totality of all physical, software, network and human exposure (Pavlovaite, *et al*., 2022).

An integrated approach can be applied to almost any domain where security is necessary, whether it is a person, computer, network, building or property, and it must always be considered in a wider context. Based on systems' considerations, integrated or holistic security involves considering how the component parts of each security system are interrelated and function within the context of larger systems (National strategy of the Republic of Macedonia for the fight against terrorism 2018-2022:17).

1. Private security companies – a theoretical approach

Regarding the definition of the security companies' concept, they essentially associate with the need to provide a sense of security to employees, customers and all those involved in the work process. The role of security agency employees is directly related to their function of securing private property, public order and social control (Schewe, 2018:2).

Security companies are engaged to protect state and non-state clients through the implementation of support activities, restoration and reconstruction, commercial business operations, etc. The activities of private security companies, regardless of their scale and geographical prevalent, can have potentially positive implications for their clients, the local population in the area of operation, the general security environment, the respect of human freedoms, the rule of law and several other aspects (Loader and White, 2017:7).

According to the contemporary theoretical approach, regarding the definition of the security companies, they are defined from the aspect of the legal normative and from the aspect of the social policy.

A private security company is a business entity that provides armed or unarmed security services and expertise to clients in the private or public sector (DCAF, 2020:52).

In this direction, security companies represent heterogeneous non-state actors and, in accordance with the instrumentalist approach regarding their activity, they can be characterized as independent private commercial subjects or as dependent on other subjects (Button, 2020:12).

Hence, *the universal characteristics* of the multitude of security company definitions relate to three basic pillars, namely: security management, operational security and physical security. Security management covers the aspects of designing the administrative control that contains the rules, guidelines and procedures for the implementation of security measures and activities. Operational security implies the effectiveness of administrative control, that is, technical access control, authorization, security typology applied to networks, systems and applications, etc. Physical security refers to the protection of personnel, data, hardware, etc., from physical threats that may injure, harm or interrupt business continuity and operations and have implications for the integrity, reliability and access to systems and data (Button and Stiernstedt, 2018:398).

Regarding the *methodological definition* of security companies, the approach can be: institutional, systemic, comparative or historical. The institutional approach to the definition of private security companies highlights their institutional dimension in the implementation of policies that regulate public powers and interests through their own means and capabilities, while the systemic approach to the definition of private security companies proposes a systemic analysis of the relations and functions of state and non-state actors engaged in providing security as well as their indirect and immediate influence. The comparative approach consists of a parallel review of the theoretical and empirical segment of the specific area and the set of specific alternatives and solutions to the preventive and protective activities provided by subjects other than the government, and the historical approach is aimed at determining the stages of evolution and transformation of the non-state private security and military activities, identifying the factors behind the growing role of private security companies in national frameworks and in international relations, and to trace the increasing dependence of states on security companies in historical perspective.

In the *context* in which they are approached, security companies can be analysed in the context of: their involvement at the national and international level, normative-legal perspective, their economics, political and social influence, etc.

The interpretation of the legislation governing the activity of security companies and the provision of security services by private subjects implies a multitude of variations in national legislation and generally refers to a private security legal entity or private security personnel assigned to carry out security tasks in order to achieve security goals (Nebolsina, 2021:76).

In order for the security tasks to be achieved in their entirety, cooperation is needed, especially of public and private security. The effectiveness of cooperation should enable the implementation of integrated strategies of action as a kind of mechanisms that can be used individually or jointly to assist maintaining security in the company's operations, while ensuring respect for human rights and humanitarian law. These principles primarily serve as a guideline and are intended for use by companies to: reduce delays and downtime in production (goods and/or services), gain access to financing and resources, strengthen the company's reputation, maintain a positive business climate and ensuring business continuity in complex business environments (Buzatu and Buckland, 2015:18).

2. Contemporary private security companies' services

Private security companies have the potential to improve the overall security situation only if their services are offered in a professional and responsible manner (Dunning, 2007:643).

The taxonomic overview of private security companies and the private security services industry, in most of the theoretical and empirical analysis focuses on the following aspects:

- *Economic aspect:* private security market, private security contracts, private security companies, private security workers;
- *Legal aspect:* private security legislation, controls and sanctions, collective agreements, admission conditions and restrictions, specific requirements, powers and competencies, use of weapons, training and related provisions, public-private cooperation, etc.

Security services, according to the taxonomy of security products, systems and services, can be categorized in the context of:

- Domain of appliance
- Security demand
- Security functions

In principle, security companies offer different types of services depending on the client's budget and current security needs. The basic level of service includes mall and small gathering security, surveillance services, investigative services, comprehensive risk assessment and risk reduction services provided to private businesses, as well as support in the post-conflict reconstruction process through the protection of defence and security forces and the agencies involved in the reconstruction (Berndtsson, 2009:72). Larger companies can

provide reliable income by tying up with local and state governments to secure factories, secure airports and other types of transportation points, government institutions and public establishments, critical infrastructure objects and other vital facilities. Top ranking services include protecting nuclear power plants, rapid deployment disaster response teams and overseas military missions.

They usually imply a combination, that is, the integration of two or more physical and technical services or products, among which the basic ones are: video surveillance, access control and detection of unauthorized access. For example, perimeter technical means and physical barriers that are integrated into the overall security system of the secured site are a key element in a layered security architecture (CISCO White Paper, 2006:9). This implies the application of an optimal number of sensors that can inform the overall security system about the movement of vehicles and pedestrians, the situation of the entrances, and whether they are opened in an authorized way or not (CoESS, 2015:36). These sensors have the ability to integrate with access control to disable alarming in the central and overall security system when authorized entry has occurred in order to reduce the rate of invalid alarms and maintain focus, among other purposes (Alwateer, 2019:26). Furthermore, fence vibration detectors, autonomous microwave sensors, autonomous surface seismic sensors and infrared sensors with the option to trigger security cameras (fixed and PTZ, with the PTZ tracking movement while the fixed camera takes detailed footage), can be used to increase situational awareness of potential threats, starting with wide perimeter surveillance such as surveillance radar technology (surveillance of a limited security area) and ending with a localized response with the perimeter barrier. Perimeter and wide-open area management is a service that is rapidly developing in the domain of border management, protection of coastlines and critical infrastructure facilities, emergency and disasters situations response, as a result of increased pressure from new threats due to their sophistication, such as unmanned drone systems (European Commission, 2022). Hence, the services offered by security companies contribute to the creation of safe urban and non-urban environments, businesses and homes, enabling public and private organizations to remotely and securely monitor facilities and space in real time with smart surveillance and security solutions (Withington, *et al*., 2010:26).

The evolution in the private security industry and the implementation of security services has been intensified during the past few decades. At the level of the European Union, for example, this process is primarily stimulated in the domain of internal security strategies, through the integration of:

- Service content and quality
- Unification of the physical and the technical segment of services
- Operators (security companies) integration
- National and international regulation standardization
- Citizen's inclusion

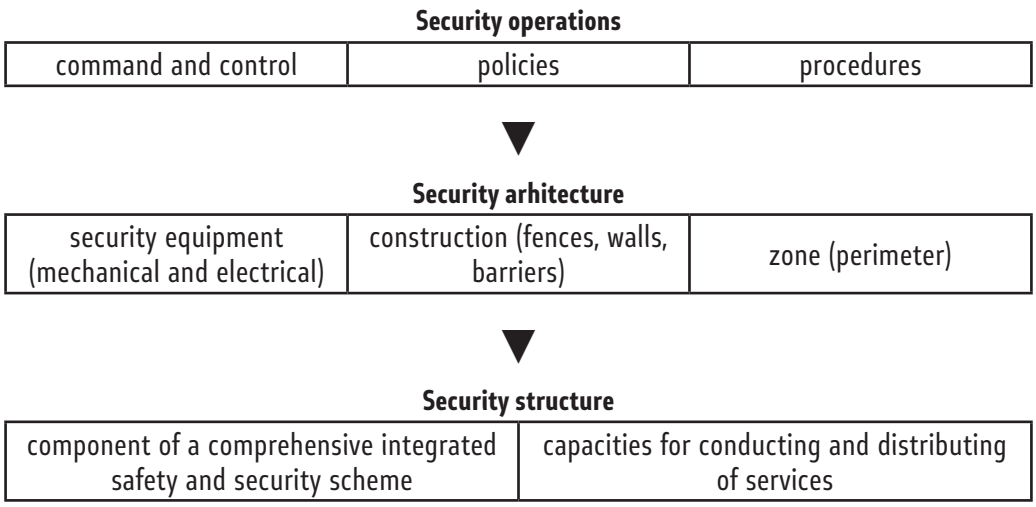
This indicates that this sector as a whole has reached maturity in terms of the volume and variety of services it offers to the market. As a result, numerous examples are evident at the national level, where security companies adapt to the demand of the national market and through the arrangements of the national regulation, they simultaneously stimulate the adaptation of the norms and standards at the supranational institutional level, which achieves the progressive development of the companies in the security industry (DCAF, 2007:27).

Considering the dynamic environment, the traditional services provided by security companies need to be supplemented with new ones in the context of the new requirements of the end recipients due to adaptation to the current and future threats arising from hyper-urbanization, the progress of technology and the concept of IoT.

In this direction, the need for implementation and application of services is imposed in the operation of private security companies for a comprehensive menu that offers a wide range of activities to respond to modern challenges in the domain of private security. This trend in the provision of services by private security companies has a multi-directional trajectory and beside the classic security domain, it spreads in almost all domains of functioning with social, political and economic implications (Bakreski, Ahic and Nadj, 2019:143).

According to current trends in security services in the private security market, through qualitative analysis they can be segmented into security operations, security architecture and security structure. Security operations are essentially the realization of security objectives that are set as a demand by the recipients of security services. The architecture of security services is a system with a layered structure and consists of a set of subsystems. Each layer is in synergy with the other subsystems, in order to respond to the requirements of the operator and to minimize the degree of threat. The security structure implies the correlation and cascading effect that the security subsystems that represent a segment of the overall scheme of the integrated security system have with each other (CoESS, 2019).

Figure 1: Components of security engineering. Source: Intrusion detection sensors used by electronic security systems for critical facilities and infrastructures: a review. Safety and Security Engineering VI. 131, 2022.



The trends in the demand for security services are driving the transformation of physical and technical security and their combined application. Namely, every organization has different needs and therefore relies on comprehensive security systems composed of multiple tangible and virtual subsystems to achieve its security goals, such as: security lighting, deterrence with physical barriers, objects distance and speed of movement radar

surveillance, access control protocols, alarming in case of unauthorized access (Cebula and Young, 2010:7).

The current services applied in the private security business by security companies consist of:

- risk management through the assessment of threats and vulnerabilities, determining strategic goals that are provided through protection against injury, loss and/or disruption, which are internationally regulated by the ISO 31000 standard
- determining the context of the environment and market trends in order to ensure continuity of operations
- personnel training for various tasks and duties, which in addition to traditional patrol and protection, include concierge service, event security, incident management, isolation and quarantine facility management, smoke, noise, animal treatment, construction site security, uninhabited and abandoned facilities, penal-correctional institutions, investigative and executive activities, as well as a series of other subtypes of security services
- application of technology with an innovative focus and application of applications, platforms and systems in the field of security that enable immediate exchange of information between customers and operators.

The services offered by private security companies are primarily adapted to respond to the risks, needs and concerns of clients through the construction of a partnership relationship with the aim of building a holistic and purpose-built solution for complex security problems and situations, i.e., a comprehensive spectrum of risk, threats and challenges security management. In this way, a mutual interaction is established between the company and the customers in the direction of creating a prosperous and safe environment. Hence, the services offered by security companies are modelled on the basis of three distinct but interrelated segments: security management, technology application, and security personnel (Bowen, *et al*, 2019:4,21).

Figure 2: Elements of an integrated approach model in the operation of security companies. Source: Taxonomy of Security Products, Systems and Services. CRISP Evaluation and Certification Schemes for Security Products, 2022.

Security management	**Technology/Appliance**	**Security personnel**
• critical infrastructure protection • risk management • border management • citizen safety (public and semi-public space) • disaster response activities and measures implementation • emergency procedures implementation • legal and business affairs	• cyber security(system security, application security, program security) • procedure safety • transactions security • situation review • process control	• human resources management • employee security • standard operative procedures • standards and criteria • training and qualification • continuous education • terminology

3. Integrated approach in the work of private security companies: significance and necessity

From the aspect of chronological development, the transformation of economic systems and their elements of production (land, machines, halls, money in the form of metal or paper) and the results of these transformative processes, contributed to the development of new concepts and the increase of their relative values. Until the second half of the last century, the dominant aspect of what was called private security was ensuring the physical security of the factors of production (mainly visible assets), but already in the past few decades the need for providing security for the so-called invisible assets has increased. Protection also implies the security of complex and fragile systems of critical infrastructure, information networks, data transfer and storage through these networks, specialized processes, etc. (Fay & Patterson, 2018:133).

In the context of a retrospective review of the development of the integrated approach to the operation of security companies, it is important to mention the foundation of the legal framework and normative designation in this domain, specifically with the example of the "Voluntary Principles for Security and Human Rights", which is a pioneering initiative formulated in 2000 by multiple stakeholders including governments, companies and non-governmental organizations. This initiative refers to the initial efforts of linking critical infrastructure of a specific energy sector with private security companies, which promotes the implementation of a set of principles to ensure security in their operations in a manner that respects human rights while conducting a comprehensive assessment of the risk in their engagement with public authorities embodied in public security in the domain of the protection of the company's facilities and premises and are divided according to three components: security assessment, public security institutions and private security companies (Voluntary Principles on Security and Human Rights, 2000).

In current conditions, the private security business, particularly the legal subjects and persons employed in this business, are required to develop a holistic approach, and in situations of a dynamic and changing world and the dangers that it brings, it requires or dictates that changes be treated as a motive for greater success and tendency to improve and implement security measures, which in accordance with the semantic meaning are not limited to physical security only. In this direction, the contemporary security company should have a broader view and range of activities that imply security to include things that are "conditionally" abstract or invisible, but are of exceptional importance, such as security and protection of electronic data, confidentiality of internet traffic and communication, etc., which in itself contributes to qualitative changes in the general concept of providing services by security companies (Bakreski, Alceski, Milosevska, 2017:114).

Due to the complex nature of the factors that influence shifts in the operation of security companies, market segmentation occurs, i.e., there are specialized companies that provide physical security services, companies that sell equipment needed for technical security, companies that provide cyber security services, companies specialized in offering services in the field of military training and expertise, etc. This, on the other hand, highlights the need for the integration of the various security domains, as well as for increasing the efficiency of the security company, while simultaneously optimizing costs (Bakreski, Gjurovski, Bardjieva, 2021:159). From this aspect, the effective management of security companies in

the third decade of the third millennium implies the full integration of security procedures and processes with a broad technological platform designed to detect risks and intervene at an early stage to ensure the resilience of the subject or person subject to security. Integrated security systems refer to the trend that occurs in a growing number of subjects from the private security business, where the merging of physical security applications occurs; for example, access control with logical security applications and biometric identification programs, allowing employees to use the network in a single, comprehensive system to create conditions for maximum overview of the situation and security environment (Roney, 2014:4).

The integrated approach in the operation of security companies implies the necessity of the synchronization of managerial, logistic and business processes. In order to achieve this, it is important that the integrated security strategy of the state is aligned with the business strategy of the companies, as well as with the action plans resulting from these strategies. It is necessary for them to be consistent with social trends, tendencies in the security environment and with the specific supply and demand in the market. This phrase is also a synonym for an approach to private security by companies that applies a broad perspective in the security approach, so that it includes not only physical or technical security measures (close protection or CCTV), but also the concept of cyber security, health and safety at work, business continuity, etc. (CRISP, 2016:2).

The creation of strategies for the implementation of the integrated approach in the operation of security companies imposes a need for inclusivity and the inclusion of experience and expertise from the relevant stakeholders, resulting from long-term engagement in the defence and security of the state, the protection of business entities, public spaces, critical infrastructure, etc., with the intention of enabling more efficient use of resources for this purpose (Chamber of RNM for private security, 2013:40).

An integrated approach to the operation of security companies in practice involves providing cost-effective, specially designed security solutions that increase profitability through:

- increased and more efficient security at lower costs
- ensuring continuity and flexibility in operations by minimizing downtime and inefficiencies
- strengthening the market reputation as a stable and reliable supplier of security goods and/or services

The process of creating a strategy can be defined as a set of activities that use one or more inputs and create a result of integrated value for the customer. The general division of the integrated approach process according to the type of work performed by the security company is determined: from the aspect of management (governance), in the domain of logistics and within the framework of business processes (Jusufranic, 2018:26). The stages of the process of creating a strategy for integrated management and operation of security companies are the following: model creation, model implementation and model implementation control. The implementation and management of the integrated model in the operation of security companies through the realization of strategies in this direction also contributes to achieving resistance, i.e., resilience of the companies themselves, which indirectly contribute to increasing the level of resilience of society through their commitment to their customers. Achieving this type of resilience, or according to the terminology that

prevails in the domain of security science and security systems – resilience, requires the ability to think, discipline and constant vigilance, i.e., adaptation to subtle tendencies in demand, as well as in security trends. For these reasons, companies that provide strategic advice on integrating the various elements of private security are emerging, i.e., companies that provide strategic consulting for the synergy of the integrated approach in the operation of security companies (Huan, *et al.*, 2021:874). The consistency of the integrated approach in the operation of security companies and the feasibility of this business concept on long-term paths, in a summarized form, counterpoises the development and adoption of a holistic governance and management system that will extend through all aspects of work, assessment of the security environment and the vision of risks and threats in the context of building a strategic and operational strategy. In addition, the integrated approach in the operation of security companies focuses on the implementation of initiatives and proactivity towards innovation, as opposed to a purely reactive impulse (Zahir, *et al.*, 2022:8).

Conclusion

The contemporary security company needs to adapt to changes that are of a different nature and cause fluctuating tendencies in the concept and operation, against the incomes and costs that are expected to increase constantly. This hypothesis is complemented by the fact that new circumstances and conditions both in the society and in the state, as well as in a wider international context, imply the need for an analogous adaptation of security companies to more heterogeneous-specific activities, in order to meet all the requirements that are complex and specific due to the complex nature of the activity and the security requirements. In this context, it should be emphasized that what was a characteristic of the private security industry is now complemented by specific needs that include legal entities with the activity of handling dangerous substances, legal entities with the activity of handling items and objects of particular cultural and historical significance, as well as those legal entities that need private security in the interest of the security and defence of the state. All this means that it is necessary to build an integrated system that will be a sufficient framework to predict and cover all the elements of the synthesized need.

Instead of using individual elements that may have compatibility issues, an integrated system brings all aspects of a company's security into one centre. Splitting security responsibilities between multiple parties or simply keeping legacy systems around for too long can create major problems for modern businesses. Integrated solutions create intuitive and customizable hubs, giving business personnel a clear overview of the company's network environment and potential vulnerabilities. Hence, in parallel, top-down management and horizontal management between homogeneous hierarchical units in the business hierarchy of security companies is necessary in order to implement and maintain protocols that will ensure the growth of companies, by ensuring compliance in implementing standards, policies and company regulations in all elements of the domain cope of work.

References:

- Бакрески О., Алчески Ѓ, Милошевска Т., (2017) Заштата на критична инфраструктура. Комора на РМ за приватно обезбедување.
- Бакрески О., Ахиќ Ј и Наќ И. (2019) Приватен безбедносен сектор во Југоисточна Европа. Случајот С. Македонија, Босна и Херцеговина и Хрватска. Комора на РСМ за приватно обезбедување.
- Бакрески О., Ѓуровски М., Барџиева М. Л. (2021) Јавна и приватна безбедност: координација и соработка. Комора на РСМ за приватно обезбедување.
- Бакрески, О. (2018) Безбедноста низ призмата на приватната безбедност. Комора на РМ за приватно обезбедување. Скопје.
- Закон за приватно обезбедување. Република Северна Македонија. Министерство за внатрешни работи.
- Извештај за севкупни активности и работа на Комората за 2021 година. Комора на РСМ за приватно обезбедување, 2021.
- Национална стратегија за сајбер безбедност 2018-2022. Акциски план 2018-2022. Министерство за внатрешни работи, 2022.
- Abrahamsen, R., Williams, R. C. (2011) Security Beyond the State. Private Security in International Politics. Cambridge University Press.
- Alwateer, M., Loke, S. W., Zuchowicz, A. M. (2019): Drone services: issues in drones for location-based services from human-drone interaction to information processing, Journal of Location Based Services, DOI: 10.1080/17489725.2018.1564845
- Bailes A., Holmqvist C. (2005) 'EU Must Regulate Private Security Firms', *European Voice*, 22-28, September 2005.
- Baldwin, D. A. (1997). The Concept of Security. *Review of International Studies, 23*(1), 5–26. http://www.jstor.org/stable/20097464
- Bardjieva M., L., & Bakreski, O. (2020). Private Security Industry in the Republic of Macedonia. International Institute of Social and Economic Sciences.
- Berndtsson., J. (2009) *The Privatisation of Security and state Control of Force: Changes, Challenges and the Case of Iraq,* School of Global Studies, University of Gothenburg.
- Born, H., Caparini, M. and Cole, E. (2007) *Regulating Private Security in Europe: Status and Prospects,* Geneva Centre for the Democratic Control of Armed Forces (DCAF), Policy Paper – №20, 2007.
- Bowen, Z., Jian, L., Wenlin, W., Zhenyu, Y., Gaojun, L., Jun, Y., & Ming, Y. (2019). Development of an interaction simulator for the scenario analysis of physical protection systems. *IEEE*.

- Brooks, D., Corkill, J., Coole, M. (2016). The Australian Security Continuum: National and Corporate Security Gaps from a Surveillance Language Perspective. In: Lippert, R., Walby, K., Warren, I., Palmer, D. (eds) National Security, Surveillance and Terror. Crime Prevention and Security Management. Palgrave Macmillan, Cham.
- Button, M. (2020). The "New" Private Security Industry, the Private Policing of Cyberspace and the Regulatory Questions. Journal of Contemporary Criminal Justice, 36(1), 39–55. https://doi.org/10.1177/1043986219890194
- Buzatu, A & Buckle, S. B. (2015) Private Military and Security Companies: Future Challenges in Security Governance. DCAF Horizon 2015 Working Paper No. 3.
- Dunning R., (2007) *Heroes or Mercenaries? Blackwater, Private Security Companies, and the U.S. Military,* The Kenan Institute for ethics, Duke University.
- Ettinger, A. (2014). The mercenary moniker: Condemnations, contradictions and the politics of definition. *Security Dialogue*, *45*(2), 174–191.
- European Commission. EU Security Market Study. Final Report. Luxembourg: Publications Office of the European Union, 31 May 2022.
- Fritsche, K. D. (2015) Drivers and challenges of an integrated guarding and technology security approach. CoESS General Secretariat, Belgium.
- Huan Lv*et al* (2021) Drone Presence Detection by the Drone's RF Communication. *Journal of Physics: Conference Series* Vol.1738. *DOI* 10.1088/1742-6596/1738/1/012044
- International Code of Conduct Association. Geneva Nations 3rd Floor Rue du Pré-de-la-Bichette 1 CH-1202 Geneva Switzerland, 2022.
- Jusufranic, I. (2018) Značaj i uloga korporativne sigurnosti u poslovanju preduzeća. Зборнандк на трудовand од четвртата меѓународна научна and стручна конференцandja на тема: ANDнтегрandрана корпоратandвна безбедност и дигиталните трансформации- предизвик за академската заедница и модерните корпорации.
- Nebolsina, M., A. (2021) Private Military and Security Companies: A Theoretical Overview. Centre for Euro-Atlantic Security, Institute of International Studies, Moscow State Institute of International Relations (MGIMO), Russia.
- OSCE 2022 Report on Violations of International Humanitarian and Human Rights Law, War Crimes and Crimes Against Humanity Committed in Ukraine Since 24 February 2022 by Professors Wolfgang Benedek, Veronika Bílková and Marco Sassòli.
- Pavlovaite, I., Huhtela, E., Vaccaro, G. D. Sanz, L. (2022) INTEL: Skills Intelligence for the Private Security Services. CoESS, June 2022.
- Private Security Companies. International Code of Conduct Association. ICoCA. Geneva, Switzerland, 2022.

- Private Security Companies. Toolkit for Security Sector Reporting: Media, Journalism and Security Sector Reform. DCAF – Geneva Centre for Security Sector Governance, 2020.
- Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie: Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework Geneva: UN, 21 Mar. 2011.
- Schewe, E. (2018) The World's New Private Security Forces. JSTOR.
- Schulz, S., Yeung, C. (2006) Private Military and Security Companies and Gender. Geneva Centre for the Democratic Control of Armed Forces, DCAF.
- Security Industry Act 2003. Australian Capital Territory. Republication No 27 Effective: 19 March 2021.
- Size of the Security Services Market Worldwide from 2011 to 2020 by Region. Statista Statistics Distribution of the Security Services Market Worldwide from 2011 to 2020.
- Size of the Security Services Market Worldwide from 2011 to 2020 by Region. Statista>Services>Security Services, 2022.
- Staff, H. (2021) The Political Economy of Private Security: How European States Privatize, Regulate and Produce Domestic Security. Lit Verlag GmbH & Co., Wien.
- Strom, K. et al. (2010) Private Security Industry: A Review of the Definitions, Available Data Sources and Paths Moving Forward. NCJRS Library.
- Taxonomy of Security Products, Systems and Services. CRISP Evaluation and Certification Schemes for Security Products, 2016.
- The Montreux Document on Private Military and Security Companies. International Committee of the Red Cross, 17 September 2007.
- Voluntary Principles on Security and Human Rights, MSI, 2000. US Department of State.
- Withington P., Fluhler H. and Nag S. (2019) Enhancing homeland security with advanced UWB sensors. *IEEE Microwave Magazine*, vol. 4, no. 3, pp. 51-58, Sept. 2019.
- Yatman, G.et al. (2015) Intrusion detection sensors used by electronic security systems for critical facilities and infrastructures: a review. *Safety and Security Engineering* VI. 131. Mert Department of Information and Security Technologies, HAVELSAN, Turkey.
- Zahir *et al* (2022) Strategic framework of using drone in cities disaster response. *IOP Conference Series Earth Environment Sciences* Volume 1091, The 9th AUN/SEED-Net Regional Conference on Natural Disaster.