# Strategic Importance of Industrial Espionage in the Turkish Defence Industry and the Development of Counterintelligence Awareness Against Espionage Methodologies

Kadir Murat Altıntaş [1,*]

## Abstract

In the 21st century, the qualitative and quantitative diversification of information technology products has significantly increased the vital dependence of all institutions, both public and private, on information and technology. Although this transformation has provided companies with substantial resource savings and operational efficiency, it has also exposed them to a cyber environment characterized by limited oversight and insufficient control. In other words, the information technology systems and infrastructures established by companies that could not remain indifferent to this technological transformation have become vulnerable to threats such as highly sophisticated data theft, information exfiltration, and the misappropriation of technological know-how. Consequently, large-scale corporations have been compelled to protect, on the one hand, all digital activities transferred into virtual environments, and, on the other hand, the technologies produced through Research and Development (R&D) activities against cyber-originated threats. The aim of this study is to conduct a strategic analysis of the adoption of Counter-Intelligence (CI) principles and the construction of CI awareness—both at the corporate and employee levels—in order to protect the industrial property rights and commercial/technological secrets legally possessed by Turkish defence industry companies, whose economic and political significance is considerable, against illegal industrial espionage attacks and their methodologies. Within this framework, the study tests the following hypothesis: the establishment of counter-intelligence awareness among managers and employees in Turkish defence industry companies regarding industrial espionage methodologies constitutes a strategically significant precaution for preventing potential industrial espionage attacks and minimizing possible damage. All data and information obtained in this study were acquired from open sources, and thematic analysis and document review approaches, which are widely accepted qualitative analysis methods in the literature, were utilized. The fact that sufficient analysis or evaluation on the subject has not been reflected in either the literature or open sources is among the most important limitations of the study, but it also adds to its originality. In this context, the content of the limited publications and documents on the subject that are reflected in open sources has been analysed according to certain rules, and an attempt has been made to reach final conclusions.

**Keywords:** Defence industry, industrial espionage, counter-intelligence, counter-espionage, espionage methodologies.

Received: 14.02.2026 Accepted: 07.05.2026 Research Article

[1] Faculty of Applied Sciences, Abant Izzet Baysal University, Bolu, Türkiye
*Corresponding author.
✉ kadiraltintas@ibu.edu.tr

**Cite this article as:**
https://doi.org/10.65834/jdsi.12.62
Altıntaş,K.M., (2026). Strategic Importance of Industrial Espionage in the Turkish Defence Industry and the Development of Counterintelligence Awareness Against Espionage Methodologies. *Journal of Defence and Security Industries: Strategy and Technology 1(2)*, 1-26.

## 1. Introduction

It would not be an exaggeration to assert that at no other period in human history have technology and innovation played such a decisive and far-reaching role in shaping our world and human life. In this process, technology not only provides strategic advantage to those who produce and effectively utilize knowledge within the information society, but also emerges as a determining variable influencing economic, cultural, and political spheres—in short, every dimension of life—by shaping levels of welfare, competitiveness, growth, and development. The knowledge, technology, and innovation that define our future, however, appear to be generated predominantly by a limited number of developed countries and corporations (Adıgüzel, 2012). Nevertheless, one of the domains most profoundly affected by technological globalization is information security (TASAM, 2016).

In today's world, the qualitative and quantitative diversification of information technology products has significantly increased the vital dependence of all institutions—without exception, whether public or private—on information and technology. While this development has provided organizations, particularly corporations, with substantial resource savings and enhanced operational efficiency, it has simultaneously exposed them to a cyber environment characterized by limited regulation and constrained oversight. In other words, companies that cannot remain indifferent to this technological transformation have developed extensive information technology systems and infrastructures that are increasingly vulnerable to highly sophisticated threats, including data and information theft as well as the misappropriation of technological know-how. Consequently, large-scale corporations have been compelled to protect, on the one hand, all digital activities relocated to virtual environments, and on the other, the technologies generated through Research and Development (R&D) processes against cyber-originated threats targeting data and information systems (Altıntaş & Asal, 2020). Information security has thus evolved beyond a concept limited to commercial and economic interests; it now intersects with political and administrative interests within the framework of the state's public relations and is further conceptualized in conjunction with national security, particularly in terms of intelligence. When this expansive sphere of influence is considered alongside the rapid transformation accompanying the materialization of information, digital networks emerge as the primary environment in which potential damage may occur (Törenli, 2007).

In corporate structures, both organizational and environmental risks exist in terms of information security; therefore, the protection of organizational and technical data is also required. Particularly, organizational culture and awareness regarding the security and privacy of big data play a crucial role in preventing human-induced data breaches (Salleh & Janczewski, 2016). Although safeguarding the confidentiality of data and information is not an easy task in today's context, the continuous flow of information has stimulated intelligence production and revealed the strategic importance of information security. Consequently, in Türkiye, intelligence activities emerge as a primary constraint that must be taken into

consideration in the process of ensuring data and information security (Şeşen & Kuzucuoğlu, 2021).

Türkiye's location at the intersection of three continents within a geostrategic geography has, for centuries, rendered the ancient lands of Anatolia a focal point of intelligence rivalries. In the twenty-first century, commercial competition among corporate entities has, in many respects, evolved into forms of technological warfare. Beyond the technological capacities of states themselves, the protection of qualified data and information belonging to private enterprises—classified as commercial or technological secrets—against hostile foreign-origin attacks has become an indispensable component of contemporary economic security. In this context, safeguarding proprietary knowledge and strategic industrial capabilities is no longer solely a matter of corporate resilience but a broader issue intertwined with national interests. Indeed, due to the technological advancements and commercial achievements observed in the Turkish defence industry in recent years, it is assessed that these developments have attracted scrutiny not only from the intelligence services of advanced Western states but also from large-scale global defence industry corporations. Such dynamics further reinforce the necessity of integrating economic security, technological sovereignty, and information security within a comprehensive national security framework.

The oligopolistic characteristics that have long prevailed among global defence industry actors—often accompanied by monopolistic market responses—have entrenched all participants within a rigid and consolidated distribution of market shares. Consequently, the entry of new global actors with the capacity not only to influence but potentially to alter the status quo in international markets is perceived as one of the most serious threats to the strategic interests of incumbent firms. Particularly in a period when political and societal expectations regarding the advancement of the defence industry have reached unprecedented levels, the presence of the Republic of Türkiye and its companies—prepared to activate substantial engineering capabilities in the development of "new products"—is regarded as a significant risk factor by established global defence manufacturers. From a market dynamics perspective, a new entrant inevitably signifies, for traditional producers, both a "loss of customers," as former client states or institutions diversify their procurement sources, and a "loss of market share," as heightened competition disrupts previously stabilized competitive balances. In this context, the expansion of Türkiye's defence-industrial and technological capabilities introduces structural pressures into a global market historically characterized by concentrated power, limited entry, and high barriers to competition.

On the other hand, in the contemporary context, the adoption of physical and digital safeguards in line with general Counter-Intelligence (CI) principles for the protection of registered assets (including trade secrets and industrial property rights) owned by Turkish defence industry companies is of critical importance; however, such measures alone are insufficient. The identification, detection, examination, investigation, as well as the verification or refutation of potential acts of industrial espionage originating from rival corporations must fall squarely within the mandate and responsibility of in-house CI units. In clearer terms, these functions

should be explicitly defined within the formal job descriptions and operational frameworks of corporate CI personnel. Accordingly, systematically informing and raising awareness among all company employees in accordance with general CI principles constitutes the essential "cement" that reinforces the protective walls surrounding registered corporate assets. By cultivating organizational awareness of industrial espionage threats, employees can internalize CI principles not merely as procedural requirements but as an integral component of corporate culture and professional conduct.

The primary objective of this study is to conduct a strategic analysis of the processes through which CI principles are adopted and a CI awareness culture is constructed among companies and employees within the Turkish defence industry. Particular emphasis is placed on the protection—within a legal framework—of industrial property rights and commercial/technological secrets against unlawful industrial espionage attacks and their associated methodologies. Given the significant economic and political importance attributed to Turkish defence industry companies, safeguarding these proprietary assets constitutes not merely a corporate priority but a matter of broader national interest. In other words, the study seeks to address the following questions: 'What is the strategic significance of industrial espionage attacks for Turkish defence industry companies, and why is the establishment of CI awareness among managers and employee imperative within the framework of espionage methodologies?' Within this scope, the study tests the hypothesis that 'the construction of CI awareness among managers and employees in Turkish defence industry companies—particularly with regard to the methodologies of industrial espionage—constitutes a strategically significant measure for preventing potential espionage attacks and minimizing possible damage'.

Statistical data and qualitative information obtained within the scope of this study were sourced exclusively from open sources and widely accepted qualitative analysis methods in the literature specifically thematic analysis and document review—were employed. One of the main limitations of the study is that sufficient analyses or evaluations on the subject have not been extensively reflected in either the existing literature or available open sources. At the same time, however, this limitation contributes to the originality of the study. Within this framework, the study sought to reach final conclusions by analysing the content of the limited publications and documents available in open sources according to specific methodological rules and criteria.

## 1.1. Recent Commercial/Technological Developments in the Turkish Defence Industry and Future Projections

The defence industry is a strategic sector that plays a critical role in ensuring national security and directly affects a country's level of independence from both economic and technological perspective as well as strategic point of view. Nations make substantial investments in the defence industry to strengthen their defence capabilities, enhance deterrence power, and reduce external dependency (Kalkan, 2025). A country's capacity in the defence industry serves as an

important indicator in determining its global power status. Within this framework, two fundamental characteristics of the defence industry stand out. First, it relies on high-technology systems that require confidentiality to ensure national security. Second, by developing these costly systems with domestic resources, the defence industry significantly contributes to the country's industrial, scientific, and technological capacity (Yılmaztürk, 2023).

This sector, through high-technology–based production processes and intensive R&D investments and activities, significantly contributes to the development of the national technological infrastructure while simultaneously supporting economic growth and generating substantial employment. The export of defence industry products provides states with greater diplomatic leverage and manoeuvring space in the international arena, thereby transforming the defence industry into a strategic instrument that supports not only security concerns but also economic development and foreign policy objectives (Kurç et al., 2017). In this context, national defence projects contribute to enhancing local engineering capabilities, increasing technological innovation, strengthening the competitiveness of the defence industry, preventing brain drain, and boosting employment. These projects also serve as a guarantee of national security, as the country's capacity to produce its own defence equipment ensures greater independence against external threats (SASAD, 2023).

According to the various data comparisons (based on the years 2023-2025) made, the Turkish Defence and Aerospace Industry achieved sales revenue exceeding USD 15 billion. Of this total, international sales accounted for USD 5.5 billion, while R&D expenditure reached USD 2.6 billion in 2023 (Defence and Aerospace Industry Manufacturers Association, 2023). In the 2024 edition of the Defence News Top 100, which ranks the world's largest defence companies, five Turkish firms are listed within the top percentile. ASELSAN, ranked 42nd, reported USD 3 billion in revenue; TUSAŞ, ranked 50th, reported USD 2.2 billion; ROKETSAN, at 71st, generated USD 1.2 billion; MKE, at 84th, had USD 905 million; and ASFAT A.Ş., at 94th, reported approximately USD 650 million in revenue. Similarly, in the 2023 list of the largest 100 companies compiled by the Stockholm International Peace Research Institute (SIPRI), three Turkish companies are featured: ASELSAN at 54$^{th}$, BAYKAR at 69$^{th}$, and TUSAŞ at 78$^{th}$ (Defence News, 2024). In 2023, the annual sales revenue of the defence and aerospace sector reached USD 15.072 billion, with the domestic production rate in the defence industry achieving 81% (Presidency of the Republic of Türkiye, Secretariat of Defence Industries, 2025).

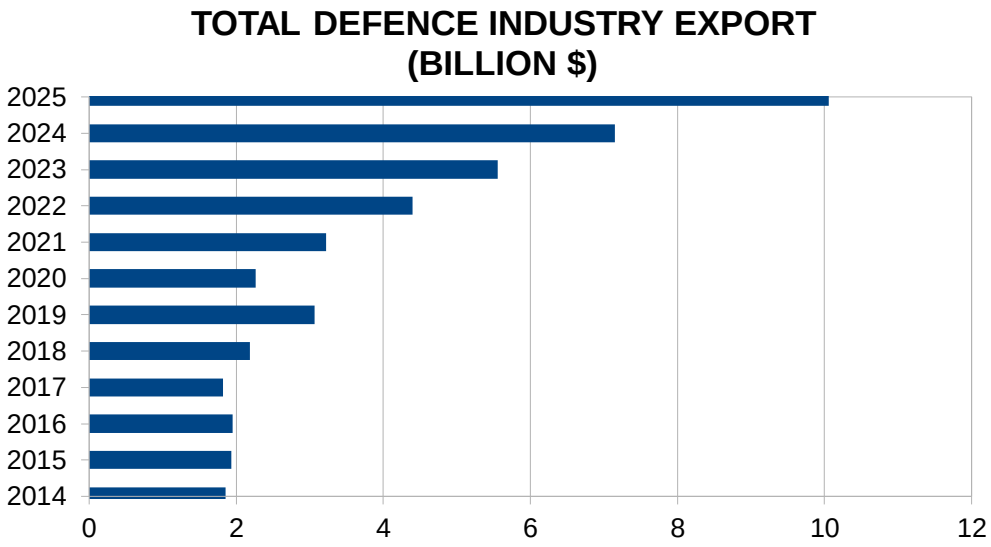


**Figure 1.** Sectoral Overview, 2024-2028 Defence Industry Sectoral Strategy Document, 2023, p. 35 and Presidency of the Republic of Türkiye, Secretariat of Defence Industries, Annual Report, 2025, p. 3.

As of 2024, there are approximately 1,300 R&D laboratories and 11 design centres in Türkiye, 66 of which operate specifically within the Defence and Aerospace sector (Ministry of Industry and Technology, 2024). Through collaborative R&D projects conducted by universities and industrial organizations under the coordination of the Secretariat of Defence Industries, the sector has seen a continuous increase in product diversity, export capacity, and technology development processes each year. As a result of R&D and defence industries ovation investments in the Turkish defence industry, domestically produced, technology-oriented defence products have been developed, while at the same time enabling the implementation of geostrategic policies that prioritize security in a region often described as a "fire circle." Furthermore, the numerous registered assets generated through these R&D and innovation efforts have contributed to the emergence of an ecosystem that also supports broader economic development policies.

The foundation of this progress lies in R&D investments and innovative production processes. In 2023, R&D expenditure increased by 27%, reaching USD 2.6 billion, while employment in the sector rose to 90,969 personnel (up from 75,660 in 2021 and 81,132 in 2022). R&D and innovation investments play a critical role, particularly in ensuring the sustainability of innovations in the defence industry and securing a competitive advantage in the global market. In 2023, the defence industry accounted for 2.5% of Türkiye's total exports (Figure 1). In terms of the regional distribution of foreign sales revenue, exports to Europe and the Americas constituted 46% of total sales abroad. Specifically, exports to the United States (U.S.) amounted to USD 1.331 billion, exports to Europe reached USD 1.220 billion, and exports to

other regions—including the Middle East, Asia, Africa, and South America—totalled USD 2.994 billion. Meanwhile, imports in 2023 rose by 22.35%, reaching USD 3.303 billion. Regionally, imports from Europe increased by 23.11%, from the America's by 22.95%, and from other countries by 18.42% (SASAD, 2023).

According to the April 2023 report by the SIPRI, Türkiye allocated 1.31% of its GDP to defence industry expenditures in 2023, with approximately 25.4% of the defence budget dedicated to equipment procurement and R&D activities (SIPRI, 2024). In 2025, defence industry expenditures are projected to increase by 12% (SIPRI, 2025).

In 2024, Türkiye's total defence industry expenditure reached USD 25 billion, while the export value of the defence and aerospace sector rose to USD 7.2 billion. As a result, the Turkish defence industry evolved into the world's 11$^{th}$ largest arms supplier. By 2024, more than 3,500 companies were actively engaged in a wide range of critical areas within the defence and aerospace sector, from original design and domestic production to modernization and modification, as well as R&D activities and international projects. By 2025, total exports of the Turkish defence industry had further increased to USD 9.87 billion (Presidency of the Republic of Türkiye, Investment and Finance Office, 2024).

Through R&D and Technology Management activities, Türkiye aims to achieve full technological independence by localizing foreign-dependent components and critical technologies in defence systems used by its security forces, as well as by acquiring advanced technologies for future systems that will provide strategic superiority (Presidency of the Republic of Türkiye, Secretariat of Defence Industries, 2023). In line with this objective, the statements of Prof. Dr. Haluk Görgün, Secretary of the Defence Industry, in the 2024–2028 Defence Industry Sectoral Strategy Document are particularly noteworthy:

> "In the new century of our nation, within the framework of our goals to 'increase the technological depth and domestic content of the defence industry, minimize foreign dependency as much as possible, ensure the sustainability of the defence industry ecosystem, and focus on breakthrough technologies,' we will focus, through the policies and strategies we implement, on enhancing the technological depth of our defence industry—which has reached a certain level of maturity at the system level—on disseminating the acquired knowledge and capabilities throughout the sector to ensure continuity, and on increasing the leverage effect of the defence industry in the economy through our visionary export models" (Presidency of the Republic of Türkiye, Secretariat of Defence Industries, 2023).

In the process of transforming from a regional power into a global actor, the Republic of Türkiye derives unique contributions and opportunities from its defence industry. In this context, both the implementation of Türkiye's regional policies and interests, as well as the execution of strategic decisions on a global scale, are supported by the combined deterrence capabilities and capacities of the Turkish Armed Forces and the Turkish defence industry.

These capabilities provide strategic support to both Türkiye's regional security and its economic development. Accordingly, it is anticipated that, particularly through high value-added products and technology-oriented production supported by R&D and innovation, the Turkish defence industry will continue to develop comprehensively in the medium and long term.

On the other hand, legally protected registered assets—classified as intangible fixed assets owned by commercial entities—have become a fundamental factor enhancing the competitive capacity and economic sustainability of globally operating companies. The primary purpose of intellectual property rights is to ensure the legal protection of high value-added products, innovations, or technological infrastructure. However, merely achieving advancements in ground-breaking technological fields through R&D and innovation investments, or creating "new products" that generate added value in the commercialization process, is no longer sufficient. Some global companies, without conducting adequate engineering work or significant R&D and innovation activities, acquire new technologies through unlawful means—often without any payment—and import them to the market, thereby creating "unfair competition." By resorting to unethical and illegal methods, these companies gain sectoral advantages. While this situation provides significant competitive superiority to the offending companies, it simultaneously causes the victimized firms to lose their commercial and technological capabilities and accumulated expertise in the short to medium term.

The consequences of the "industrial espionage" survey conducted by a non-governmental organization-BITKOM, representing more than 2200 companies in Germany's information, communication and new media sectors, have been announced that seven out of every ten industrial companies in the Germany have been the victims of sabotage, data theft or industrial espionage attacks in recent years (BITKOM, 2021). Elizabeth et.al. finds out that 'unfair competition' in the domain of 'Intellectual Property Rights' involves actions by an operator that infringe the legislation's rules, harm operators' legitimate rights and interest on the market, thereby threatening socio-economic order. The study concluded that unfair competition acts in the field of intellectual property rights (like industrial espionage, infringement of trade secrets, trademark infringement) impede innovation, stifle, and affect competition in the real market. And the occurrence of these unfair competition practices is common, even though there are existing legal frameworks that regulate this sector (Elizabeth et al., 2021).

Today, illicit industrial espionage attempts target not only the defence industry infrastructures and large-scale companies of developed western countries but also smaller and medium-sized enterprises in developing nations that, despite having limited capacity, are more dynamic and hold significant future potential. In some cases, even local commercial organizations that support macroeconomic development and possess growth potential can become victims of industrial espionage attacks. In other words, beyond the Turkish defence industry, technology-oriented firms operating in sectors such as wireless communications, consumer electronics, acrylic fiber, image processing and artificial intelligence technologies, and global gaming

software—even those with relatively limited production and export capacities—are also exposed to these risks.

## 1.2. The Strategic Importance and Methodology of Industrial Espionage within the Context of Illegal/Unethical Technology Transfer

The trade secrets[2] and intellectual property rights[3]—arguably the most important assets of companies—essentially protect the economic value of firms' technologically developing resources. For the qualified data and information possessed by companies to be recognized as "registered assets," they are generally expected to meet three fundamental criteria: they must be confidential, they must hold commercial value due to their confidentiality, and they must be subject to specific preventive measures to ensure their secrecy (Lippoltd & Schultz, 2014).

In today's world, where the commercialization of technology remains a prevailing trend, companies that undertake large-scale R&D and innovation investments, thereby dedicating substantial time, effort, and financial resources to enhancing their technological capabilities—have gained a competitive edge in international markets and achieved notable financial success. However, industrial espionage attacks targeting legally protected registered assets—such as trade and technological secrets or intellectual property rights—enable malicious competitors to attain the desired level of technological advancement without incurring comparable investments of time, labour, or capital. In this sense, industrial espionage initiatives, frequently observed in the twenty-first century, have evolved into a global phenomenon that effectively challenges the existence of companies operating within legal frameworks, notwithstanding prevailing international norms and domestic legal restrictions. By contrast, companies may lawfully obtain access to a close equivalent of an original product by supporting limited technical data acquired through legitimate means with methods such as reverse engineering and competitive intelligence. When conducted within established legal boundaries, such practices do not constitute a criminal offense.

The historical origins of industrial espionage activities go back to ancient times. The expansion of international trade as well as technological advancements have increased the theft of data

[2] According to the definition of "trade secret" set forth in the third section of the October 2006 Draft Law on Trade Secrets, the term encompasses "data, information, and documents related to the field of activity of a commercial enterprise or company that are known or accessible only to a limited number of its members and other authorized personnel; that are likely to cause harm if learned by competitors; that must not be disclosed to third parties or to the public; and that are of substantial importance for the company's success and efficiency in economic life."

[3] Commercial and/or technological data and information relating to registered assets—such as trademarks, patents, industrial designs, integrated circuit topographies, geographical indications, or utility models—are legally protected against unauthorized reproduction for the duration of their registration under intellectual property regimes. However, when hostile actors originating from rival companies reinforce the limited technical data disclosed to the public within the framework of patent law with confidential (technological) information unlawfully obtained through industrial espionage, they do not hesitate to introduce ostensibly "new" products to the market. This practice fosters an environment of "unfair competition" in international markets while simultaneously posing a direct threat to the commercial sustainability of the victimized companies.

and information between societies. In 1474, Venice, one of the leading states of that time, granted significant commercial privileges to merchants who brought technological innovations from various parts of the world to the country (Altıntaş & Asal, 2020). In 1712, Reverend François Xavier d'Entrecolles, who visited Jingdezhen in China, secretly learned the methods of producing Chinese porcelain and brought this knowledge back to Europe. Subsequently, manufacturers used this technology-based information to begin and develop porcelain production in Europe (Rowe and Brook, 2009).

In the 21st century—an era marked by an unprecedented rise in the global perception of industrial espionage as a serious threat—intense competition and hostile conduct have emerged among international corporations, often supported directly or indirectly by rival states. In this context, industrial espionage activities frequently target companies operating in sectors such as defence and aerospace, medical technologies, software, automotive, and electronics. For technology-oriented corporate entities, potential threats may originate not only from competitors but also from suppliers, stakeholders, and even dissatisfied current or former employees. These insider risks, combined with external hostile actors, significantly increase the vulnerability of high-technology firms. A case reported by the news agency Reuters illustrates this risk: the European aerospace giant Airbus dismissed 16 employees and launched an internal investigation in 2019 following an industrial espionage incident. The suspected employees were accused of unlawfully attempting to obtain communication systems and classified documents belonging to the German armed forces (Reuters, 2019). In another case, a military contractor named Hohn Murray Rowe was held responsible in September 2025 for sharing sensitive U.S. defence industry information—particularly classified data related to U.S. Air Force electronic warfare technologies—with foreign nationals. A court in South Dakota found the individual guilty and sentenced him to 126 months' imprisonment along with a USD 25,000 fine (U.S. Department of Justice, 2025). These cases demonstrate that industrial espionage constitutes not merely a theoretical or abstract risk but a tangible and recurring threat capable of generating severe legal, financial, and strategic consequences.

Although industrial espionage resembles economic espionage (Wagner, 2012; Soilen, 2016), it is generally conducted covertly and deceptively by private companies acting on their own behalf. In other words, industrial espionage refers to the acquisition of economic intelligence by the private sector using clandestine and unlawful means (Porteous, 1994). According to Baltacı (2015), industrial espionage encompasses activities carried out by a private company—or by individuals acting on its behalf—aimed at obtaining information of an economic intelligence nature that cannot be acquired from open sources, through covert and illegal methods directed against competitors. Ultimately, industrial espionage can be defined as the covert and deceptive acquisition—through ethically and legally questionable methods—of competitors' trade and technological secrets or confidential data and information protected under intellectual property rights (and not accessible through open sources), by commercial entities seeking to gain advantage in international competition (Altıntaş & Asal, 2020). The primary goal of industrial espionage is to obtain confidential and strategic information about rival companies (Toriola, 2011). According to another definition, industrial espionage is the

theft of a business's confidential or protected information (such as trade secrets or customer lists that are not publicly available) for use by a competitor or a foreign country (Benny, 2014).

On the other hand, the possible expectations and ultimate objectives of companies engaging in industrial espionage activities may be summarized as follows (Altıntaş & Asal, 2020):

a. To gain competitive superiority and prestige within the sector,
b. To save resources allocated particularly to R&D activities,
c. To cause reputational damage to rival firms,
d. To enhance effectiveness in internal decision-making processes.

A recent case illustrates these motivations in practice. A Chinese national, Ji Wang, who worked on projects funded by U.S. Defence Advanced Research Projects Agency (DARPA) and the private company Corning Incorporated, was involved in the development of optical fibers for high-powered lasers with both military and commercial applications. He unlawfully used non-public data and information—including secret trade production technologies required for manufacturing advanced optical fibers—for his personal commercial future and for establishing his own company. Following his arrest by law enforcement authorities, Ji Wang was found guilty, and at a hearing scheduled for April 15, 2026, he is expected to face a potential sentence of up to ten years' imprisonment (U.S. Department of Justice, 2025). This case demonstrates how the illicit acquisition and exploitation of confidential technological knowledge can directly serve competitive, financial, and strategic ambitions, while simultaneously generating severe criminal consequences.

Parties engaged in economic espionage do not refrain from spying on one another, even when they are friendly or allied states (Moyer, 1994). Countries allied with the U.S.—such as France, Israel, Germany, South Korea, and Japan—have reportedly targeted U.S. industry over the past several decades and have not hesitated, when deemed necessary for national interests, to appropriate commercial and technological secrets or to infringe intellectual property rights (Schweizer, 1993). Industrial espionage disputes between corporations likewise impose significant legal, financial, and temporal costs on both parties. For example, in 2006 the Polish roof-window manufacturer Fakro initiated legal proceedings against Velux on grounds of unfair competition. However, after more than a decade of litigation, the European Commission ultimately rejected the complaint in 2018. Similarly, in 2018, Uber reached a settlement with Waymo by transferring equity valued at approximately USD 244.8 million—equivalent to 0.34% of Uber's shares based on a USD 72 billion valuation (Toren, 2018). These cases illustrate those industrial and technological disputes, whether framed as unfair competition or trade secret litigation, often result in protracted legal battles and substantial economic costs, even when resolved through settlement mechanisms.

Another illustrative case concerns the Swiss-based private company Crypto AG, which produced encrypted communication devices intended to enable secure military and diplomatic communications among NATO member states and other countries. Toward the end of the twentieth century, the company reportedly sold encrypted devices to more than 120 countries

worldwide. However, what its customers were unaware of was that these cryptographic systems allegedly contained a "backdoor" mechanism accessible to the Central Intelligence Agency (CIA). In 1992, a Crypto AG engineer was detained and interrogated by Iranian intelligence authorities, bringing increased scrutiny to the company's activities. Despite various disclosures and allegations over time, the company continued its operations for years and ultimately ceased activities in 2018 (Miller, 2020). This case underscores the complex intersection between intelligence operations, private sector technology providers, and international trust in secure communication systems, illustrating how commercial cryptographic technologies may become instruments of state-level intelligence competition.

The number of disclosed industrial espionage cases represents only the "tip of the iceberg" (Androulidakis & Kioupakis, 2016). Cybersecurity attacks generating victims across 139 countries were analysed in the 2025 Data Breach Investigations Report. According to the report, a total of 22,052 security incidents formally reported and subjected to legal proceedings by companies of varying sizes and sectors were examined, and 12,195 of these cases were confirmed to involve verified data breaches (Verizon, 2025). However, victims of industrial espionage are often highly reluctant to report incidents to judicial authorities due to concerns over reputational damage in the eyes of customers and shareholders. Consequently, companies frequently tend to pursue out-of-court settlements with attackers or rival firms (Waziri & Yerima, 2011). Moreover, because victimized companies are generally unable to immediately detect data exfiltration or information misappropriation attempts, it is often difficult to determine the probable scope and extent of the damage incurred.

However, according to a 2018 report prepared by the Centre for Strategic and International Studies (CSIS), the estimated financial losses incurred by companies because of cybercrime and cyber espionage amount to approximately USD 600 billion (Lewis, 2018). Beyond the direct losses suffered by companies due to industrial espionage attacks, it is also necessary to consider indirect damages—although difficult to quantify—such as long-term harm to business prospects, erosion of competitive positioning, and the loss of customers (McKown, 2017).For this reason, relying solely on legal remedies to compensate for damages arising from industrial espionage is not a realistic strategy. Instead, awareness training and the cultivation of CI consciousness among managers and employees constitute far more functional and proactive measures in preventing industrial espionage activities (Kahn, 2019).

On the other hand, the absolute advantages that defence industry companies in Türkiye enjoy in accessing a highly skilled workforce—primarily stemming from the long-established engineering education infrastructure and project experience provided by Turkish universities—constitute the primary reason for their success in international competition today. However, it must be remembered that this highly qualified workforce is simultaneously the main target and potential victim of industrial espionage attacks. Therefore, a foundational awareness should be instilled among these individuals through education and training aligned with general CI principles. There have been public allegations that the Dutch government has incentivized engineers working in Türkiye's defence industry to relocate to the Netherlands and, moreover,

"deliberately" persuaded engineers involved in strategic defence projects to leave the country (Acar, 2018). Reports also indicate that the number of Turkish engineers who have moved to ASML—a company specializing in the production of machinery and facilities for semiconductors used in computer manufacturing—has reached approximately 1,300 (Nebil, 2024). This situation underscores the strategic importance of protecting intellectual and human capital, as the exfiltration of skilled personnel can directly facilitate technology transfer to foreign competitors and compromise national defence capabilities.

Within this framework of Altintas Pyramid (2021a) industrial espionage methodologies initially commence with Open Source[4] and Competitive Intelligence[5] activities. After acquiring preliminary information—serving as the foundation for potential illicit industrial espionage targeting specific companies—through open source and competitive intelligence efforts, a subsequent phase emerges that requires significantly greater expertise and experience.

At this stage, which requires a specific knowledge base and skill set in espionage, the core activity revolves around "Social Engineering," often succinctly described as the "art of human deception/hacking." Within this context, personnel considered the "weak link" inside a target company are identified and "profiled," after which the attacker exploits the individual's personal vulnerabilities to gain unauthorized access to the company's systems. In more precise terms, social engineering involves the deliberate manipulation of human emotions and deficiencies to coerce a target employee into disclosing confidential data and information about their employer, using various persuasion and deception techniques while bypassing ethical standards (Gehl & Lawson, 2022). Operations that exploit emotions such as fear, excitement, patriotism, or concerns over reputation and trust with clients or the public compel employees to make mistakes. These social engineering campaigns not only result in significant data and

[4] According to the official website of the Milli İstihbarat Teşkilatı (Turkish National Intelligence Service), open sources are defined as any information, documents, materials, or individuals, institutions, and organizations that can provide such information, whose disclosure, acquisition, and use pose no security concern (i.e., non-classified). Open-Source Intelligence (OSINT) is explained as the process of carefully analysing these open sources, collecting information from effective and reliable channels, and delivering it to the analyst in a timely manner and proper format to produce actionable intelligence (www.mit.gov.tr/sozluk.html#A, Accessed: 30.01.2026). Sources utilized to generate OSINT include the cyber domain, professional reports, trade fairs, land registry records, publicly available patent information, social media, print and broadcast media, and similar publicly accessible platforms.

[5] In a highly competitive business environment, decision-makers need to protect their company's strategies from competitors while simultaneously acquiring as much information as possible about competitors' objectives and plans. Consequently, in today's dynamic markets, it has become essential for companies to anticipate and understand competitors' actions to effectively position their products and services. Understanding competitors is also a critical component in developing a viable corporate strategy. Effective strategic planning requires the integration of high-quality competitive intelligence. To achieve this, companies must develop alternative intelligence sources, scan various aspects of their environment, and sensitize employees to the necessity of gathering intelligence. As observed, company executives need to collect and process information that is valuable for strategy formulation, including insights about competitors, customers, suppliers, governments, technological trends, and broader environmental developments. In summary, the generation and processing of information regarding a company's external environment for strategic purposes is referred to as competitive intelligence (Özdemir, 2010).

information loss but can, in some cases, render the systems of competitor companies entirely inoperative.

In October 2010, Glenn Duffie Shriver was convicted of conspiring to communicate classified U.S. national defence information to foreign actors and was sentenced to four years' imprisonment. Born in Virginia in November 1981, Shriver studied at a university in Michigan and participated in a 45-day summer program in Shanghai at East China Normal University. He later had the opportunity to complete an additional academic year there and developed advanced Chinese language proficiency. Shriver was reportedly approached with an offer to write a political article on U.S.–China relations for a Chinese newspaper. Subsequently, the newspaper's representative introduced him to other Chinese officials, and a cooperative relationship gradually developed. Rather than recruiting him directly as an intelligence asset, they allegedly encouraged him to apply for positions within U.S. law enforcement or intelligence institutions such as the CIA. Shriver received approximately USD 70,000 in several payments from Chinese officials. In June 2010, while preparing to travel to South Korea, he was detained at an airport. According to reports, a covert personality assessment conducted by Prof. Geling Shang—one of the coordinators of the summer program in China—identified Shriver's pronounced financial motivations. This vulnerability was strategically exploited during the recruitment process, and his primary weakness was manipulated to facilitate his engagement. The case demonstrates how social engineering and long-term cultivation strategies—particularly those leveraging financial incentives and psychological profiling—can be employed to infiltrate sensitive national security institutions (Reuters, 2010).

Another prevalent method within industrial espionage methodology is "Parallel Employment" a highly effective attack vector with significant damage potential. This technique involves identifying personnel within the target company who occupy operationally critical positions and persuading them to engage in dual employment—effectively, transforming them into de facto agents acting on behalf of a rival entity. Accordingly, employees at all organizational levels may be assessed as potential targets. Particular attention is often directed toward individuals who exhibit financial vulnerabilities or personal weaknesses, including susceptibility to inappropriate relationships. Once the primary motivational driver of the selected individual is identified and exploited, the recruitment (or engagement) process becomes considerably easier. Through this mechanism, access to the desired confidential data and proprietary information can be systematically secured. Parallel employment thus represents a hybrid insider threat model, combining elements of recruitment, coercion, and exploitation, and underscores the critical importance of robust internal CI awareness and personnel security practices within strategically sensitive sectors.

In February 2024, Chenguang Gong, a naturalized U.S. citizen since 2011, was arrested for allegedly stealing trade-secret technologies developed by a private R&D company on behalf of the U.S. government. Gong illegally transferred over 3,600 files onto personal storage devices, inflicting substantial financial damage on the victim company, which had invested more than seven years and tens of millions of dollars into developing these technologies. Among the

stolen files were designs for infrared sensors intended for satellite-based systems used to track ballistic and hypersonic missiles, as well as sensor schematics designed to implement countermeasures to interfere with missiles' infrared tracking capabilities (U.S. Department of Justice, 2024). This case highlights the critical vulnerabilities of proprietary technologies and the potentially severe financial and strategic consequences of insider-enabled industrial espionage.

Another method within industrial espionage methodology may be summarized as the strategic "Placement of a Spy" within the target organization's critical technical positions. In such operations, the individual's true motivation is deliberately concealed and often masked by carefully constructed cover narratives. These infiltration operations, which require considerable patience and a high degree of expertise, are typically associated with individuals possessing professional intelligence backgrounds or the discipline derived from formal military training. Within this framework, unlawful technology transfers are executed directly by an individual formally employed on the organization's payroll, thereby embedding the espionage activity within the legitimate operational structure of the company. This method represents a sophisticated insider threat model, in which the organization's own human capital is systematically leveraged to facilitate covert acquisition and exfiltration of sensitive technological assets.

Chinese electronics engineer Wei Sun was convicted for illegally transferring sensitive defence technology data from Raytheon Missiles and Defence, where he had worked for over a decade, to China. Due to his senior engineering role, Sun had access to most of the company's classified information related to missile guidance systems and other defence technologies. Between December 2018 and January 2019, during business trips to China, he removed sensitive data from the company laptop without implementing any protective measures, despite being aware of established security protocols, and delivered the information to Chinese counterparts (South China Morning Post, 2020). As a result, Sun was sentenced in the U.S. to 38 months of imprisonment. This case exemplifies the insider threat dimension of industrial espionage, highlighting how privileged access and technical expertise can be exploited to exfiltrate critical defence-related intellectual property across international borders.

The increasing use of the Internet for data transmission and electronic communication in the final decades of the 20$^{th}$ century has simultaneously facilitated unauthorized interference by malicious actors, rendering traditional notions of crime and punishment largely ineffective in the uncontrolled and insecure cyberspace. Consequently, ill-intentioned parties capable of gaining illegal access to sensitive data and information through 'Cyberattacks' inevitably began targeting technological assets produced through large-scale R&D investments and activities. In recent years, cyberattacks have become a significant concern—indeed, a near-nightmare—for defence industry companies seeking to protect their intellectual property. These attacks can be organized remotely from geographically distant locations at almost zero cost, making the legal prosecution of perpetrators extremely difficult and, in many cases, preventing the effective administration of justice. The content and methodology of such cyberattacks

predominantly involve the interception of competitors' email traffic and the unauthorized control of electronic communication systems, providing attackers with high-impact results relative to the minimal resources expended (Altıntaş, 2021).

In March 2025, the U.S. Department of Justice filed multiple charges against 12 Chinese cyber actors. Referred to as 'Cyber Mercenaries' this group was accused of serious offenses, including the theft of sensitive information belonging to the U.S. Department of Defence Intelligence and unauthorized access to the computer networks of defence industry suppliers. The indictment, focused on cyber espionage, specifically alleges that Yin Kecheng and Zhou Shuai, between 2011 and 2024, identified vulnerabilities in the target companies' computer networks, deployed malicious software, and established dedicated virtual servers to exfiltrate sensitive information (Cyber Security News, 2025).

In recent decades, Türkiye's defence and aerospace industry efforts to develop 'new products' have attracted significant attention in international markets and are being closely monitored. Consequently, in line with CI principles, the security of technological assets and trade secrets within the Turkish Defence and Aerospace Industry has become more critical than ever, making it imperative to implement the necessary measures to protect registered intellectual property and proprietary assets.

## 2. Discussion

Industrial espionage targeting the trade secrets or intellectual property rights of defence industry companies—often indirectly facilitated by adversary states or deliberately aimed at by competing firms—constitutes one of the most serious threats to both national and economic security. Approaching the issue solely from the perspective of criminal law, or enforcing stricter judicial measures, does not guarantee the prevention of potential industrial espionage incidents in the future. Similarly, physical security measures implemented by defence industry companies, or law enforcement efforts to safeguard sensitive company assets, do not ensure the complete protection of registered intellectual property and proprietary information. In summary, for defence industry companies, both internalizing counter-intelligence awareness at the individual level and establishing counter-intelligence principles at the corporate level are of strategic importance.

CI should not be the exclusive domain of intelligence agencies. Highly sensitive institutions, such as diplomatic missions, economic bodies, and energy authorities, must also establish dedicated CI units (Kavsıracı & Demirbaş, 2020). Similarly, for private sector entities, it is imperative to cultivate CI awareness both at the organizational level and among individual employees. The adoption of a CI mindset by managers and staff, and its integration as a habitual practice, constitutes a more effective protective measure against industrial espionage attacks than even the most stringent legal sanctions.

Intelligence can be succinctly defined as the collection of necessary information by a state to ensure its security or gain strategic advantages. Since other states naturally seek similar

information for their own interests, it is expected that they will also engage in information-gathering activities. At this point, the protection of strategically important state information and the prevention of its acquisition by foreign intelligence organizations—i.e., counterintelligence—becomes critically important (Tezsever, 1999). CI can be described as the process of identifying potential threats posed by foreign intelligence services, neutralizing these threats, and manipulating organizations attempting to collect intelligence on the state in ways that serve one's own national interests (Godson, 2004). Just as intelligence activities are employed to gain superiority over or neutralize enemy elements, CI functions as a "radar" activity aimed at detecting and neutralizing the adversary's tools or capabilities (Özdağ, 2018). In essence, CI activities encompass all protective security measures for safeguarding data, information, documents, personnel, materials, and facilities, alongside active counterespionage operations.

CI activities, which must inevitably be considered by defence industry companies, encompass a variety of operations with distinct characteristics. Activities that primarily involve taking traditional measures to physically and digitally protect trade secrets or intellectual property rights—where the "defensive reflex" predominates—fall under the scope of CI operations. Such traditional CI measures include classifying documents according to confidentiality levels, implementing physical security and protective measures, selecting personnel for critical positions and subsequently monitoring their financial behaviours including those of family members, and enforcing encrypted access protocols for both building/room entry and intranet/internet usage. For instance, in August 2021, the British Intelligence Service discovered that David Smith, assigned to the United Kingdom's Berlin Embassy, had not used bank or credit cards for an extended period. Following an investigation by British CI authorities, it was revealed that Smith had leaked information to the Russian Federation Intelligence Service and was subsequently arrested (Conner, 2021).

Counter-Espionage (CE), a narrower subset of CI, specifically focuses on detecting, neutralizing, and ensuring the legal or operational resolution of espionage activities. This includes not only identifying infiltration or spy attempts conducted by adversarial actors but also, where applicable, manipulating the opposing side through deliberately leaking or misleading information and attempting to convert an operational asset into a double agent. For example, in 1994, Aldrich Ames, who served as a CI officer at the U.S. CIA, was convicted of long-term espionage on behalf of the Soviet Union and sentenced to life imprisonment. During this period, Ames received approximately $4.6 million in unofficial payments from Russian intelligence, which allowed him to maintain a lifestyle far beyond that of his colleagues. Factors such as financial difficulties arising from his second wife's penchant for luxury and his longstanding struggle with alcohol addiction were reportedly exploited by Russian operatives in recruiting him (Encyclopaedia of Intelligence and Counterintelligence, 2015).

The philosophy of CI, encompassing both defensive and offensive strategies, is structured around four core functions (Van Cleave, 2013, 60). Interpreting these stages in the context of

commercial enterprises allows for a better understanding of industrial espionage threats and enables more effective responses. These processes can be briefly summarized as follows:

**a. Identification and Assessment of Risks and Threats:** The ability to discern the true intentions behind competitors' activities and to analyse the potential (both short and long-term) risks and threats these activities may pose,

**b. Identification of Vulnerabilities and Assessment of Hostile Activities:** Following the detection of existing weaknesses, determining the areas in which competitors' actions—disguised under the guise of commercial activities—are concentrated in a hostile or competition-impeding manner,

**c. Neutralization and Legal Prosecution of Responsible Parties:** Following the detection of industrial espionage attempts by competitor companies through defence measures, taking action to neutralize the perpetrators and subsequently initiating legal proceedings.

**d. Turning Attacks Against Competitors (Counter-Exploitation):** As an alternative to legal referral, engaging operational personnel to compel a change of allegiance, thereby misleading the competitor company with erroneous data and information—in short, "baiting" the adversary.

Establishing CI awareness among employees and standardizing protective measures against both physical and cyber threats are indispensable for safeguarding a company's trade secrets and intellectual property rights. This is because the human element lies at the core of CI activities. It is particularly noteworthy that nearly all potential interactions in any malicious attack originate from human actions. In this context, the human factor simultaneously assumes both the roles of victim and perpetrator. If employees are not fully informed about the security measures in place or fail to fully embrace them, the functionality of a company's CI policies cannot be ensured. Therefore, it is essential to equip personnel with comprehensive CI training programs and to periodically emphasize the strategic importance of these measures. However, training alone is insufficient. The ultimate objective is to cultivate genuine CI awareness among employees, fostering a mindset in which the philosophy of CI becomes an integral part of their professional conduct and daily practice.

CI activities constitute a comprehensive set of protective measures employed by companies to safeguard against the "unfair competition" initiatives of rival firms. Simultaneously, they establish a defensive barrier against the competitive intelligence efforts of competitors. However, from a proactive perspective, effectively preventing industrial espionage requires the early detection of hostile attempts. Successfully achieving this challenging objective demands substantial experience, accumulated knowledge, and intuitive capacity, alongside the strategic utilization of various tools and methodologies.

Piecing together small fragments of information to form the complete picture—or recognizing the significance of seemingly trivial behaviours and materials—is almost a way of life for CI specialists who question everything and probe behind the scenes. Consequently, it is useful to

briefly outline certain techniques that hold strategic importance in CI operations and are utilized in the detection of industrial espionage attempts:

**a. Dumpster Diving:** Companies may consider the discarded materials of competitors—such as paper scraps, flash drives, non-functional prototypes, old notebooks, and post-it notes that have not been fully destroyed—as valuable sources of data and information. In particular, employees of high-tech firms with substantial R&D investments may inadvertently create opportunities for industrial espionage if they fail to exercise sufficient care with materials disposed of in office trash or waste areas. In highly competitive global markets, the covert collection and analysis of physically discarded items whose structural integrity is partially intact can provide critical insights into a company's current operations and future strategies (Altıntaş, 2021). For example, a paper collector repeatedly retrieving waste from a company's surrounding trash areas is highly suspicious. Therefore, defence industry personnel should always destroy obsolete materials using shredders rather than simply discarding them (Prunckun, 2019).

**b. Determining Vulnerability:** This activity aims to identify potential weaknesses of a target individual and subsequently exploit those vulnerabilities or manipulate them for personal gain (Prunckun, 2019). Human vulnerabilities may arise from financial incentives, physical limitations, past traumas, or even sexual preferences and other personal shortcomings (Davies, 2005, 23). Consequently, employing individuals in defence industry companies—particularly in managerial positions—whose motivations are primarily self-serving and whose vulnerabilities are pronounced is extremely risky. At a minimum, however, senior managers who are aware of these vulnerabilities should closely monitor and supervise such personnel.

**c. Reconnaissance and Observation:** CI personnel within a company are responsible for monitoring an internal target employee, when necessary, but without engaging in any physical intervention. In situations where data or information leakage is suspected, it is critical to track and analyse the locations visited and individuals contacted by the employee under surveillance. In addition to utilizing in-house cameras for observation, the detection of any dead-drop[6] points can only be achieved through close tracking of the suspect employee. During monitoring operations, CI specialists may employ legally permissible electronic surveillance devices but must also ensure the strict protection of the target individual's legally protected personal data.

Moreover, it is the responsibility of company CI officers to train critical technical personnel or managers in defensive reactions before events such as overseas business meetings or trips, particularly when there is a risk of physical or digital surveillance by competitor company representatives or foreign intelligence services. Employees in key positions should also be

[6] **Dead-Drop:** A dead-drop is a secure communication method used between parties (e.g., a case officer and an agent) in intelligence operations. It involves prearranging a secret location—such as behind a rock, beside a statue, or under a bench—where classified or sensitive information obtained through espionage can be deposited by one party and later retrieved by another. This technique is employed when direct contact between parties could arouse suspicion or when one party is believed to be under surveillance.

educated about "black bag operations[7]" during foreign accommodations. Competitor personnel may sometimes persuade hotel staff to gain covert access to an important technical employee's room or luggage, potentially leading to copying or even disappearance of sensitive documents.

**d. Denial and Deception:** A common practice in competitive business environments, denial and deception involves manipulating data and information to gain an advantage over rival companies, obscure future plans, and conceal key capabilities. Considering the high speed of social media dissemination and the significant time required to detect falsified content, the digital realm has effectively become a lawless platform, making legal tracking extremely difficult. This environment also conceals the behind-the-scenes support of public entities (e.g., intelligence agencies) in ostensibly private corporate industrial espionage operations, providing the so-called "Plausible Deniability." Deliberate dissemination of false information via social media as a deception tool has become an effective competitive instrument, causing potentially severe consequences for those unable to distinguish reality from fabrication. In denial and deception operations, which must be coordinated and complementary, the primary requirement is strict adherence to confidentiality principles while compelling the target company to make strategic errors. For example, deception campaigns suggesting the existence of lucrative business opportunities in a specific region are inherently deniable in both content and outcome.

**e. Agent/Source Exploitation:** Individuals within a competitor organization—or within a target company—may be persuaded to provide confidential information in exchange for strong personal incentives. Acting as auxiliary intelligence assets, these insiders systematically relay information regarding planned, ongoing, or potential corporate actions to the controlling intelligence officer (or the operational manager of the organization's espionage initiative) (Urhal, 2008, 558). Similarly, in a defence industry company, a CI officer may obtain sensitive information from personnel in strategic departments in exchange for specific motivators. While rigorous internal inspections, strict security measures, or employee monitoring may erode trust and loyalty among staff, continuous management guidance emphasizing that protective measures are not personalized can yield short- to medium-term benefits. Otherwise, employees may begin perceiving one another as potential informants, inevitably decreasing productivity in the medium to long term. Directly sourced intelligence is generally more secure, faster, and cost-effective than other technical surveillance methods, explaining the method's prevalence. Despite its advantages in crime prevention and evidence collection, source exploitation remains susceptible to manipulation and potential ethical or legal concerns and therefore should only be designed and implemented by experienced CI personnel.

[7] **Black Bag Jobs:** In human intelligence operations, black bag jobs refer to illicit infiltration attempts into physical locations or cyber environments that are otherwise restricted or secured. The term "black bag" originates from the black bag carried by burglars, which contains tools intended for use during their covert activities. These operations aim to gain unauthorized access to sensitive areas or systems to obtain information or assets.

## 3. Conclusion

In the second quarter of the 21st century, within a global climate where international economic, technological, and political competition is intensifying day by day, private enterprise managers who have internalized intelligence and espionage concepts—and view intelligence as a force multiplier—are indispensable for the sustainability of companies. Meanwhile, industrial espionage, which has increased both quantitatively and qualitatively in recent years, poses a serious threat to the commercial and technological assets of all medium- and large-scale companies, particularly those operating in technology-focused defence sectors, and can cause disproportionately high damage relative to its cost. In this context, the technological know-how and trade secrets currently possessed by the Turkish defence industry are under significant threat due to widespread and destructive industrial espionage attacks on an international scale.

Developing specific standards for the implementation of physical and cyber measures to protect the proprietary assets of Turkish defence industry companies, or in other words reducing the CI philosophy merely to defence against physical or cyber-attacks and designing an all-encompassing protective system accordingly—is useful but insufficient. In addition, it is necessary to establish internal corporate training programs aimed at informing and raising awareness among employees at all levels of the organization in accordance with general CI principles. In other words, organizing educational programs for managers and employees of Turkish defence industry companies on general CI principles and current industrial espionage methodologies constitutes a highly valuable corporate initiative. However, more importantly, at a minimum, all employees must comprehend the strategic significance of the CI doctrine in the face of industrial espionage threats and develop corresponding awareness, thereby internalizing and normalizing CI practices as a way of life; this represents the most effective measure to prevent data and information leakage. In the contemporary environment, it cannot be claimed that severe legal sanctions alone effectively prevent unfair competitive practices among companies in the context of industrial espionage.

Furthermore, within a proactive CI framework, it is essential to plan protective measures against all forms of industrial espionage in advance and to anticipate potential subversive activities, thereby fostering both individual and organizational defensive culture. Moreover, in the 21st century—where perception management on an international trade scale has become more critical than ever—commercial competitive strategies, which can be conceptualized as an "information war" by rival companies, naturally include psychological operations. Consequently, it is mandatory to establish a defensive infrastructure and culture against potential propaganda campaigns and disinformation efforts, particularly via "new media" platforms, as part of CI activities. In this regard, the establishment of strategically important CI units within Turkish defence industry organizations constitutes a highly valuable initiative; in their absence, similar responsibilities may need to be delegated to human resources departments and the organizational structure reconfigured.

Finally, based on strategic analyses of CI activities and document reviews within the relevant literature, the hypothesis that "the development of CI awareness among managers and

employees regarding industrial espionage methodology in Turkish defence industry companies is a strategically important measure for preventing potential industrial espionage attacks and minimizing probable losses" has been qualitatively confirmed.

In this context, Chinese-origin companies with a historically extensive record of involvement in industrial espionage increasingly target technologically advanced Western companies and innovation hubs. The most pressing questions in this regard concern the degree to which legally registered commercial entities, which outwardly appear as private companies, act independently from the state, and the extent to which Chinese intelligence services are involved in industrial espionage operations on behalf of these companies. Analysis of numerous judicial cases, processed by the U.S. Department of Justice and reflected in open-source documentation, clearly indicates that Chinese intelligence services are positioned at the very centre of these industrial espionage activities.

## Conflict of Interest

There is no conflict of interest among authors.

## Funding

This research received no funding.

## Ethical Statements

Not applicable.

## Data and Code Availability

Not applicable.

## Supplementary Materials

Not applicable.

## References

Acar, İ. (2018, January 16). *Savunma sanayinden Hollanda'ya beyin göçü*. *Sabah Gazetesi*. https://www.sabah.com.tr/ekonomi/2018/01/16/savunma-sanayiinden-hollandaya-beyin-gocu.

Adıgüzel, M. (2016). *Teknolojinin küreselleşmesi ve Türkiye açısından bir değerlendirme*. Nobel Akademik Yayıncılık.

Altıntaş, K. M., & Asal, S. (2020). *Ekonomik istihbarat kapsamında endüstriyel espiyonaj:Ticari tüzel kişilikler açısından endüstriyel casusluğun stratejik önemi* (5. baskı). Nobel Akademik Yayıncılık. ISBN: 978-625-439-223-8

Altıntaş, K. M. (2021a). Comparative analysis of strategic relationship between industrial versus corporate espionage within the framework of implementation methods. *Global Security and Intelligence Studies, 6*(1), 105–124. https://doi.org/10.18278/gsis.6.1.5

Altıntaş, K. M. (2021b). İstihbarata karşı koyma prensipleri bakımından atık istihbaratının stratejik önemi ve karşılaştırmalı analizi. *Uluslararası Kriz ve Siyaset Araştırmaları Dergisi, 5*(2), 879–914.

Baltacı, H. (2015). Ekonomik güvenlik bağlamında ekonomik istihbaratın rolü ve önemi. In S. Aydın (Ed.), *Ekonomik istihbarat* (pp. 81–132). Adalet Yayınevi.

Benny, D. J. (2014). *Industrial espionage: Developing a counterespionage program*. Taylor & Francis Group.

BITKOM. (2024). *German businesses under attack: Losses of more than 220 billion euros per year*. URL: https://www.bitkom.org/EN/List-and-detailpages/Press/German-business-losses-more-than-220-billion-euros-per-year.

Conner, N. (2021, January 27). *MI5 began probe into British embassy security guard accused of being 'Putin spy' in Berlin after he stopped using his credit and debit cards*. Daily Mail. https://www.dailymail.co.uk/news/article-9893287/MI5-began-probe-accused-Putin-spy-stopped-using-credit-cards.html

Cyber Security News. (2025, March 13). US charges 12 Chinese hackers for hacking national security infrastructure. https://cybersecuritynews.com/us-charges-12-chinese-hackers.

Defence News. (2024). *Top 100 for 2024*. https://people.defencenews.com/top-100.

Carlisle, R. (2015). *Encyclopedia of intelligence and counterintelligence*. Routledge.

Elizabeth, Y. N., Yu, L. M., Palmer, D. P., & Anyomi, B. (2021). Unfair competition in the field of intellectual property rights: Analyzing concepts, acts of unfair competition and laws. *Journal of Politics and Law, 14*(3).

Gehl, R. W., & Lawson, S. T. (2022). *Social engineering: How crowdmasters, phreaks, hackers, and trolls created a new form of manipulative communication*. MIT Press.

Godson, R. (2004). *Dirty tricks or trump cards: U.S. covert action & counter intelligence*. Transaction Publishing.

Kahn, R. A. (2017). Economic espionage in 2017 and beyond: 10 shocking ways they are stealing your intellectual property and corporate mojo. *Business Law Today*, 1–5.

Kalkan, D. (2025). Savunma sanayinde milli teknoloji hamlesi: Ankara ili örneği. *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, 86*, 582–596.

Kavsıracı, O., & Demirbaş, M. (2020). İstihbarat faaliyetlerinin devlet güvenliği açısından incelenmesi. *Anadolu Strateji Dergisi, 2*(1).

Kurç, Ç., & Neuman, S. G. (2017). Defence industries in the 21st century: A comparative analysis. *Defence Studies, 17*(3), 219–227. https://doi.org/10.1080/14702436.2017.1353537

Lewis, J. (2018). *Economic impact of cybercrime, no slowing down*. McAfee.

Lippoldt, D. C., & Schultz, M. F. (2014). Trade Secrets, Innovation and the WTO. *E-15 Think Piece. Geneva: ICTSD and WEF, with IMD*.

McKown, C. (2021, January 27). *The American Greed report: Corporate spying costs billions, can it be stopped?* CNBC. https://www.cnbc.com/2017/05/13/the-american-greed-report-corporate-spying-costs-billions-can-it-be-stopped.html

Miller, G. (2020). The intelligence coup of the century. *The Washington Post*. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

Nebil, F. S. (2024, April 1). *Savunma sanayii'nden Hollanda'ya giden Türk mühendis sayısı 1.300 oldu*. Türk-İnternet.com. https://turk-internet.com/savunma-sanayiinden-hollandaya-giden-turk-muhendis-sayisi-1-300-oldu/

Özdağ, Ü. (2018). *İstihbarat teorisi*. Ankara: Kripto Basım Yayım Dağıtım.

Özdemir, E. (2010). Rekabet istihbaratı toplama ve etik: Bir alan araştırması. *İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, 43*, 67–95.

Porteous, S. D. (1994). Economic espionage: Issues rising from increased governmental involvement with private sector. *Intelligence and National Security*, 9(4), 735–752.

Reuters. (2010, October 23). *American pleads guilty to trying to spy for China*. https://www.reuters.com/article/us-usa-china-spying-idUSTRE69L3CK20101022/

Reuters. (2019, December 1). *Airbus dismisses 16 employees in German compliance investigation*. https://www.reuters.com/article/business/airbus-dismisses-16-employees-in-german-compliance-investigation-idUSKBN1Y5149/

Rowe, W. & Brook, T. (2009). *China's Last Empire: The Great Qing.* Cambridge, Massachusetts: The Belknap Press of Harvard University Press. p. 368. ISBN 978-0-674-03612-3.

Salleh A. K. & Janczewski L. (2016) Technological, Organizational and Environmental Security and Privacy Issues of Big Data: A Literature Review. *Procedia Computer Science*. December. 100: 19-28. DOI:10.1016/j.procs.2016.09.119.

Sanayi ve Teknoloji Bakanlığı. (2021–2024). *Girişimci bilgi sistemi*. https://gbs.sanayi.gov.tr/

Sevinç, S. (2022). *İstihbarata karşı koyma faaliyetleri kapsamında bir örnek olay incelemesi: Rubicon operasyonu.* (Yüksek Lisans Tezi, Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü, Ankara).

South China Morning Post. (2020, November 18). *Former Raytheon engineer jailed for exporting military-related tech to China.* https://www.scmp.com/news/china/diplomacy/article/3110339/former-raytheon-engineer-jailed-exporting-military-related

Savunma ve Havacılık Sanayi İmalatçılar Derneği (SASAD). (2023). *Performans raporu*. https://www.sasad.org.tr/sasad-sektor-performans-raporu-2023-1751544308

SIPRI. (2024). *Military expenditure database: Armaments, disarmament and international security*. https://www.sipri.org/sites/default/files/2024-06/yb24_summary_en_2_1.pdf

SIPRI. (2025). *Military expenditure database: Armaments, disarmament and international security*. https://www.sipri.org/sites/default/files/2025-06/yb25_summary_en.pdf

Solberg Søilen, K.S., (2016). Economic and industrial espionage at the start of the 21st century –Status quaestionis. *Journal of Intelligence Studies in Business, 6*(3), 51–64.

Schweizer, P. (1993). *Friendly spies: How America's allies are using economic espionage to steal our secrets*. New York: Atlantic Monthly Press.

Søilen, K.S. (2016) Economic and industrial espionage at the start of the 21st century–status quaestionis. *Journal of Intelligence Studies in Business*, 6 (3) pp. 51-64. DOI: https://doi.org/10.37380/jisib.v6i3.196

Şeşen, Y., Kuzucuoğlu, A.H. (2021). Veri ve Bilgi Güvenliği Bağlamında İstihbarat Faaliyetleri. *Lamre Journal*, 2(2), 93-110.

TASAM-Türk Asya Stratejik Araştırmalar Merkezi. (2016). *Küreselleşmenin boyutları ve etkileri*. https://tasam.org/tr-TR/Icerik/211/kuresellesmenin_boyutlari_ve_etkileri

T.C. Cumhurbaşkanlığı Yatırım ve Finans Ofisi. (2024). *Savunma ve havacılık*. https://www.invest.gov.tr/tr/sectors/sayfalar/defensandaerospace.aspx#:~:text=Savunma%20sanayiinin%20i%C5%9F%20hacmi%20son,den%20fazla%20%C5%9Firket

T.C. Cumhurbaşkanlığı Savunma Sanayi Başkanlığı. (2023). *2024–2028 savunma sanayi sektörel strateji dokümanı*. https://www.ssb.gov.tr/Images/Uploads/MyContents/F_20240917164305314800.pdf

T.C. Cumhurbaşkanlığı Savunma Sanayi Başkanlığı. (2025). *2024 yılı faaliyet raporu*. http://www.sp.gov.tr/upload/xSPRapor/files/ut8N6+SSB_2024_Yili_Faal_Rap.pdf

Tezsever, S. (1999). Milli Güvenliğimiz İçinde İstihbarat. *İstanbul: İstanbul Üniversitesi Basımevi*.

Toren, P. (2018, February 14). Some lessons from the Waymo (Alphabet) versus Uber theft of trade secret litigation. *Ipwatchdog*. http://www.ipwatchdog.com/2018/02/14/waymouber-theft-trade-secret-litigation/id=93528/

Toriola, T. (2011). *Industrial Espionage or Competitive Intelligence*. Purdue University. https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2011-10report.pdf.

Törenli, N. (2007). Küreselleşen dünyada bilgi güvenliği ve Türkiye. III. İletişim Teknolojileri Ulusal Sempozyumu (ITUSEM) Bildiriler Kitabı, Adana.

Urhal, Ö. (2008). *Kamu güvenliği açısından istihbarat ve örgütlü suçlar*. Adalet Yayınevi.

U.S. Department of Justice. (2025, September 15). Former defence contractor sentenced to over 10 years in prison for attempted espionage. Office of Public Affairs. https://www.justice.gov/opa/pr/former-defence-contractor-sentenced-over-10-years-prisonattempted-espionage

U.S. Department of Justice. (2025, November 5). Fiber laser expert convicted by federal jury of economic espionage and theft of trade secrets.

https://www.justice.gov/opa/pr/fiber-laser-expert-convicted-federal-jury-economic-espionage-and-theft-trade-secrets

Verizon Business. (2025). *Data breach investigations report-2025: Executive summary*. https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf

Yılmaztürk, A. (2023). Türkiye'de savunma sanayi sektörü ve ekonomi üzerindeki etkisinin değerlendirilmesi. *Enderun Dergisi, 7*(2), 139–165.

Wagner, R. E. (2012). Bailouts and the potential for distortion of federal criminal law: Industrial espionage and beyond. *Tulane Law Review, 86*(5), 1017–1055.

Waziri, K. M., & Yerima, T. F. (2011). Industrial espionage and intellectual property rights protection: How legal is it legal. *International Journal of Sustainable Development, 4*(3), 1-22.