UDC 327.84:343.326:351.746.1
DOI: 10.5937/spm103-70956
Original research article

Srđana Đurašević*

Faculty of International Politics and Security, University UNION – Nikola Tesla

INDUSTRIAL ESPIONAGE AND TERRORISM: POINTS OF INTERSECTION WITH INTELLIGENCE SERVICES

ONLINE FIRST

Abstract

This paper examines industrial espionage in relation to intelligence services and terrorism, treating information, know-how, and trade secrets as strategic economic and security assets in globalised markets. Using qualitative conceptual analysis, a review of relevant scholarly literature, and a doctrinal analysis of the Serbian legal framework, it distinguishes unlawful industrial espionage from lawful competitive intelligence. It analyses the relationship between industrial and economic espionage, the roles of state and non-state actors, and the circumstances in which intelligence services may become involved. The paper also considers the limited points at which industrial espionage and terrorism may intersect, particularly through reconnaissance, cyber-enabled intrusions, and threats to critical infrastructure, while emphasising their distinct primary purposes. Special attention is given to the legal framework for protecting trade secrets in the Republic of Serbia. The analysis concludes that industrial espionage need not be connected to a formal intelligence service and may also be conducted by corporate actors, insiders, private intermediaries, or state-linked actors.

Keywords: industrial espionage, economic espionage, intelligence services, terrorism, trade secrets, competitive intelligence, national security

INTRODUCTION

Timely and reliable information, technical know-how, and protected business information are important assets in contemporary economic and security competition. Digital

* E-mail: sdjurasevic@unt.edu.rs; ORCID: 0009-0009-0141-7442

networks, cross-border supply chains, and transnational business relations facilitate knowledge exchange but also create more points at which confidential information may be exposed. Organisations may lawfully use competitive intelligence to understand markets and competitors; industrial espionage, by contrast, involves covert, improper, or unlawful acquisition of proprietary information. The World Intellectual Property Organization (WIPO) treats competitive intelligence as a lawful business practice while distinguishing it from unfair or improper acquisition of trade-secret information (World Intellectual Property Organization [WIPO] 2024, 73). The terminology remains inconsistent across disciplines, and industrial espionage and competitive intelligence are often distinguished primarily by legality and ethics (Hou and Wang 2020, 2).

The research objectives of this paper are both scientific and practical. At the scientific level, the paper seeks to clarify the concept of industrial espionage and its relationship with economic espionage, intelligence services, and terrorism. At the practical level, it examines the methods used to acquire protected business information, the circumstances in which intelligence services may become involved, and the legal and organisational measures available for prevention and protection. In this way, the analysis aims to contribute to a more precise understanding of the risks associated with the unlawful acquisition of trade secrets and other sensitive information.

This study adopts a qualitative, concept-oriented design. It first synthesises scholarly literature on industrial and economic espionage, intelligence activity, and terrorism and then applies doctrinal legal analysis to the Serbian rules governing trade secrets, classified information, and related protected information. Doctrinal research focuses on law and legal concepts and is therefore appropriate for identifying the structure, scope, and internal distinctions of the applicable legal rules (Hutchinson and Duncan 2012, 85). The study does not attempt to estimate the prevalence of industrial espionage in Serbia because a sufficiently robust public dataset was not identified; instead, it clarifies the principal concepts, actors, methods, and legal distinctions relevant to the research question.

Espionage is not confined to wartime. Historical accounts show that practices aimed at obtaining protected political, military, economic, and technological information long predate contemporary intelligence institutions and have appeared in different institutional forms across historical periods (Uljanov 2025, 273–274). In wartime, intelligence collection may directly support military operations; in peacetime, it may inform foreign policy, security, technological, and economic decision-making. The applicable methods, institutional arrangements, and legal consequences nevertheless vary across jurisdictions and periods.

ONLINE FIRST

Modern espionage cannot be reduced either to its traditional military-political associations or to economic competition. The strategic value of economic and technological information has grown alongside knowledge-intensive production, while national legal systems continue to define espionage according to their own protected interests and institutional frameworks. In Serbia, Article 315 of the Criminal Code covers, inter alia, the transfer of secret military, economic, or official data or documents to a foreign state, foreign organisation, or person serving them, as well as specified forms of participation in a foreign intelligence service (Krivični zakonik 2005, čl. 315).

Against this background, the paper examines intelligence methods relevant to industrial espionage, the actors who may engage in such activities, and the boundary between lawful information gathering and the unlawful acquisition of protected information. Its central research question is whether industrial espionage must necessarily be connected to intelligence services. The analysis, therefore, focuses on the forms and methods of industrial espionage and on the circumstances in which intelligence services represent only one among several possible categories of actors.

The contribution of the paper lies in distinguishing industrial espionage from economic espionage and lawful competitive intelligence, and in identifying the conditions under which intelligence-service and terrorism-related dimensions become relevant. By applying these distinctions to the Serbian legal framework, the paper seeks to provide a clearer analytical basis for understanding industrial espionage without treating it as automatically synonymous with state intelligence activity, terrorism, or ordinary competitive information gathering.

SECRECY, CLASSIFIED INFORMATION, AND ESPIONAGE

Secrecy limits access to information whose disclosure may harm a legally or socially protected interest. The protected interest may be private, commercial, governmental, military, or security-related, so the legal consequences of disclosure depend on the category of information and the applicable regime. Earlier legal scholarship treats secrecy as a legally relevant quality connected to restricted availability of information (Dimitrijević 1972, 296), while contemporary scholarship similarly places information and secrecy at the conceptual core of espionage (Uljanov 2025, 273–274). The existence of protected information also creates a corresponding need for protective and counterintelligence measures.

Serbian law separates classified information from other forms of confidentiality. The Law on Classified Information establishes four classification levels (*državna tajna, strogo poverljivo, poverljivo,* and *interno*), under Articles 14 and 15 (Zakon o tajnosti podataka 2009,

ONLINE FIRST

čl. 14–15). The Criminal Code separately regulates the unauthorised disclosure of a state secret in Article 316 (Krivični zakonik 2005, čl. 316). Accordingly, "state secret" should be used as a specific legal category rather than as a generic label for any confidential material.

Espionage has legal, political, and operational dimensions, and its boundaries are not defined identically across legal systems or academic disciplines. In theoretical terms, it is closely connected with the intentional acquisition of information whose secrecy gives it value to a competing or adversarial actor (Uljanov 2025, 273–274). In legal analysis, however, whether conduct constitutes an offence depends on the protected information, the method of acquisition or transfer, the actor, and the applicable law. The Serbian Criminal Code, for example, ties the offence of espionage to specified secret military, economic, or official data and to a foreign state or foreign intelligence nexus (Krivični zakonik 2005, čl. 315). These distinctions help separate espionage from open-source research and other lawful forms of information collection.

THE CONCEPT AND CHARACTERISTICS OF MODERN ESPIONAGE

Intelligence activity has a much longer history than the Cold War. States and political communities used espionage and protected sensitive information in ancient, medieval, early modern, and modern contexts, while professionalisation and technological development altered the institutions and techniques through which it was conducted (Uljanov 2025, 273–274). The Cold War significantly expanded the scale, resources, technological capabilities, and political salience of intelligence services, but it did not create intelligence activity itself.

Intelligence systems differ in organisation and legal mandate, but intelligence work is commonly described through linked functions that include direction, collection, processing or analysis, and dissemination. NATO and UK doctrine have long used a direction–collection–processing–dissemination model, while other formulations separate processing and analysis more explicitly (Davies, Gustafson, and Rigden 2013, 58–59). The organisational form and the authority to conduct additional activities, including covert action, depend on national law and policy rather than following automatically from the intelligence function.

Collection requirements may concern military, political, economic, scientific, technological, or security matters, depending on lawful priorities. Collected material is not itself finished intelligence: it must be processed, evaluated, analysed, and communicated to decision-makers. The distinction between processing raw information and analysis or assessment of its wider implications is central to several intelligence-cycle formulations (Davies, Gustafson, and Rigden 2013, 58–59). The quality of the resulting assessment depends

ONLINE FIRST

on source reliability, methodological discipline, contextual understanding, and a clear separation of evidence from assumption.

INTELLIGENCE COLLECTION, COUNTERINTELLIGENCE, AND COVERT ACTION

Intelligence collection begins from requirements and priorities and may draw on open sources, human sources, liaison, and technical means, subject to the law and oversight applicable to the organisation concerned. Collection is one component of a broader process that also includes processing or analysis and dissemination (Davies, Gustafson, and Rigden 2013, 58–59). Counterintelligence, by contrast, is protective: it is directed at identifying and countering hostile intelligence activity and safeguarding people, information, institutions, and capabilities. Its operation need not be exclusively foreign-facing. In Serbia, the statutory remit of the Security Information Agency includes protection of the security of the Republic, detection and prevention of activities directed at undermining the constitutional order, and the collection, processing, and assessment of security-intelligence data (Zakon o Bezbednosno-informativnoj agenciji 2002, čl. 2).

Intelligence analysis and covert action should be treated as different functions. Analysis interprets and assesses collected information for decision-makers, whereas covert action is an intervention intended to influence events while the sponsor's role remains unacknowledged or deniable. Contemporary scholarship notes both the traditional association of covert action with concealed sponsorship and the practical spectrum between secrecy, exposure, and non-acknowledgement (Cormac and Aldrich 2018, 477–480). Because covert action is separately authorised in systems that permit it, it should not be presented as an inherent or routine function of every intelligence service.

The defining distinction is therefore one of purpose: espionage seeks information, whereas covert action seeks to shape conditions or behaviour. Covert action has traditionally been associated with intervention whose sponsorship is not publicly acknowledged, although actual operations vary considerably in how visible or attributable they are (Cormac and Aldrich 2018, 477–480). Lawful lobbying, public diplomacy, advocacy, and ordinary political contacts should not be reclassified as espionage merely because they seek influence. Security and criminal-law concerns arise when influence activity is coupled with covert direction, deception, corruption, unauthorised access, or comparable prohibited conduct.

Political espionage can accordingly be defined more narrowly as covert or unlawful acquisition of protected political information – such as information concerning negotiations,

ONLINE FIRST

decision-making, intentions, or institutional plans – for the benefit of a state or another sponsor. The broader phenomenon of covert influence is analytically different because its purpose is to alter behaviour or conditions rather than simply to acquire information (Cormac and Aldrich 2018, 477–480). Maintaining this distinction prevents political intelligence collection from being conflated with propaganda, public advocacy, disinformation, or terrorism.

INDUSTRIAL ESPIONAGE AND TERRORISM

Industrial espionage and terrorism should be treated as distinct analytical categories. Industrial espionage concerns the covert or unlawful acquisition of proprietary commercial or technical information and is generally distinguished from lawful competitive intelligence by the means used and the legal or ethical status of the acquisition (Hou and Wang 2020, 2, 6). Terrorism, by contrast, is organised around fear-generating or coercive political violence and its communicative effects on audiences beyond the immediate victims (Schmid 2012, 158–159). Industrial espionage may target trade secrets, technical know-how, research data, source code, business strategies, or other information whose secrecy has economic or strategic value (WIPO 2024, 17, 99). The actors can include insiders, private organisations, and state-linked entities; the relevant question is therefore not simply who the actor is, but how the information is acquired and for whose benefit (Hou and Wang 2020, 6).

The most plausible points of contact between the two phenomena are operational rather than conceptual. Terrorist actors have used networked technologies for communication, propaganda, recruitment, and information-related activities, and documented cases also show terrorist-linked actors using hacking and stolen data even where the objective was not infrastructure destruction (Banks 2017, 517). At the same time, “cyberterrorism” remains a contested category: EU-level discourse has repeatedly struggled to define it and has sometimes conflated cyberterrorism with the broader use of the Internet by terrorist actors (Baker-Beall and Mott 2022, 1092–1096). Reconnaissance, unauthorised access, the collection of technical information, or exploitation of insiders can therefore resemble methods associated with industrial or cyber espionage while serving a fundamentally different purpose.

Critical infrastructure is a particularly important area of potential overlap. Technical reconnaissance or access to information about system architecture, access points, dependencies, or vulnerabilities can support attack planning, while similar information may be sought in industrial espionage for economic or technological advantage. Cyberterrorism scholarship places critical infrastructure at the centre of many high-impact scenarios but also stresses the anticipatory character of much of this discourse; no publicly known case identified

ONLINE FIRST

in the relevant analysis involved proscribed terrorists using malware to cause kinetic disruption to infrastructure (Baker-Beall and Mott 2022, 1096–1097). The shared target or technique, therefore, does not erase the analytical distinction: the intended end – attack preparation *versus* economic or strategic exploitation – remains decisive.

ECONOMIC ESPIONAGE

Economic and industrial espionage predate the digital era. Efforts to obtain protected economic, technological, and strategic information can be traced across historical periods, while industrialisation and the expansion of knowledge-intensive production increased the value of technical know-how (Uljanov 2025, 273–274). Digital connectivity altered the scale and reach of these practices rather than creating them; cyber capabilities made it possible to penetrate corporate networks remotely and substantially expanded the operational scope of economic espionage (Banks 2017, 514).

Economic espionage and industrial espionage overlap but are not necessarily synonymous. The literature commonly associates economic espionage with activity conducted or orchestrated for governmental benefit, while industrial or corporate espionage is more often used for comparable acquisition undertaken without direct government involvement or for private commercial advantage (Hou and Wang 2020, 6). The distinction is not uniform across disciplines, but it is analytically useful because it directs attention to the beneficiary and strategic purpose of the acquisition, not only to the type of information sought.

Innovation-intensive sectors can make confidential know-how particularly valuable because developing equivalent knowledge may require substantial time, expertise, and investment. This creates incentives both to protect trade secrets and, for some actors, to seek them unlawfully (WIPO 2024, 17, 99). Where acquisition is state-directed or intended primarily to benefit a foreign state, it is more appropriately analysed as economic espionage. Recent dyadic research finds that state-sponsored cyber economic espionage is concentrated more heavily between countries with similar product and manufacturing profiles, consistent with a strategy of targeting knowledge that the acquiring state is positioned to absorb and use (Akoto 2024, 59).

The growing strategic value of proprietary information increases the importance of preventive protection. Relevant measures include internal confidentiality rules, non-disclosure agreements, physical and electronic access controls, cybersecurity safeguards, and evidence that the holder consistently treated the information as secret (WIPO 2024, 99). These measures

ONLINE FIRST

are not merely organisational best practice: the existence of reasonable steps to preserve secrecy is also a core element of trade-secret protection (WIPO 2024, 17).

INDUSTRIAL ESPIONAGE

Industrial espionage is not a post-1945 phenomenon, although postwar technological rivalry and later digitalisation expanded its potential scale, speed, and reach (Uljanov 2025, 273–274; Banks 2017, 514). High-value know-how may be an attractive target where lawful research and development would require substantial investment, but unlawful acquisition carries legal, reputational, and security risks. Historical evidence also shows that stolen information can have measurable economic effects: research using data on East German informants in West Germany finds that industrial espionage narrowed sectoral productivity gaps, with returns driven disproportionately by relatively high-quality information (Glitz and Meyersson 2020, 1055). This evidence demonstrates the potential value of misappropriated knowledge without implying that espionage is a normal or legitimate substitute for research and development.

Contemporary targets can include technical know-how, manufacturing processes, source code, research data, business strategies, and other information that derives commercial value from remaining secret (WIPO 2024, 17). Unlawful acquisition can occur through multiple routes, including breach of confidentiality obligations, industrial espionage, hacking, inducement to breach, or coercion (99). In strategically sensitive sectors, the same information may also have national-security significance. The motive can therefore range from private commercial advantage to state-linked technological acquisition.

The immediate object of industrial espionage is information that the acquirer cannot legitimately obtain and that has commercial, technological, or strategic value because it is controlled or kept secret. Under the trade-secret doctrine, legal protection normally depends on three linked elements: the information is not generally known or readily accessible, it has commercial value because it is secret, and the lawful holder has taken reasonable steps to preserve secrecy (WIPO 2024, 17). Serbian law adopts the same core structure and expressly includes know-how, business information, and technological information within the concept of a trade secret (Zakon o zaštiti poslovne tajne 2021, čl. 2). The legality of the method of acquisition is therefore central to distinguishing competitive intelligence from misappropriation.

ONLINE FIRST

LAWFUL COMPETITIVE INTELLIGENCE AND UNLAWFUL INDUSTRIAL ESPIONAGE

Learning about competitors is not, in itself, espionage. Competitive intelligence is a lawful business practice involving systematic collection and analysis of information, whereas acquiring a competitor's trade secret through unfair, improper, or otherwise unlawful means may constitute misappropriation (WIPO 2024, 73). Public filings, patents, published research, lawfully marketed products, and other legitimately accessible material can therefore be used for competitive analysis. The decisive questions are the status of the information, the source from which it was obtained, the method used, and any contractual or legal restrictions that apply.

Reverse engineering illustrates the importance of the acquisition method. Trade-secret protection generally does not prevent examination of a lawfully obtained product to discover how it works, although contractual restrictions may alter the result in a particular jurisdiction (WIPO 2024, 27). Serbian law likewise treats observation, study, disassembly, or testing of a publicly available or lawfully possessed product as lawful acquisition where the acquirer is not bound by a valid restriction on obtaining the information or on reverse engineering (Zakon o zaštiti poslovne tajne 2021, čl. 3). Employees' general skills and experience must also be distinguished from protected trade secrets; the legal balance depends on applicable labour and contract rules and on any continuing confidentiality obligation (WIPO 2024, 27).

Competitive intelligence may rely on information obtained openly through professional, market, and public sources, but the analysis changes once acquisition depends on improper conduct. WIPO identifies breach of confidentiality obligations, industrial espionage, hacking, inducement to breach, and coercion as examples relevant to proving unlawful or improper acquisition (WIPO 2024, 99). Serbian law similarly treats unauthorised access, appropriation, or copying of materials containing a trade secret, and other conduct contrary to good business practices, as unlawful acquisition (Zakon o zaštiti poslovne tajne 2021, čl. 4). Public-interest disclosure should be analysed separately from espionage: the statute limits trade-secret measures and remedies where disclosure of unlawful conduct is undertaken to protect the public interest (čl. 17).

Physical theft, unauthorised entry, and the removal or copying of documents or devices are traditional means of acquiring protected information. Cyber capabilities have added a remote and scalable route: economic espionage can now involve penetration of corporate networks and extraction of commercially valuable information across borders, substantially

ONLINE FIRST

expanding activity that existed before the Internet (Banks 2017, 514). Under the trade-secret doctrine, hacking and other improper means can support a finding of misappropriation (WIPO 2024, 99). Interception or recording of communications, however, must be assessed under the specific criminal, privacy, communications, and procedural rules of the relevant jurisdiction rather than characterised categorically across all legal systems.

Industrial espionage is not governed by a single uniform offence across jurisdictions, and the applicable legal response depends on the conduct involved. In Serbia, civil-law protection against unlawful acquisition, use, and disclosure of trade secrets is primarily regulated by the 2021 Law on the Protection of Trade Secrets (Zakon o zaštiti poslovne tajne 2021, čl. 1, 4). The same factual conduct may also engage the Criminal Code, classified-information rules, or other legislation where their statutory elements are met. The 2021 statute expressly repealed the previous 2011 Law on the Protection of Trade Secrets (čl. 22).

LEGAL PROTECTION AGAINST INDUSTRIAL ESPIONAGE IN THE REPUBLIC OF SERBIA

Available public material does not provide a sufficiently robust empirical basis for estimating the scale of industrial espionage in Serbia or identifying a dominant perpetrator category. Potential exposure can arise from insiders, competitors, cyber actors, intermediaries, or state-linked actors, but attribution should rest on verified cases. Where the targeted information concerns defence, dual-use technology, critical infrastructure, or other strategically significant sectors, trade-secret protection may intersect with national-security interests. For that reason, the issue is best addressed through combined legal, organisational, cybersecurity, and security measures rather than assumptions about ownership, nationality, or sector.

Under Serbian law, the existence of valuable information alone is insufficient for trade-secret protection. The information must be secret, have commercial value because of that secrecy, and be subject to reasonable measures taken by the lawful controller to preserve confidentiality. The statute itself gives examples of such measures, including internal rules, physical or electronic access controls, document marking, restricted access to premises and files, and confidentiality or non-disclosure arrangements (Zakon o zaštiti poslovne tajne 2021, čl. 2). Comparable measures are also identified in international trade-secret guidance as evidence that a holder has taken reasonable steps to maintain secrecy (WIPO 2024, 99).

Cross-border investment, research partnerships, supply chains, and technology transfer create legitimate flows of commercially valuable information, but they also increase the number of relationships in which confidential material must be managed. International

ONLINE FIRST

cooperation or foreign ownership is not evidence of espionage in itself; risk assessment should focus on conduct, access, purpose, and the protection applied to the information. From a trade-secret perspective, the principal risks include unlawful copying or access, breach of confidentiality, hacking, inducement to breach, and other improper acquisition methods (WIPO 2024, 99). Any claim about the prevalence of such conduct in Serbia, however, requires empirical evidence rather than inference from general international risk patterns.

Serbia's current trade-secret regime is set out in the Law on the Protection of Trade Secrets, published in the Official Gazette of the Republic of Serbia, No. 53/2021. The statute replaced the 2011 law (Zakon o zaštiti poslovne tajne 2021, čl. 22). It defines a trade secret through three cumulative criteria – secrecy, commercial value arising from secrecy, and reasonable protective measures – and expressly states that protected information may include know-how, business information, and technological information (čl. 2). The law also distinguishes lawful acquisition, including independent discovery and reverse engineering under specified conditions, from unauthorised access, appropriation, copying, use, or disclosure (čl. 3–4). These provisions supply the principal civil-law framework for assessing many forms of conduct commonly described as industrial espionage.

CONCLUSION

Industrial espionage should be understood as the improper or unlawful acquisition, use, or disclosure of confidential commercial, scientific, or technical information for economic, technological, or strategic advantage. It overlaps with economic espionage but is not identical to it, and it must also be distinguished from lawful competitive intelligence. Intelligence services may be involved in particular cases, especially where state strategic interests are present, but industrial espionage does not necessarily depend on a formal intelligence service. Competitive pressure, technological rivalry, and the high cost of research and development can create strong incentives to obtain valuable information. Yet, they do not make espionage a normal or inevitable feature of corporate competition. Firms and states also acquire technology and knowledge through lawful mechanisms such as research, licensing, investment, partnerships, recruitment, and reverse engineering, where permitted by law.

The actors involved in the unlawful acquisition of protected information may include insiders, corporate competitors, private intermediaries, cyber actors, criminal groups, and state-linked entities. The key analytical questions are therefore who seeks the information, by what means, for whose benefit, and under which legal regime. This makes the distinction between lawful and unlawful acquisition central to the analysis: public-source research, independent

ONLINE FIRST

development, and lawful competitive intelligence should not be labelled as espionage, whereas unauthorised access, theft, hacking, bribery, breach of confidentiality, and similar improper methods may constitute trade-secret misappropriation or other offences.

The value of information depends on its content, scarcity, timeliness, commercial utility, and strategic relevance. Information security and trade-secret protection are consequently important components of corporate resilience and, in strategically sensitive sectors, of national economic security. The close connection between technological development and economic strength encourages states and firms to invest in research, acquire technology lawfully, and protect strategically important knowledge. When actors resort to unlawful acquisition, the appropriate responses may include legal enforcement, counterintelligence, cybersecurity, personnel security, and organisational safeguards.

The central research question can therefore be answered in the negative: industrial espionage need not be connected to an intelligence service. Intelligence services can be important actors in state-directed economic or technological espionage. Still, many cases involve corporate competitors, insiders, private intermediaries, or cyber actors without a formal connection to intelligence services. Effective protection thus requires an integrated approach that combines legal protection, information security, cybersecurity, personnel security, and awareness of both state and non-state threats.

ONLINE FIRST

REFERENCES

Akoto, William. 2024. “Who Spies on Whom? Unravelling the Puzzle of State-Sponsored Cyber Economic Espionage.” *Journal of Peace Research* 61 (1): 59–71. DOI: 10.1177/00223433231214417

Baker-Beall, Christopher, and Gareth Mott. 2022. “Understanding the European Union’s Perception of the Threat of Cyberterrorism: A Discursive Analysis.” *JCMS: Journal of Common Market Studies* 60 (4): 1086–1105. DOI: 10.1111/jcms.13300

Banks, William C. 2017. “Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage.” *Emory Law Journal* 66 (3): 513–526. Last accessed on September 21, 2026. https://scholarlycommons.law.emory.edu/elj/vol66/iss3/3/

Cormac, Rory, and Richard J. Aldrich. 2018. “Grey Is the New Black: Covert Action and Implausible Deniability.” *International Affairs* 94 (3): 477–494. DOI: 10.1093/ia/iiy067

Davies, Philip H. J., Kristian Gustafson, and Ian Rigden. 2013. "The Intelligence Cycle Is Dead, Long Live the Intelligence Cycle: Rethinking Intelligence Fundamentals for a New Intelligence Doctrine." In *Understanding the Intelligence Cycle*, ed. Mark Phythian, 56–75. London: Routledge.

Dimitrijević, Dragoljub. 1972. „Pojam tajne i njena pravna određenost." *Jugoslovenska revija za kriminologiju i krivično pravo* (2): 296–302.

Glitz, Albrecht, and Erik Meyersson. 2020. "Industrial Espionage and Productivity." *American Economic Review* 110 (4): 1055–1103. DOI: 10.1257/aer.20171732

Hou, Tie, and Victoria Wang. 2020. "Industrial Espionage – A Systematic Literature Review (SLR)." *Computers & Security* 98: 102019. DOI: 10.1016/j.cose.2020.102019

Hutchinson, Terry, and Nigel Duncan. 2012. "Defining and Describing What We Do: Doctrinal Legal Research." *Deakin Law Review* 17 (1): 83–119. DOI: 10.21153/dlr2012vol17no1art70

Krivični zakonik, „Službeni glasnik RS", br. 85/2005, 88/2005 – ispr., 107/2005 – ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019, 94/2024 i 63/2026.

Schmid, Alex P. 2012. "The Revised Academic Consensus Definition of Terrorism." *Perspectives on Terrorism* 6 (2): 158–159.

Uljanov, Sergej V. 2025. „Krivičnopravni okviri i oblici ispoljavanja špijunaže." *Strani pravni život* 69 (2): 271–291. DOI: 10.56461/SPZ_25206KJ

World Intellectual Property Organization [WIPO]. 2024. *WIPO Guide to Trade Secrets and Innovation*. Geneva: WIPO. DOI: 10.34667/tind.49735

Zakon o Bezbednosno-informativnoj agenciji, „Službeni glasnik RS", br. 42/2002, 111/2009, 65/2014 – odluka US, 66/2014 i 36/2018.

Zakon o tajnosti podataka, „Službeni glasnik RS", br. 104/2009.

Zakon o zaštiti poslovne tajne, „Službeni glasnik RS", br. 53/2021.

ONLINE FIRST

Срђана Ђурашевић*

Факултет за међународну политику и безбедност, Универзитет УНИОН – Никола Тесла

ИНДУСТРИЈСКА ШПИЈУНАЖА И ТЕРОРИЗАМ: ТАЧКЕ ПРЕСЕКА СА ОБАВЕШТАЈНИМ СЛУЖБАМА

Резиме

Рад разматра индустријску шпијунажу у односу на деловање обавештајних служби и тероризам, уз јасно разграничење незаконите индустријске шпијунаже од законитог конкурентског обавештавања. Примењују се квалитативна концептуална анализа, анализа релевантне научне литературе и нормативна анализа правног оквира Републике Србије. Анализирају се однос индустријске и економске шпијунаже, улога државних и недржавних актера и околности у којима се могу укључити обавештајне службе. Посебно се указује на то да веза индустријске шпијунаже и тероризма није непосредна нити нужна, већ се јавља у ограниченим тачкама преклапања, као што су извиђање, прикупљање техничких података, злоупотреба сајбер-капацитета, коришћење инсајдера и приступ осетљивим подацима о критичној инфраструктури. Истовремено, различити циљеви ових активности захтевају њихово јасно аналитичко и правно раздвајање. Законити начини прибављања пословних информација, укључујући јавно доступне изворе, независно откриће и, под законом утврђеним условима, обрнути инжењеринг, разликују се од незаконитих метода попут неовлашћеног приступа, крађе, хаковања, подмићивања и повреде обавезе поверљивости. Посебан део рада посвећен је правној заштити пословне тајне у Републици Србији и важећем Закону о заштити пословне тајне из 2021. године. Закључује се да индустријска шпијунажа не мора бити повезана са формалном обавештајном службом, јер њени актери могу бити и корпоративни конкуренти, инсајдери, приватни посредници и сајбер-актери, док се улога државних служби посебно јавља у случајевима у којима постоји стратешки, технолошки или безбедносни интерес.

ONLINE FIRST

* Имејл: sdjurasevic@unt.edu.rs; ORCID: 0009-0009-0141-7442

Кључне речи: индустријска шпијунажа, економска шпијунажа, обавештајне службе, тероризам, пословна тајна, конкурентско обавештавање, национална безбедност[**]

ONLINE FIRST

[**] This manuscript was submitted on March 4, 2024, and accepted by the Editorial Board for online publication on June 11, 2025.