Marmara Üniversitesi Siyasal Bilimler Dergisi • Marmara University Journal of Political Science • Cilt 14, Sayı 1 Mart 2026
ISSN 2147-6926, ss. 1-15 • DOI: 10.14782/marmarasbd.1794718

RESEARCH ARTICLE / ARAŞTIRMA MAKALESİ

Emerging Defense Industries and the Growing Espionage Threat: A Case Study of Türkiye

Yükselen Savunma Sanayileri ve Artan Casusluk Tehdidi: Türkiye Örneği

Yusuf DİNÇEL*

Abstract

Defense industries have become one of the most critical pillars of national sovereignty and strategic autonomy in today's world, where technological developments are accelerating and geopolitical competition is intensifying. The case of Türkiye is particularly noteworthy, as it illustrates how the achievements of emerging powers in the defense sector simultaneously generate growing security vulnerabilities. This article constitutes a single-case analysis grounded in qualitative research methods and draws on multiple sources, including think tank publications, academic literature, and media accounts. The article examines five major espionage incidents directly targeting the Turkish defense industry and, through comparative analysis, identifies recurring patterns and threat dimensions. The findings reveal that Türkiye's rapid advancements in unmanned aerial vehicles, guided missile technologies, and electronic warfare systems have rendered it a priority target for hostile actors. The espionage methods identified include phishing-based cyberattacks, leaks of classified project information, illicit data trade via social media platforms, and covert operations. Turkish intelligence institutions, most notably the National Intelligence Organization (MİT), have developed a range of countermeasures in response, such as preventive briefings, security screenings, and targeted operations. Nevertheless, vulnerabilities in digital infrastructure and insider threats continue to expose critical components of defense projects to external exploitation. In conclusion, espionage activities directed at Türkiye's defense sector are multifaceted, adaptive, and strategically consequential. These threats affect not only the security of companies but also the country's national security strategies. The case of Türkiye reveals a broader reality, indicating that espionage attempts will increase in parallel with the progress in the defense industry.

Keywords: Defense Industry, Türkiye, Espionage, Counterespionage, National Security

* Dr. Öğr. Üyesi, Uluslararası İlişkiler Bölümü, Polis Akademisi, Ankara, dncl_10@hotmail.com, ORCID: 0000-0002-2615-6025

How to cite this article/Atıf için: Dinçel, Y. (2026). Emerging Defense Industries and the Growing Espionage Threat: A Case Study of Türkiye. *Marmara Üniversitesi Siyasal Bilimler Dergisi, 14*(1), 1-15. DOI: 10.14782/marmarasbd.1794718

Makale Gönderim Tarihi: 1 Ekim 2025 **Yayına Kabul Tarihi:** 12 Şubat 2026

Öz

Savunma sanayileri, teknolojik gelişmelerin hızlandığı ve jeopolitik rekabetin yoğunlaştığı günümüzde ulusal egemenliğin ve stratejik özerkliğin en kritik unsurlarından biri hâline gelmiştir. Türkiye örneği, yükselen güçlerin savunma alanındaki başarılarının aynı zamanda artan güvenlik açıklarını da beraberinde getirdiğini göstermesi bakımından dikkat çekicidir. Bu makale, nitel araştırma yöntemlerine dayalı tekil bir vaka çalışması niteliği taşımakta olup, düşünce kuruluşu yayınları, akademik literatür ve medya haberleri gibi farklı kaynaklardan elde edilen verilerden yararlanılmıştır. Bu makalede, Türk savunma sanayisini doğrudan hedef alan beş önemli casusluk olayı ele alınmış, karşılaştırmalı analiz yoluyla tekrar eden kalıplar ve tehdit boyutları ortaya konulmuştur. Elde edilen bulgular, Türkiye'nin özellikle insansız hava araçları, güdümlü füze teknolojileri ve elektronik harp sistemlerindeki hızlı ilerleyişinin, onu hasım aktörler açısından öncelikli bir hedef haline getirdiğini göstermektedir. Tespit edilen casusluk yöntemleri arasında oltalama temelli siber saldırılar, gizli projelere ilişkin bilgi sızıntıları, sosyal medya platformları üzerinden yasa dışı veri ticareti ve gizli operasyonlar öne çıkmaktadır. Türkiye'nin istihbarat kurumları, özellikle Millî İstihbarat Teşkilâtı (MİT), bu tehditlere karşı brifingler, güvenlik taramaları ve hedefe yönelik operasyonlar gibi çeşitli karşı tedbirler geliştirmiştir. Ancak, dijital altyapıdaki zafiyetler ve içeriden gelen tehditler, savunma projelerinin kritik bileşenlerini hâlâ risk altında bırakmaktadır. Sonuç olarak, Türkiye'nin savunma sanayisine yönelik casusluk faaliyetleri çok boyutlu, uyarlanabilir ve stratejik sonuçlar doğuracak niteliktedir. Bu tehditler yalnızca şirketlerin güvenliğini değil, aynı zamanda ülkenin ulusal güvenlik stratejilerini etkilemektedir. Türkiye örneği, savunma sanayinde ilerlemenin artmasına paralel olarak casusluk girişimlerinin de artacağına işaret eden daha geniş bir gerçeği ortaya koymaktadır.
Anahtar Kelimeler: Savunma Sanayi, Türkiye, Casusluk, Karşı Casusluk, Ulusal Güvenlik

1. Introduction

National defense has always been a cornerstone of state sovereignty, yet in the contemporary era it is increasingly shaped by rapid technological progress and intense geopolitical competition. Defense industries have transformed from being simple suppliers of military hardware into complex ecosystems where innovation, security, and strategy intersect. As nations expand their technological capacity, they not only seek independence from foreign suppliers but also become attractive targets for external interference. Among the most pressing challenges confronting these industries today is the rise of espionage, which manifests in both traditional and cyber domains.

Espionage targeting the defense sector is not a new phenomenon; however, the methods employed have grown significantly more sophisticated. While classical practices relied on human networks and physical infiltration, modern approaches often exploit digital vulnerabilities, supply chains, and even open sources of information. This dual nature of espionage, where human and cyber elements intertwine, places defense industries at the very center of global security debates.

The case of Türkiye provides a particularly compelling context for examining this phenomenon. Over the past two decades, Türkiye has undergone a remarkable transformation in its defense sector, shifting from dependency on external suppliers to becoming an exporter of advanced systems. This rapid development has elevated its international profile but has also exposed the sector to heightened risks, as evidenced by multiple espionage incidents ranging from cyber intrusions to insider leaks. Türkiye's geopolitical location further amplifies its exposure to

intelligence operations by external actors, making its defense industry both a symbol of strategic autonomy and a target of hostile interest.

This study adopts a qualitative single-case study design to analyze the dynamics of espionage in Türkiye's defense industry. The case study method is well-suited for examining the complex intersections of politics, economics, and security, and while Türkiye constitutes the primary focus, comparative references to the experiences of the United States (U.S.), Russia, China, and European countries help situate the findings within a broader context. Multiple data sources were employed: policy reports prepared by think tanks such as SETA, SWP, and IISS; academic articles and books; and national and international media accounts.

Five major espionage incidents were examined in detail: the Dropping Elephant cyberattack; the 2021 insider information leaks involving Defense Industry Agency (SSB) employees and military personnel; the disclosure of import-export data via Telegram; the information-sharing case involving 26 FETO-affiliated individuals; and the prosecution of Mustafa Tanrıverdi, former Director of the Mechanical and Chemical Industry Corporation (MKEK). Together, these cases reveal recurring patterns such as cyber threats and insider infiltration. Data saturation was reached when common themes began to recur, indicating that further case inclusion would not substantially alter the findings.

While this research is contextually bounded to Türkiye, its methodological approach and diverse case selection enhance the reliability and transferability of the results, enabling meaningful inferences for other emerging defense industries under comparable conditions. Ultimately, the central question guiding this study is: to what extent does espionage shape the resilience and strategic autonomy of an emerging defense industry, and what vulnerabilities and risks accompany this transformation? Addressing this question through the case of Türkiye sheds light on broader debates regarding sovereignty, technological independence, and the global dynamics of power.

2. Theoretical Framework: The Relationship between the Defense Industry and Espionage

The concept of national defense occupies a significant place in international relations literature. All countries, before being exposed to any threat, seek to strengthen their national defense with the support of the defense industry sector. According to Paul R. Viotti, national defense affects a nation's security, bureaucracy, and decision-makers, and should be considered within the framework of interstate relations. The nationalization of the defense industry and the reduction of dependency on other countries is a strategy preferred by all states, as it holds critical importance for national sovereignty (Özer, 2019, pp. 23-24).

Cases of espionage within the defense industry are generally associated with industrial espionage in literature. The statement made by U.S. President Ronald Reagan on 30 November 1985 regarding espionage, "Espionage should not be perceived as a game; if we value our freedom and

way of life, we must confront this phase of struggle seriously", highlights the critical importance of combating espionage. In a world where foreign intelligence services and terrorist groups exist, the fight against espionage remains a priority for states. Industrial espionage refers to attempts by competing companies or foreign intelligence services to obtain or copy, without authorization, an institution's confidential and sensitive information through technical surveillance. Industrial intelligence should not be confused with competitive intelligence. In competitive intelligence, the focus is on information about rival firms collected from open sources. The analysis of this information to reach conclusions is considered a legal and ethical activity (Benny, 2014, pp. 1-3).

Through industrial espionage, states or companies can incur substantial material losses (Hou & Wang, 2020, p. 1). In traditional industrial espionage, the theft of physical documents, plans, formulas, prototypes, and materials is involved. However, in modern industrial espionage, a target company's information is acquired through breaches of cybersecurity. Regardless of whether espionage is traditional or modern, insider collaboration is a prevalent feature of industrial espionage cases (Philips & Pohl, 2025, p. 143). Industrial espionage is conducted to gain economic and political advantages. In this context, it may be carried out for personal or corporate profit, to strengthen a state's foreign policy, or to enhance its defense capabilities (Hamilton, 1967, p. 3).

Historically, there has been intense competition in the field of industrial intelligence, particularly between the U.S. and the Soviet Union, both during the Cold War and in the preceding years. In the 1930s and 1940s, the Soviet Union closely monitored American military-industrial technology. During this period, many Soviet engineers were employed in industrial facilities in the U.S. Consequently, some engineers engaged in espionage on behalf of the Soviets attempted to gather information about the U.S. military and defense industry capacity. Furthermore, during World War II, Soviet spies operated within the U.S. government to assess American military capabilities (Sibley, 1999, pp. 95-97). Similarly, during the Cold War, a comparable struggle occurred between West and East Germany. During this period, Gerhardt Ronneberger, an electrical engineer employed in Western Europe as an industrial spy by the East German intelligence agency Stasi, sought to acquire classified technologies in the West (Zatlin, 2008, p. 49).

In the modern era, the defense industry is primarily targeted through cyber espionage. For example, China employs cyber espionage against the U.S. Rather than attempting to replicate all U.S. weapons technologies, Chinese actors focus on espionage targeting more critical subsystems. In this context, Chinese hackers have targeted private companies, law firms, and intermediary firms that are closely associated with military technologies (Farley, 2016, pp. 6-7). Throughout history, states have engaged in espionage to obtain information about each other's military capabilities. The rise of a state's defense industry attracts the attention of other states, and espionage techniques are frequently employed to accurately assess its capacity.

Furthermore, European states have historically struggled to develop a robust defense industry due to their long-standing reliance on the security guarantees provided by the U.S. Within this context, during the ongoing war between Russia and Ukraine that began in 2022, it was

observed that European countries were relatively weak in producing artillery shells and other military equipment, and consequently, they were unable to provide adequate support to Ukraine. Following these developments, European states have aimed to increase domestic production within their defense industries and reduce dependence on overseas sources. While facing financial constraints, European armies have also recognized security vulnerabilities in products imported from China. This situation has allowed China to conduct industrial espionage activities across Europe and to increase its influence within European defense industry facilities through the products it supplies. In 2023, it was revealed that a Chinese government-owned company, which produces armored vehicles, had been designing interior spaces for the Dutch military for over a decade. The Dutch military, which had placed its first order with this company in 2013, had not conducted an intelligence review of the company and had procured millions of dollars' worth of services. Even the subcomponents supplied by Chinese companies to European states create opportunities for China to access sensitive information regarding the defense industries of these countries. European defense industries are heavily reliant on microchips manufactured in China, prompting efforts to source these components from alternative countries. Notably, North Atlantic Treaty Organization (NATO) member states have been importing certain critical components from China to develop their weapons systems. Furthermore, it has been identified that products sourced from China are used in military equipment such as air defense radar systems and fighter jets. The origin of subcomponents used in large systems produced by defense industry companies in the U.S. or Europe represents a critical detail. In this context, states such as China can conduct espionage on military systems through the components they supply to these subsystems (Dyami Analysts, 2024).

3. Türkiye's Rising Defense Industry: Institutional and Strategic Background

Türkiye's high performance in the defense industry in recent years, particularly its evolution from an import-dependent position to an export-oriented one, has attracted the attention of many states at the global level. Within this framework, it is necessary to assess the factors that have contributed to Türkiye's attainment of this position. Following its accession to NATO in 1952, Türkiye required increased foreign assistance to strengthen its military capabilities. While this reliance contributed to the strengthening of the Turkish Armed Forces, it simultaneously hindered the development of the domestic defense industry. During this period, dependency on U.S. military equipment intensified. Furthermore, following Türkiye's military intervention in Cyprus in 1974, the U.S. imposed an arms embargo on Türkiye, clearly illustrating the consequences of external dependency in the defense industry. After this date, Türkiye recognized the need to establish a national defense industry using domestic resources. In this context, Aselsan, a company engaged in military production and currently a key investor in Türkiye's defense sector, was founded in 1975. Additionally, in 1985, the Defense Industry Development and Support Administration (Savunma Sanayi Geliştirme ve Destekleme İdaresi Başkanlığı, SAGEB) was established. However, due to regional conflicts, financial crises, and arms embargoes, Türkiye was unable to achieve significant momentum in the defense industry during this period. While many

NATO member states reduced defense spending following the end of the Cold War, Türkiye continued to seek military equipment from its European and American allies due to separatist activities in the southeast by the PKK terrorist organization and disputes with Greece over the Aegean Sea and Cyprus. During this period, Türkiye faced both overt and covert arms embargoes. This situation fostered a sense of isolation and underscored the importance of domestic weapons production. By 2002, with the Justice and Development Party (AKP) coming to power, the new government prioritized domestic solutions over technology transfer in the defense sector. After 2010, investments in Türkiye's defense industry increased, and following 2016, the sector entered a process of restructuring (Baysal, 2025, pp. 31-24; Egeli et al., 2024, pp. 14-16). Today, there is a close relationship between the rising trajectory of Türkiye's defense industry and its foreign policy initiatives. At various points, when the supply of military equipment requested from Western allies was restricted, Türkiye increasingly recognized the critical importance of domestic production within the defense industry.

Türkiye's current armament projects are managed by the SSB, a state-affiliated institution. This body identifies the deficiencies in the modernization of the Turkish Armed Forces and develops projects accordingly. Within the present system, the SSB is directly subordinated to the Presidency and therefore operates under political directives concerning the defense industry. Significant progress has been achieved in the sector following the alleviation of SSB's budgetary responsibilities and its acquisition of the authority to finance weapons projects in Türkiye. Today, the leading defense industry companies in Türkiye include TUSAŞ, Baykar, Roketsan, STM, and Aselsan. Despite negative economic indicators in recent years due to inflation, defense expenditure has remained unaffected by the country's challenging economic conditions. In 2001, Türkiye's defense spending within the central budget was $7.22 billion, whereas by 2024 this figure had risen to approximately $25 billion. Moreover, according to 2023 data, 80% of the components used in the Turkish defense industry were supplied through domestic production, compared to 73% in 2022. Parallel to these developments, Türkiye's arms exports have increased significantly. In 2014, Türkiye's arms exports were approximately $1.9 billion; by 2024, the value of defense and aerospace exports had reached $7.154 billion. Export activities targeting Africa, Asia, and Gulf countries have been steadily rising. Weapon systems produced by the Turkish defense industry have been deployed in various conflict zones around the world and have proven their effectiveness. One of the most significant components of Türkiye's defense industry is the production and export of military drones. The Bayraktar TB2 drone, produced by the Turkish company Baykar, is currently in the military inventories of 34 different countries. In 2024, Baykar's export volume reached $1.8 billion (Bastian, 2024, pp. 2-4).

Since 2020, the trajectory of Türkiye's relations with African countries has increasingly been shaped by a security dimension. In this context, unmanned aerial vehicles (UAVs) have become the focal point across the continent. The success of Turkish drones, particularly the Bayraktar TB2, on the battlefield during the conflicts in Libya and Nagorno-Karabakh has drawn considerable international attention. Turkish-origin drones are regarded as effective in terms of combat techniques while also being cost-efficient, making them an attractive option for the defense

strategies of other states. Turkish weapons systems are not limited to UAVs but also include naval platforms, helicopters, and armored vehicles, which have proven effective as well. Armaments produced by the Turkish defense industry are currently used by the militaries of Senegal, Mali, Niger, Uganda, Ethiopia, Côte d'Ivoire, Nigeria, and Kenya (Donelli, 2022). Through these arms sales, Türkiye's trade volume with African states has been steadily expanding. Moreover, the Turkish government has strategically employed the defense sector as a tool of political and diplomatic influence.

In parallel with domestic and international developments over the last two decades, Türkiye has made significant progress in the field of defense industry in order to safeguard its national security. Türkiye's military and defense strategy entered a major transformation following the Arab Spring uprisings that erupted in the Middle East in 2011. The increasing activities of non-state armed groups in both neighboring and more distant regions, the redrawing of nation-state borders, the proliferation of proxy wars, and the struggle for power among Middle Eastern states posed direct threats to Türkiye's national security, prompting Ankara to adopt a more proactive foreign policy. This policy shift compelled Türkiye to pursue an ambitious military strategy. In particular, the developments during the Syrian civil war and the associated security threats emanating from this region led Türkiye to implement a strategic and tactical-level military approach (Yeşiltaş, 2020, pp. 90-92). At this point, it has been observed that military equipment produced by the Turkish defense industry has been effectively employed in precision operations. Türkiye's foreign policy initiatives are thus often shaped in parallel with advances in its defense industry, a dynamic that is critical for understanding the country's strategic preferences and security-oriented policies in the international arena.

4. Espionage Threats Targeting Türkiye's Defense Industry

Espionage can be conducted through classical human intelligence (HUMINT) methods as well as in cyberspace. Cyber espionage is defined as the act of gaining access to sensitive information belonging to a rival state or corporation through computers and subsequently selling this information for financial gain. While an individual engaged in traditional espionage on behalf of a foreign country may be prosecuted if apprehended, identifying and capturing cyber espionage perpetrators is not always feasible. Nevertheless, this does not alter the fact that cyber espionage constitutes a form of espionage. Due to its capacity to exfiltrate large volumes of data, cyber espionage is considered to be more intrusive than traditional espionage (Weissbrodt, 2013, pp. 370-372). Rival states not only employ traditional espionage techniques but also resort to cyber espionage. The primary factors that render cyber espionage attractive for states are its relatively low cost and the difficulty in conclusively attributing such operations to specific actors.

In recent years, espionage activities have accelerated in parallel with the growing capacities of states in the defense industry. In this regard, Türkiye's enhanced ability to manufacture critical military assets such as drones, electronic warfare systems, and guided missiles has not only drawn

scrutiny from allied states but has also become a focal point for rival actors. Cyber espionage operations targeting the projects, Research and Development (R&D) activities, or strategic decision-making processes of Türkiye's defense industry do not merely aim to undermine its economy but also have the potential to generate severe military and diplomatic consequences. In this context, the cyber espionage campaign conducted by the group known as Dropping Elephant against the Turkish defense sector warrants particular attention. Emerging in 2015, Dropping Elephant has carried out cyber operations targeting military, political, and economic institutions across the globe, with a primary focus on China and Southeast Asian countries. Additionally, in 2018, the group targeted think tanks in the U.S. (Unaran, 2025).

The attack was launched in July 2025 through fraudulent conference invitation emails concerning UAVs, which contained LNK file attachments disguised as harmless documents. When opened by the targeted Turkish defense company, the malicious files enabled cyber intruders to gain access to comprehensive data related to UAVs. The timing of this cyberattack is particularly noteworthy, as it coincided with the continuation of close defense cooperation between Türkiye and Pakistan, against the backdrop of persistent military tensions between India and Pakistan. In this sense, the attack can be interpreted as an operation driven by geopolitical motivations (Arctic Wolf, 2025). This case exemplifies a sophisticated form of cyber espionage aimed at undermining Türkiye's recent rise in the defense industry. Through this attack on a single defense company, Türkiye's national security was directly threatened, and its strategic defense capacity was deliberately targeted (Unaran, 2025). The campaign represents a transition to asymmetric intelligence warfare, in which low-cost phishing methods are employed against high-value military research and development. The timeframe indicates that it involved not only data theft but also strategic sabotage of Türkiye's diplomatic defense. Through active cooperation with Pakistan, the attackers intended to obtain a local tactical advantage by targeting certain UAV technologies. Technically, the present case highlights that the human aspect of the human-computer interface in defense security is the most vulnerable, which is why zero-trust architecture is required in corporate communications.

In addition to cyber espionage, attacks targeting the Turkish defense industry have also been carried out through traditional espionage. In April 2021, a group consisting of employees of the SSB and military personnel transferred information regarding classified defense industry projects to foreign-based companies. Investigations conducted by security forces revealed that these individuals sold highly classified project data in exchange for money, and as a result, they were arrested (Taşdan, 2021). It has been observed that individuals working in the defense industry sector and personnel employed in security institutions may engage in espionage activities under the guidance of foreign intelligence services. The incident of selling crucial defense industry information in exchange for financial incentives underscores the sensitivity and strategic importance of this sector.

The SSB leak underscores the importance of insider threats in high-level procurement agencies. Contrary to offenders outside a company, employees know which pieces of data are the most

harmful when shared, e.g., tender specifications or cost-benefit studies. This case demonstrates that monetary rewards are still a strong instrument of foreign intelligence agencies even in highly patriotic industries. It requires the replacement of periodic security clearances with continuous behavioral checks and a least-privilege access policy in state defense institutions to reduce the chances of institutional betrayal.

In another case, it was revealed that confidential import and export data, as well as information related to weapons technologies belonging to leading Turkish defense companies, had been offered for sale on Telegram and other social media platforms. According to a statement by the Turkish Ministry of Trade, the perpetrators obtained data from the ministry's systems through illegal means and sold it on foreign websites. A subsequent investigation by the public prosecutor's office found that the leaked information had reached a level that could threaten Türkiye's national security and may have been accessed by terrorist organizations and foreign intelligence services. It was further determined that data on Aselsan's production of automatic weapons and machine guns had been sold to companies in East Asia possessing large-scale databases. In response, intelligence and law enforcement units created a fake Telegram account to identify individuals operating within the espionage network. Following the operations, seven people were arrested, and an examination of their banking transactions revealed thousands of dollars in transfers from foreign companies (Newsroom, 2025).

The normalization of espionage is an indication of the commodification of defense information on messaging services such as Telegram. Strategic intelligence ceased to be solely the preserve of state actors; it has become an online asset that can be purchased and sold on the black market. The databases of East Asian inclusion suggest that the secrets of defense trade in Türkiye are being cultivated as competitive intelligence and for reverse-engineering. The weakness of this case is structural: the security of defense data is only as strong as the weakest administrative system (e.g., managing the customs/trade systems, which was evident in the given case), which demands an integrated umbrella of security across all government ministries.

It is known that the FETO terrorist organization has previously engaged in activities threatening Türkiye's national security by exposing classified information from the defense industry. In March 2021, during a joint operation carried out by Turkish intelligence and law enforcement units, 26 individuals were detained on charges of conducting espionage in the Turkish defense industry. According to official statements, the detainees were members of FETO and had previously worked in defense industry companies such as Aselsan, Roketsan, and Havelsan. Moreover, it was determined that they had shared information on Turkish defense projects, including pricing, technical specifications, and contracts with foreign defense companies (Bekdil, 2021).

The case explains how ideologically driven so-called sleeper cells can evolve into industrial spies. The joint information (pricing and contracts) implies a mission to decompose the competitiveness of Türkiye in the international market. Such leaking of technical specifications gives foreign competitors the means to work out countermeasures against Turkish systems before they are even

introduced. This emphasizes that counterespionage should involve due diligence on the history of personnel to guard against ideologically motivated sabotage, which is much harder to discover than mere monetary motivation.

As observed in the aforementioned cases, corporate espionage techniques have been employed against the defense industry sector. Accordingly, foreign intelligence services have targeted the defense industry to gain access to sensitive technologies, military advancements, and state secrets. Individuals engaged in espionage may either be former employees of defense industry organizations or continue to work actively within them. In the intelligence literature, such individuals are referred to as insider threats. Those categorized as insider threats can access sensitive data through their security clearances. Detecting insider threats within institutions related to the defense industry is particularly challenging. In addition, instances of Intellectual Property (IP) theft frequently emerge within the defense sector. In this context, the theft of project plans and designs concerning weapons systems, aircraft, and other military equipment is typically organized through insider information, cyberattacks, supplier and subcontractor networks, covertly operating front companies, and the coordination of international logistics channels. Rival actors who obtain such classified information are able to replicate projects, whose research and development processes normally span many years, at significantly lower costs. This type of espionage is therefore considered a priority risk factor for the state as a whole.

Many defense industry institutions collaborate with supplier firms. Individuals acting with espionage motives may infiltrate supply chains through these companies and gain access to critical information. Furthermore, such individuals may obtain opportunities to implant malicious software into systems. In some cases, spies prefer direct physical surveillance methods to gather information on defense industry projects. For example, they may record meeting conversations or exploit personal relationships to collect sensitive planning data. Finally, cyber espionage is often employed with the aim of seizing defense industry projects (ISI Defense, 2024).

5. Counterespionage in the Turkish Defense Industry: Strategies and Intelligence Practices

The concept of counterintelligence, as noted above, is not limited solely to espionage activities; it is also directly related to processes of information transfer and the corruption of knowledge. Whether in the domains of policy or technology, the transmission of information can significantly alter an actor's informational advantage. Similarly, the loss of strategically significant information can result in the forfeiture of critical advantages to rival or adversarial actors and initiate a process of decline. The transfer of knowledge and technology poses a threat to the national security of many countries worldwide. Regardless of whether the threatening actor is foreign or domestic, or whether they operate through insider or cyber espionage, the fundamental objective remains the acquisition of informational superiority (Tromblay, 2017, pp. 2-3). In the defense industry, the transfer of information or technology is a common occurrence due to espionage elements. At this

point, it is essential for states to provide training to individuals working in this sector, whether in the public or private domain, to mitigate the risks associated with espionage.

In order to prevent espionage incidents in the defense industry, it is first necessary to raise the awareness of individuals working within this sector. In parallel with technological advancements, there are situations today in which spies do not necessarily need direct access to defense industry institutions. Publicly available social media posts constitute a significant source of open-source intelligence. For example, when an engineer working in the defense sector shares information about a project they are involved in or announces their travel to another city via social media, it poses a considerable security risk. Job postings on platforms such as LinkedIn should avoid unnecessary disclosure of sensitive information, and company executives should be aware that competitors may monitor statements regarding new products. While information shared publicly may not pose a direct threat on its own, the aggregation of multiple open-source pieces can reveal critical insights about a defense company's projects. An employee in the defense industry might receive invitations via email to attend fully funded conferences or visit overseas defense facilities. It is important to recognize that such offers are among the classic methods employed by intelligence services. Furthermore, an employee accepting such an offer faces a high risk of malware being installed on their laptop while abroad. Hotel rooms may also be targeted in operations conducted by intelligence agencies. During breaks between conference sessions, an intelligence officer may engage the employee in dialogue to extract information about them or their company. Broad questions posed during post-session Q&A segments may also serve as pretexts for informal conversations, allowing for a more personal rapport to be established. Invitations from unfamiliar institutions should therefore be evaluated with this perspective in mind. Moreover, the "honey trap" scenario frequently depicted in espionage films also occurs in real life. A high-ranking employee of a defense company may engage in seemingly innocent conversations with an attractive and persuasive individual encountered at an event, which could later escalate into blackmail and the disclosure of critically important information. Individuals acting with espionage intent often use flattery to distract their targets. It is crucial to recognize that Russian and Chinese intelligence services are particularly experienced in conducting honey trap and blackmail operations (Ivezic, 2025).

The incidents described above can potentially affect any personnel working in critical institutions. For this reason, it is essential for the counterintelligence units of intelligence agencies to adequately inform the public. For instance, in Türkiye, the MİT has conducted briefings specifically targeting individuals employed in the defense industry. Given the rapid growth of Türkiye's defense sector in recent years, particularly in the production of UAVs and other military equipment, it has attracted the attention of foreign intelligence services. In this context, between 2009 and 2020, personnel assigned to MİT's counterintelligence units organized informational meetings on espionage for approximately 22,000 employees across 411 different institutions (Hürriyet Daily News, 2022). MİT carefully monitors the activities of foreign intelligence services targeting the defense industry and conducts operational measures at appropriate times. For example, in 2021, Mustafa Tanrıverdi, the Director of the MKEK Kırıkkale Weapons Factory, was caught in the act while attempting to sell

classified information on the Turkish-made MPT-76 and MP-5 rifles for financial gain, thanks to a joint operation by intelligence and law enforcement authorities (Aslan, 2021).

The MKEK attack can be viewed as a typical example of the Intellectual Property (IP) theft of a core military asset. The MPT-76 was a step toward sovereign infantry performance; the loss of its blueprints would have been tantamount to the annulment of several years of research and development. This case serves as a cautionary example that top officials who may have actual physical access to blueprints are the main targets of foreign interests. It stresses the importance of physical and digital tagging of sensitive documents, whereby any unauthorized copying or export of technical drawings automatically initiates intelligence alerts.

To prevent espionage activities in Türkiye's defense sector, multidimensional and systematic measures must be implemented. First, it is crucial to subject defense industry personnel to regular security vetting, not only upon hiring but periodically throughout their tenure. In addition, providing employees with awareness training on espionage, cybersecurity, and social engineering will contribute to the early detection of potential threats. From an institutional perspective, monitoring employee interactions with foreign representatives or companies, within defined ethical and security frameworks, acts as a protective measure against espionage. Moreover, establishing confidential reporting channels for suspicious activities will strengthen the security culture within organizations. In terms of physical security, enhancing biometric verification systems, camera surveillance, and visitor restrictions will be effective in safeguarding critical facilities. Finally, developing information-sharing mechanisms with friendly and allied countries and conducting joint counterintelligence exercises at the international level will enable the construction of a stronger and more resilient defense sector capable of withstanding espionage threats targeting Türkiye's defense industry.

6. Discussion

This article aimed to review the effects of the emergence of a new defense sector on reshaping the magnitude, tactics, and strategic impact of espionage, using a single-case study of Türkiye. The Türkiye example shows that both the rapid development of defense industrial potential and the increase in strategic independence occur in tandem with greater exposure to espionage, which, in turn, confirms the main assumption that technological development and vulnerability are structurally interdependent.

The analyzed cases show that the targeting of Türkiye's defense industry by espionage attacks is not occasional or isolated but systematic and dynamic. Foreign intelligence agencies and other actors have an interest in sectors that yield high strategic and economic payoffs. Success in UAVs, guided missile systems, and electronic warfare technologies has made Türkiye's defense industry a key component in both regional and global power rivalry, elevating it beyond a supportive sector within the country. This has turned Turkish defense organizations into easy targets of cyberattacks, insider groups, and black markets for illicit information, demonstrating that the

emergence of an advanced defense industry inevitably attracts the unwanted attention of hostile intelligence agencies.

Theoretically, the results highlight the distinction between lawful competitive intelligence and unlawful industrial espionage. Although competitive intelligence relies on open-source information, the Turkish examples show a shift toward covert acquisition methods, particularly cyber-based espionage and insider-led leaks. The Dropping Elephant cyberattack is a prime example of one of the most asymmetric forms of modern industrial espionage: low-cost phishing was used against high-value military research and development targets. This demonstrates how cyber espionage amplifies the magnitude and effects of intelligence operations, allowing the exfiltration of large volumes of data with limited risk of detection.

Meanwhile, the insider cases discussed (the SSB leak, the data sales via Telegram, and networks linked to terrorist organizations) demonstrate that insider threats remain the most effective and hard-to-trace means of espionage. These incidents show that the intersection of ideological interests, financial rewards, and institutional privileges can result in severe security breaches. Contrary to the notion that high levels of technological protection alone are sufficient, the Turkish experience makes it clear that human vulnerabilities remain central to espionage relationships, even in highly securitized contexts such as the defense industry.

It can be inferred that espionage should not be perceived solely as a foreign policy threat but as an outcome of defense industrialization. Defense industries are complex systems where technological innovation, foreign policy ambitions, and national security concerns converge. The Türkiye example indicates that espionage operates on tactical, operational, and strategic levels: tactically by stealing data and conducting phishing attacks, operationally through insider networks and supply chain vulnerabilities, and strategically by compromising long-term competitiveness and credibility in global defense markets. In this respect, the results contribute to theoretical discussions by showing that espionage is not merely a reaction to state actions but also an integral component of the power dynamics within the international system.

7. Conclusion

The findings of this study demonstrate that espionage directed at emerging defense industries is both multifaceted and adaptive, encompassing traditional human-driven approaches as well as sophisticated cyber operations. Türkiye's defense sector, while achieving remarkable growth and technological independence, has simultaneously become a primary target for hostile intelligence activities. The examined cases reveal that espionage threats not only jeopardize specific projects or companies but also have the potential to undermine national security strategies and disrupt broader defense planning.

One of the most striking observations is how espionage exploits vulnerabilities within digital infrastructures, insider networks, and global supply chains. The capacity to infiltrate systems through

cyber intrusions, manipulate individuals with access to sensitive data, or extract information via covert corporate channels underscores the evolving and persistent nature of these threats. Moreover, the interconnectedness of modern defense industries with international partners amplifies the risk, as external dependencies may create additional avenues for exploitation.

These dynamics suggest that espionage can influence not only the operational resilience of a defense industry but also the perception of its reliability in the global arena. In this sense, espionage becomes both a tactical tool and a strategic weapon, capable of shaping industrial competitiveness and international alignments. The challenge for Türkiye, and for other rising defense powers, is therefore to construct a robust counterespionage framework that integrates technological safeguards, institutional resilience, and human awareness.

The central implication is that a more rapidly advancing defense industry creates a greater incentive for adversaries to penetrate it. Future research should explore how counterespionage practices can be institutionalized to limit the risk of insider threats, mitigate vulnerabilities in supply chains, and neutralize cyber intrusions before they escalate. Developing systematic methods to safeguard knowledge, intellectual property, and operational autonomy is not only a matter of industrial security but also a prerequisite for sustaining strategic independence in an increasingly contested global environment.

References

Arctic Wolf. (2025) Dropping Elephant APT Group Targets Turkish Defense Industry with New Campaign and Capabilities: LOLBAS, VLC Player, and Encrypted Shellcode. Arctic Wolf, July 23. https://arcticwolf.com/resources/blog/dropping-elephant-apt-group-targets-turkish-defense-industry/ (Accessed: 03.09.2025).

Aslan, D. (2021) Turkish Counterespionage Ops Shield Dissidents. Daily Sabah, October 26. https://www.dailysabah.com/politics/news-analysis/turkish-counterespionage-ops-shield-dissidents (Accessed: 05.09.2025).

Bastian, J. (2024) Turkey: An Emerging Global Arms Exporter. Growing Competitiveness and Strategic Recalibration of the Turkish Defence Industry. Stiftung Wissenschaft und Politik (SWP) SWP Comment No. 6/2024. Berlin. https://doi.org/10.18449/2024C06

Baysal, B. (2025) Evaluating the Advances and Challenges in Turkey's Defence Industry: A Comparative Analysis. Southeast European and Black Sea Studies 25(1), 31–52.

Bekdil, B. E. (2021) Turkey Detains 26 Suspects Over Defense Industry Espionage Charges. Defense News, March 30. https://www.defensenews.com/industry/2021/03/30/turkey-detains-26-suspects-over-defense-industry-espionage-charges/ (Accessed: 05.09.2025).

Benny, D. J. (2014) Industrial Espionage: Developing a Counterespionage Program. Boca Raton: Taylor & Francis Group.

Donelli, F. (2022) UAVs and Beyond: Security and Defence Sector at the Core of Turkey's Strategy in Africa. Stiftung Wissenschaft und Politik (SWP). https://doi.org/10.18449/2022MTA-PB02 (Accessed: 05.09.2025).

Dyami Analysts (2024) Risks of Chinese Espionage in Europe's Defense Industry. Dyami Security Intelligence, June 28. https://www.dyami.services/post/risks-of-chinese-espionage-in-europe-s-defense-industry (Accessed: 05.09.2025).

Egeli, S. et al. (2024) From Client to Competitor: The Rise of Turkiye's Defence Industry. International Institute for Strategic Studies. http://dx.doi.org/10.13140/RG.2.2.15922.00962.

Farley, R. (2016) Intellectual Property, Cyber Espionage, and Military Diffusion. Global Security and Intelligence Studies 1(2), 2–20.

Hamilton, P. (1967) *Espionage and Subversion in an Industrial Society: An Examination and Philosophy of Defence for Management*. London: Routledge.

Hou, T. & Wang, V. (2020) Industrial Espionage: A Systematic Literature Review. Computers & Security, no. 98, 1–12.

Hürriyet Daily News (2022) MİT Eyes 'Counterespionage Briefings' on Turkish Defense Industry. May 9. https://www.hurriyetdailynews.com/mit-eyes-counterespionage-briefings-on-turkish-defense-industry-173651 (Accessed: 06.09.2025).

ISI Defense (2024) Spotting Corporate Espionage. November 8. https://isidefense.com/blog/spotting-corporate-espionage (Accessed: 06.09.2025).

Ivezic, M. (2025) Quantum Tech and Espionage: What Every Researcher Must Know. Postquantum, August 1. https://postquantum.com/post-quantum/espionage-quantum/ (Accessed: 08.09.2025).

Newsroom (2025) Türkiye Arrests 7 in Defense Industry Espionage Case Linked to Telegram. Türkiye Today, September 23. https://www.turkiyetoday.com/nation/turkiye-arrests-7-in-defense-industry-espionage-case-linked-to-telegram-3207368 (Accessed: 08.09.2025).

Özer, A. İ. A. (2019) The Rise of the Turkish Defense Industry. Ankara: SETA Publications.

Philips, P. J. & Pohl, G. (2025) Industrial Espionage: Window of Opportunity. Information Security Journal: A Global Perspective 34(2), 143–155.

Sibley, K. A. S. (1999) Soviet Industrial Espionage Against American Military Technology and the US Response. Intelligence and National Security 14(2), 94–123.

Taşdan, C. (2021) Savunma Sanayi Projelerini Yabancı Firmalara Aktaranlara Operasyon: 6 Gözaltı. Anadolu Ajansı, April 27. https://www.aa.com.tr/tr/turkiye/savunma-sanayi-projelerini-yabanci-firmalara-aktaranlara-operasyon-6-gozalti/2221930# (Accessed: 10.09.2025).

Tromblay, D. E. (2017) Protecting Partners or Preserving Fiefdoms? How to Reform Counterintelligence Outreach to Industry. Information Technology & Innovation Foundation. https://itif.org/publications/2017/10/16/protecting-partners-or-preserving-fiefdoms-how-reform-counterintelligence/ (Accessed: 09.09.2025).

Unaran, I. (2025) Turkish Defense Industry Faces Cyber Espionage Threat. Data Flow X, August 5. https://www.dataflowx.com/post/turkish-defense-industry-faces-cyber-espionage-threat (Accessed: 08.09.2025).

Weissbrodt, D. (2013) Cyber-Conflict, Cyber-Crime, and Cyber-Espionage. Minnesota Journal of International Law 22(2), 347–387.

Yeşiltaş, M. (2020) Deciphering Turkey's Assertive Military and Defense Strategy: Objectives, Pillars, and Implications. Insight Turkey 22(3), 89–114.

Zatlin, J. R. (2008) Out of Sight: Industrial Espionage, Ocular Authority and East German Communism, 1965–1989. Contemporary European History 17(1), 45–71.