

# DIŞ KAYNAK KULLANIMI YOLUYLA İSTİHBARAT TEMİNİ VE ÖZEL İSTİHBARAT ŞİRKETLERİNİN YAPISAL ANALİZİ-YÜKLENİCİ ŞİRKETLER

**Kadir Murat Altıntaş\***

## Öz

*Son yarım yüzyılda, ekonomik ve siyasi küreselleşme, bilişim ve iletişim teknolojisindeki gelişmeler, internetin insan yaşamına entegrasyonu (nesnelerin interneti), insanlığı çok farklı bir dünya ile karşı karşıya bırakmıştır. Bu dönemde, kamu istihbarat otoriteleri tarafından tespit edilen terör saldırılarına ilişkin değişen temel algılar, ticari kuruluşların istihbarat toplama konusunda ön plana çıkmasına neden olmuştur. Özel İstihbarat Şirketlerinin (ÖİŞ) günümüzde resmi istihbarat kurumlarının dikkate değer bir tamamlayıcısı haline geldiği, kolaylıkla iddia edilebilir. Tamamen ticari amaçlar için çalışan ve teorik olarak standart bir ticari kuruluştan herhangi bir farkı bulunmayan ÖİŞ, siyasi karar vericiler için alternatif istihbarat temin kaynağı haline dönüşmüştür. Günümüzde ÖİŞ, çok uluslu şirketlerin karmaşık küresel ticari faaliyetlerini analiz etmenin yanı sıra, dünyanın çeşitli bölgelerindeki ekonomik ve siyasi olaylar hakkında jeopolitik danışmanlık hizmeti de sunmaktadır. Ancak, tüm dünyada çok çeşitli alanlarda hizmet veren ÖİŞ'nin faaliyet sınırları ve görev kapsamı arasında kavramsal olarak bir netlik bulunmamaktadır. Bu çalışmanın temel amacı, ÖİŞ'lerinin diğer post-modern askeri temelli taahhüt şirketlerine göre yapısal farklılıklarını vurgulamak ve misyonları çerçevesinde görev kapsamının genel kabul görece bir biçimde daha açık tanımlanması ve sınıflandırılması için bir model oluşturmaktır. Sonuç olarak, bu eğilimin işlevselliği ve nihai başarısı ÖİŞ'lerinin görev, yetki ve sorumluluklarının netleştirilmesine ve resmi istihbarat teşkilatları ile uyumlu çalışabilecekleri yasal altyapının oluşturulmasına bağlıdır.*

**Anahtar Kelimeler:** İstihbarat, Vekil Organizasyonlar, Özel İstihbarat Şirketleri

\* Prof. Dr., Bolu Abant İzzet Baysal Üniversitesi, Uygulamalı Bilimler Fakültesi, kadiralintas@ibu.edu.tr, <https://orcid.org/0000-0001-8422-1086>.

Bu makaleye atıf için: Altıntaş, Kadir Murat. (2022). Dış Kaynak Kullanımı Yoluyla İstihbarat Temini ve Özel İstihbarat Şirketlerinin Yapısal Analizi-Yüklenici Şirketler, SDE Akademi Dergisi, 2(6), 14-37

# OUTSOURCING INTELLIGENCE AND CONCEPTUAL MODELLING OF PRIVATE INTELLIGENCE AGENCIES- CONTRACTORS

**Kadir Murat Altıntaş**

## **Abstract**

*Transforming perceptions of terrorist attacks identified by public intelligence authorities in the last half century have led commercial entities to burst into prominence for intelligence gathering. It can easily be asserted that some of Private Intelligence Agencies (PIAs) have evolved into a remarkable complement of official intelligence institutions. Operating with purely trading motives and hypothetically no distinction from a standard commercial enterprise, PIAs are organized as an alternative intelligence gathering institutions for political decision makers. Today, PIAs provide also geopolitical consultancy about regional economic and political events at some parts of the world as well as analysing the complex global commercial activities of multinational corporations. However, there is a conceptual uncertainty between the operational limitations and task scope of PIAs that serve in a wide range of activities all around the world. The primary aim of this study is to emphasize the conceptual differences of PIAs compared to other post-modern military based contracting companies and to model for a better classification of task scope within the framework of their mission among themselves. Consequently, the functionality and ultimate success of this tendency largely depends on the clarification of the tasks, authorities and responsibilities of PIAs and the establishment of legal infrastructure in which they can work in harmony with the official intelligence agencies.*

**Keywords:** *Intelligence, Proxy Organizations, Private Intelligence Agencies*

## **Introduction**

In the 21st century, economic security of nations has become the crucial part of national security for both developed and developing countries. Therefore, within the constraints of today's hybrid warfare concept, in other words in a global environment where asymmetric struggles are common between countries, it is a necessity for nations to take comprehensive precautions to protect their economic, political, technological and military gains from external threats. In this framework, security concept (both economic and political) has become one of the primary issues for almost every institution and every nation, regardless of their status.

The digital revolution that created the information age recently and the innovations observed in communication technologies have deeply affected national economies as well as commercial entities' global operations, revealing the need for an advanced organizational structure. At this point, we come across the concept of 'outsourcing', which has been widely accepted in management literature for many years and is used by global businesses on a large scale. Developed countries have been particularly affected by this management tendency, and almost all service areas, including basic public services, were completely transferred to private enterprises.

In today's world, where the demand for information constitutes the main necessity for security of both countries and companies, the absolute realization of national and investment safety depends largely on the production of sufficient and satisfactory intelligence for relevant parties. At this point, there has been a remarkable evolution that took place, namely the end of Cold War, as a result of the dissolution of the Union of Soviet Socialist Republics. A surplus of highly skilled labour force emerged from the leading intelligence services of eastern Bloc countries. At the end, the period resulted in several employment opportunities of that qualified workforce at multinational corporations which have become giants in the world economy.

In recent years, the quantitative and qualitative boundaries of service-delivery differentiation between public and private institutions have al-

most been blurred, and it is observed that a new security and intelligence approach has come to the fore, especially in western sophisticated societies. Inadequate communication and information sharing between intelligence communities of countries, as well as the ineffective competition among the members of intelligence communities, resulted in a wide spread security problems for countries. Due to the ineffective closeness between public intelligence agencies and insufficient political decision-making mechanism in recent years, the quantity and quality of the products (intelligence) has declined gradually.

Besides, the diminishing motivation of labour force by various reasons (exhaustion, lack of satisfying financial opportunities, strict bureaucratic practices, etc.) has also decreased their management performance in intelligence production process. For all these reasons, the delegation of intelligence production process to private contractors, under the supervision and administration of public intelligence agencies and political authorities has been heavily involved in the international agenda of security professionals. In some cases where the intelligence is not satisfactory in terms of quality and quantity or inadequate intelligence sharing between military and intelligence authorities, obtaining intelligence from a third party can be a more effective solution for strategic decision-making processes of political authorities. Today, the vast majority of private contractors established in this business have been implemented by people who have a significant experience in intelligence production at public institutions recently.

Due to all these recently experienced prominent incidents, the threat perceptions of developed countries and global companies have seriously been evolved and this has resulted in private contractors coming to the forefront of intelligence gathering. However, there is not adequate clearness regarding the task scope and operational limitations of PIAs activities. In other words, the mission and responsibility of PIAs both in literature and practice are indefinite and interpenetrated among each other. The main reason for this is that PIAs operate on many different issues and their assumed tasks with other contracting firms are sometimes overlap-

ping. Also, the '2018 UN Human Rights Special Procedures, Mercenaries and Special Military/Security Companies' regulation is not sufficiently explanatory regarding the authorities and responsibilities of contracting firms accompanied with the lack of any international legal enforcement.

In this study, data and information regarding the activities of PIAs, which are still operating on a global scale, were analysed. In this sense, the data and information belonging to 49 PIAs, which have a significant market share in this service segment and whose data can be accessed, were utilized. The primary aim of this study is to emphasize the conceptual differences of PIAs compared to other post-modern military based contracting firms and to model for a better clarification of the task scope of PIAs among themselves as well as their mission. The study concludes with the structural transformation of PIAs into a new identity emphasizing their conceptual differences from other contracting firms and provides a fundamental model for the activities of PIAs for the first time in the literature.

## **1. Outsourcing of Intelligence within the Framework of Hybrid Warfare**

The main consequence observed in the power struggles among countries is that conventional battles (which require enormous expenditure and destructive consequences) lost its priority and was replaced with a brand-new warfare concept called 'Hybrid War - Gerasimov Concept'. While the tendency eradicated the sharp frontier between war and peace gradually, it also removes the virtual borders of military and civilian people. Besides, due to the hesitation of participating intelligence with private contractors, local intelligence authorities are generally reluctant to share information with society in developing countries. As a result, these countries had to take a more limited initiative and indicate an uncertain approach for transferring intelligence services to private industry.

While before Cold War, intelligence services were carried out within the framework of one-dimensional and standard patterns, since then it has

gained a multi-dimensional and global characteristic. For this reason, the perception of threat in terms of traditional security policies has completely transformed and the need for a new intelligence settlement has begun to emerge. In a world, where there are no economic, political and geographical constraints, 'proxy battles' come to the fore and a new intelligence gathering approach has needed to arise recently. Due to the loss of availability of traditional intelligence service supply, the necessity of recruiting qualified personnel with unusual qualifications has come up, especially for services such as translation, interrogation or local staff engagement.

In 2006, there were over 6000 private contract linguists supporting various operations in the Global War on Terrorism at a total annual cost exceeding US\$ 250 million (Voelz 2009). Today, close to a million contractors hold a security clearance in the United States. This is a quarter of all cleared personnel, and more than the total population of the District of Columbia, where most major federal government institutions are located. Tens of thousands of contractors contribute to core intelligence functions like collection and operations, analysis and production, and even mission management (Office of the Director of National Intelligence 2015). Diversifying of global intelligence gathering caused official intelligence agencies face with a workload that they could not easily cope with. Within this framework, official intelligence agencies particularly from western developed countries outsourced some of their specialized services to the private contractors. Finally, this period resulted about the privatization of certain part of intelligence gathering activities and this circumstance gained momentum especially after the first Gulf War.

Aside from the September 11 initiator of religious extremists prepared to use violence, intelligence is now aligned to other societal shifts, of globalization, the growth of technology, and securitization across a range of government policies and programs. Tracing these changes in intelligence concepts since 1945, it is possible to identify the trajectory towards public-private partnerships, where 'intelligence is now a big business' (Hermann 1996). Besides, a rigid approach to intelligence exchanges that does not

recognize the role and contributions of the private sector, leads to far too many incomplete pictures (Palmer 2013).

In the twenty-first century, more than ever before, government intelligence agencies collaborate with the private sector to counter diverse security threats. Speaking at an industry conference, an official from Office of the Director of National Intelligence recognised how essential the private sector has become to the national intelligence effort, stating: ‘We can’t spy if we can’t buy.’ (Everett 2007). In the last decade, the US intelligence community has disbursed hundreds of billions of dollars to acquire goods and services from the industry and intensified its efforts to liaise with the private sector. The extent to which American spies interact with the private sector is unparalleled and comes as a shock to outsiders, yet it is a severely underrepresented subject in the literature on intelligence (Van Puywelde 2019).

The 2018 report, prepared by the United Nations Human Rights Council through a working group established to examine human rights violations, briefly covers private enterprises established in security and intelligence issues; defined as ‘legal entities providing military and/or security services on a balancing basis by natural and/or legal people. However, there are many diverse groups within the private military industry: mercenaries, private security companies, private detective companies, private intelligence companies, or private military companies (United Nations 2018). The amount of intelligence that is shared in the private sector and between major multi-national companies that own and operate major civil infrastructures is substantial. In their day-to-day operating environments, there are clear pressures for any intelligence product to be valuable to the respective company in terms of its reputation, its profits, protection from industrial/economic espionage, and the potential to expand its business into new areas. These corporate priorities create an ongoing business demand for targeted intelligence product that is integrated into strategic and operational decision making (Palmer 2013:5).

Private intelligence sector teams can also support strategic decision-making. For example, if an energy company is exploring new market entry

in Nigeria, executives might be concerned about corruption, kidnapping, pipeline tapping, piracy, and Boko Haram. The intelligence assessment would examine what threats would translate into real risks for the company, considering the company's prospective vulnerabilities and the likely impact. Boko Haram would pose a credible threat to operations planned in Borno state, but not the Niger Delta, where more pressing concerns would be pipeline tapping, kidnapping, and piracy. New market entry support can also identify political instability and reputational concerns prior to investment. While some intelligence teams focus on strategic opportunity intelligence, most activity in the private sector intelligence field continues to be concentrated on risk and security (Campbell 2011). In the case of private sector intelligence, consumers of private intelligence—corporate executives, travellers, or any other employees being protected or supported by intelligence—are unlikely to have sufficient familiarity with intelligence tradecraft to accurately assess the quality of the service. A key driver of professionalization is to establish baselines and standards to overcome the asymmetry of information between experts and clients (Morrow 2022).

Technological advances and the concomitant universal reliance on such innovations to communicate and to conduct personal and business transactions electronically have generated an unprecedented number of data points about individuals who use email, surf the web, speak via telephone, wire money, bank and travel commercially, and transact business via the Internet. All of the information about particular electronic transactions is possessed in large measure by private firms involved in commerce, finance, and telecommunications. With high-powered computers and increasingly sophisticated software, analysts can mine these stores of data and detect particularly significant patterns of behaviour, including activities ostensibly indicative of terrorist planning (Michaels 2008). Entrusting part of the intelligence production to private organization, has both advantages and disadvantages. Intelligence provided by the private sector is important in order to manage information overload and provide timely and sound intelligence. On the other hand, the quality of the intelligence produced might vary. The private sector might be unaware (for reasons that have to do with



national security) or unable to understand, what an intelligence consumer is looking for. In addition, the private sector is concentrating on providing short term analysis and not long term assessments (Liaropoulos 2006).

## **2. The Need for Private Intelligence Agencies (Contractors)**

Private Intelligence Agencies are one of the advanced global organizations that emerged within the framework of a new security approach observed in Post-Modern societies. They are non-state comprehensive units that provide strategic intelligence support, supply especially technology-based services, perform covert/ clandestine HUMINT-Human Intelligence operations, and present investment consultancy services to public intelligence agencies as well as multinational corporations. Though, they act purely with standard commercial motives, PIAs carry out intelligence gathering activities independently from any other organizations.

Acting purely with commercial motives and no difference from a standard business, PIAs are organized as a substitute to traditional intelligence agencies, in other words creating an alternative intelligence source with a different content for political decision makers. Besides, PIAs provide geoeconomically consultancy for regional economic and political developments to multinational corporations in a global environment as well as analysing their overseas commercial operations. In addition, PIAs can analyse economic/financial investment trends on a global scale and provide strategic analysis support to minimize the possible risks and uncertainties for decision-making mechanisms of multinational corporations. For instance, they provide services which plan to invest in the emerging markets of Africa, Eastern Europe and East Asia, in other words geographies that are not easy to comprehend and contain serious investment risks.

Though most experts accepted the reality of a fundamental transformation in the practice of warfare, few saw that a parallel revolution was occurring in the intelligence world, even though this specific field of national security was undergoing similar challenges and change. The 'Revolution

in Intelligence Affairs' in the 1990s and early 2000s actually occurred and its affects have become increasingly evident. This 'intelligence revolution' resulted from a combination of changes in international politics, information technologies, and socio-political context (Denece 2014).

There was a need for commercial augmentation especially for carrying out of non-traditional military overseas operations where there wasn't adequate supply of labour force. In order to support this diverse range of operations, the government was forced to return to commercial augmentation, particularly for specialized intelligence tasks such as translation, interrogations, debriefings, and document and media exploitation in obscure target languages where the military services and US Intelligence Community (IC) could not maintain sufficient levels of trained personnel (Voelz 2009).

IC historically has relied on contractors to help meet national security goals, but that reliance deepened after the September 11, 2001 attacks. A decade after the attacks, the IC remains heavily reliant on contractors, so this hearing was held to discuss reasons for this continued reliance such as: (1) specialized technical capability deficiencies within the government workforce; (2) cultural, military, or linguistic expertise deficiencies within the government workforce; and (3) greater flexibility with contractors that allows government to quickly fill and remove positions (Allen 2011).

On 14 May 2007 a senior procurement executive from the Office of the Director of National Intelligence gave a presentation to an intelligence industry conference in Colorado convened by the Defence Intelligence Agency (DIA). Her presentation, 'Procuring the Future', was posted on the DIA website, but later modified and subsequently removed. In it, she revealed that the proportion of the US intelligence budget spent on private contractors is 70 per cent. By removing the scale from a table on intelligence expenditures but not the underlying figures, she also revealed that the amount the United States spends on such contractors is US\$ 42 billion, out of an implied total intelligence budget of US\$60 billion for the 2005 financial year (Chesterman 2008).

Some of the main obstacles to export trade that have been clearly identified are related to the business community's dearth of knowledge in key areas necessary for international operations. Too many businesses have little or no knowledge of foreign markets and have not developed the pertinent skills needed to assess the relative competitiveness of other companies in the same sector, find potential new suppliers, understand the relevant regulations in new markets, or detect new business opportunities. Good business intelligence also grows out of a sophisticated understanding of user/consumer needs. They therefore have a greater need for intelligence training that empowers them to define requirements, gain an understanding their environments, and carry out intelligence reporting than larger organizations (Matey 2013).

Private firms offer a wide range of operational support to government intelligence agencies, such as target tracking and monitoring through satellites, human sources development in foreign countries, interrogation of persons of interest, and enhanced interrogations (such as in Guantanamo Bay prison). Many private intelligence firms help the government to identify terrorists on a worldwide scale by providing lists containing names, locations, group affiliations, and potential violent activities in which suspected terrorists are involved. As for technical support, government intelligence agencies rely on private contractors to provide hardware and software solutions to technological challenges. For instance, corporations provide technical support through development of customized information technology, information sharing architecture design, elaboration of encryption algorithms, and global network platforms (Lemieux 2018).

A historical view of private intelligence suggests that in the modern era corporations and government agencies have always been linked in some way and will continue to be. However, the type and number of private actors participating in national intelligence have varied considerably. Some place the peak for private intelligence in the United States in the first decade of the twenty-first century. Others see only superficial abatement of the trend towards intelligence contracting and outsourcing in recent

years. Despite the questions that these conditions pose for the way that intelligence is understood, organized, and conducted, private intelligence remains poorly researched (Hansen 2014). Similar to the early study of private security, scholarly work explaining and understanding private intelligence has emphasized disagreements far more than it has produced consensus knowledge. This is due, in part, to institutional secrecy and the absence of empirical examples of private intelligence practice (Bean 2015). Despite claims of private intelligence providing goods and services more efficiently and effectively, the empirical evidence suggests that the outsourcing of intelligence is marked by inefficiency, corruption and criminality. These problems are not produced occasionally or depend on personalities; rather, the problems are structural in nature, such as the likelihood of a revolving door, public intelligence's need to outsource "dirty work", etc. (Butt 2010).

### **3. The Conceptual Modelling of PIAs**

Today, PIAs continues to collect data and information for global interests of multinational corporations in various regions of the world, and also they have been widely contracted by public intelligence agencies for long years. Though PIAs do not have any official linkage with other organizations or governments, it gives them to be a more flexibility when serving in much wider regions of the world. Also, they carry on business in an economic and political environment that is not limited by certain international/national legislations. The other side of the issue in terms of national security is industrial espionage attacks, which have experienced frequently in sophisticated industry segments of developed countries. It is one of the most serious threats to the economic security of industrialized nations. Governments and corporations which do not want to be in evidence of an economic/industrial espionage attempts, almost cooperate with private intelligence agencies to avoid from various legal sanctions. Hereby, they were engaged with 'proxy activities' to carry out certain special activities

by private contractors. In addition, PIAs also provide counterintelligence services to multinational corporations as part of their service portfolio.

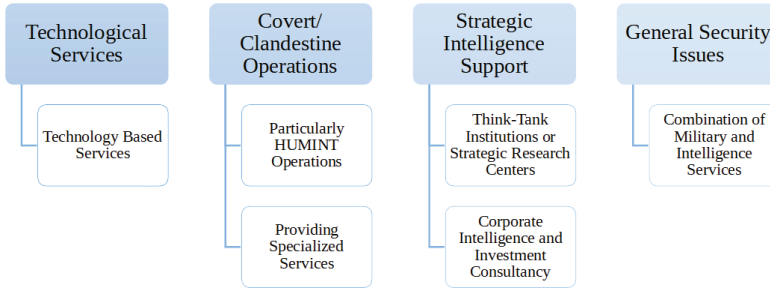
Since the legal status of employees of PIAs was interpreted as a freelance individual (independent contractor), the legal responsibility of activities which carried out in terms of international/national laws must be undertaken only by the individual directly. On the other hand, various illegal incidents have generally been legally pursued against international laws. Nevertheless, satisfactory results have not been achieved to protect the rights of the victims.

Although there is not any significant distinction about the mission and responsibility of PIAs among each other, the possible differences come up with the undertaken contracts they perform. Conceptual modelling of PIAs has been structured for the first time in the literature by the Author, within the framework of their main task scope and operational limitations of their activities. From this point of view, the general functions of PIAs are discussed in the form of basically at four main titles and six different sub-headings:

1. PIAs which specialize in technology-based services,
2. PIAs which specialize in covert/ clandestine operations,
3. PIAs which specialize in strategic intelligence support,
4. PIAs which specialize in general security issues.

In line with the general classification stated above, it is possible to sum up the area of specialization and task scope of the PIAs into six different sub-headings. Displaying various samples of PIA's from all around the world currently, it is possible to simplify the categorization of service segment more perceptible and manageable. In the figure below (Figure 1), there is a detailed modelling of the mission and responsibility of PIAs within the relevant operational limitations:

**Figure 1: The Conceptual Modelling of PIAs**



**1. Technology-Based Services:** PIAs which specialize in providing services that require extensive technological infrastructure, such as SIGINT-Signal Intelligence or IMINT-Image Intelligence. In order to support the global operations of military forces or intelligence agencies, some of PIAs, which undertake the responsibility for the execution of high-tech operations, use their technological know-how in areas where governments hesitate to invest in or do not want to allocate adequate resources to these leading technologies (such as surveillance satellites, geospatial intelligence, signal analysis, etc.). Leidos-Lockheed Martin, Science Application International Corporation-SAIC, ASI Group (integration of technical tracking hardware into flight systems), The Steele-NSO Group (producer of the famous spyware Pegasus), BAE Systems (software for geospatial intelligence analysis, information technology solutions, integrated warfare intelligence systems, analytic solutions for operations, applied intelligence), Pluribus (simplifying increasingly complex cloud network operations by securing and automating networking across distributed cloud environments), CSRA (information technology services for US national security agencies) are the primary examples of this type of PIAs.

**2. Particularly HUMINT Operations:** In line with the content of assigned contracts, these types of PIAs provide services, such as recruiting local collaborators (agents or informants or staffed resources), translation services in various regional languages, counterintelligence and counterespionage services, target tracking and conducting surveillance or private investigations. Major examples of this type of PIAs are Nortrop Grum-

man, GK Sierra, Kroll, Booz Allen Hamilton, International Intelligence Limited, Jane's Information Group (providing technical intelligence or intelligence for all kinds of threats to countries or defence industries).

**3. Providing Specialized Services:** Services such as special interrogation and prison management (CACI International-USA), industrial espionage and surveillance (Surefire Intelligence-USA), explosive destruction or search/rescue (KBR-Halliburton), perception management and analysis, social media manipulation campaigns or rival research by artificial intelligence projects, strategic disinformation, fake news production or cyber security (Archimedes Group-Israel, Psy-Group-Israel, Cambridge Analytica-UK., Black Cube-Israel, Esoteric Ltd.-UK, DarkMatter-UAE, Everbridge NC4-US), critical infrastructure protection in challenging operational regions of the world-oil or natural gas risk management, protective security and crisis management (Olive Group-UAE) are generally performed by this type of PIAs.

**4. Think-Tank Institutions or Strategic Research Centres:** They are special organizations (which are generally financed from public resources or to whom they are organically affiliated) that provide strategic data and information support, as well as political, social and economic analysis and offer policy options. Such organizations are highly functional project development entities in terms of managing and strategically directing the social perception and provide valuable recommendations to decision makers in the process of transforming information into policies and strategies. Remarkable examples are US Air Force-related Rand Corporation, CIA-related Stratfor, MI6-related Chatham House, Mossad-related Jinsa etc. They also support the international vision of multinational companies by providing comprehensive geopolitical risk assessments as well as assisting access to alternative sources by making use of their global network. In fact, they have generally assumed responsibility mostly at the 'analysis' phase of strategic intelligence gathering process (Geos Groupe-France).

**5. Corporate Intelligence and Investment Consultancy:** Believing that geography is never a restrictive variable, certain PIAs offer their clients

not only strategic intelligence support but also services such as commercial intelligence, competitive intelligence and international investment consultancy. In addition, they provide services to their international clients such as intelligence gathering training support, executing strategic investment analysis, improving public relations strategies and international market research with open-source intelligence. Primary examples of such Agencies are Hakluyt & Company, Abraxas Corp., Frontier Horizons, Fusion GPS, Smith Brandon International, Diligence, Global Strategies Group-KPMG, Economic Intelligence Unit, Control Risks Group-Control Risks, GPW-Grayson, Pender and Wordsworth, Global Source (competitive intelligence support and risk analysis for international financial markets), and Oxford Analytica can be given.

**6. Combination of Military and Intelligence Services:** PIAs produce general security solutions for their international customers (multinational companies, NGOs, states, non-state actors, etc.) with a focus on both military and intelligence activities such as domestic/external tactical combat operations, providing operational intelligence, and providing military training at various levels. Some of the spectacular Agencies all around the world are Academi-Constellis, Aegis, Northbridge Services Group, Triple Canopy-Constellis, Asia Security Group, Dyncorp, iJET (an intelligence-driven risk management Agency and solution provider that helps multinational corporations and government agencies survive and thrive in the face of global threats) and International Regional Security Agency (information gathering and intelligence production for fundamentalist terrorist organizations).

Today, American Central Intelligence Agency (CIA) still maintains commercial relations with many companies operating in the private sector directly, and purchases not only services but also products especially in technology-oriented matters, through outsourcing. Even these companies, in a sense, work as R&D departments of the CIA. The major companies that develop products in this sense are: personal investigation-InQtel, video surveillance-3VR, criminal tracking-CrimeDex, digital evidence col-



lection-Adaptx, DNA/RNA and protein analysis-Biomatrica, large-scale data storage-Cloudera, WiFi sensors-GainSpan, foldable satellite dishes-GATR, low-energy radio products-Ember, Virtual-Holographic simulation-Infinite Z, portable cameras on clothing- Looxcie, electricity-saving software-MiserWare, monitoring other people's computer-OpenSpan, health check with human body contact-Seventh Sense, detecting inaudible sounds-Sonitus Medical Inc., handheld super-powered radars-Spotter RF, handheld X-Ray-Walleye that shows inside solid objects, information gathering from social media-Visible Technologies (Hickley, 2012).

## **Conclusion**

There are so many different kinds of private contractors (such as private military companies, mercenaries, security companies, detective companies, private intelligence agencies) within the system regarding the conversion of security services to the private enterprises in the world. The execution of a certain part of intelligence gathering, which is one of the most strategic public service areas, by means of PIAs, have been successfully performed by western developed countries for about a quarter of a century. In a global environment, where the opportunities and capabilities of PIAs are widely used by sovereign countries, private contractors are used as an alternative to official armed forces or intelligence agencies in order to achieve the leading countries' strategic goals in various geographies of the world.

When the PIAs' activities have analysed in recent years, it was seen that they have operated on many different matters within the scope of intelligence gathering. But there is not any clear differentiation among their mission and task boundaries. In other words, there is a conceptual uncertainty between the operational limitations and task scope of PIAs that serve in a wide range of activities all around the world.

In this study, at first, to distinguish PIAs from other private contractors, the fundamental description and task scope has been determined with the help of various samples that are still in practice. In addition, to make

up the shortage about the inadequacy of PIAs' conceptual modelling research in literature, they are structurally classified into four main headings and six different subheadings in terms of their functionality; PIAs which are specialized in technology-based services, covert operations, strategic information support and general security issues. In addition, these agencies are categorized into other six sub-headings: Technology-Based Services, Particularly HUMINT Operations, Providing Specialized Services, Think-Tank Institution or Strategic Research Centres, Corporate Intelligence and Investment Consultancy, and Combination of Military and Intelligence Services. It is estimated that this conceptual categorization will fulfil the ambiguous gap between PIAs in itself and will also clarify the theoretical basis of PIAs with different contractors.

The remarkable and growing trend of outsourcing intelligence services to private enterprises, which has been observed in the world recently, indicates that private contractors will also be favoured and draw interest also in developing countries. The functionality and ultimate success of this tendency largely depends on the clarification of the tasks, authorities and responsibilities of PIAs and the establishment of legal infrastructure in which they can work in harmony with the official intelligence agencies.

## References

Allen, Charles E. (2011). Intelligence Community Contractors: Are We Striking the Right Balance? Oversight of Government Management, the Federal Workforce, the District of Columbia Subcommittee, Activities of the Committee on Homeland Security and Governmental Affairs. [https://irp.fas.org/congress/2011\\_hr/contractors.pdf](https://irp.fas.org/congress/2011_hr/contractors.pdf).

Bean, Hamilton. (2015). Privatizing Intelligence. Routledge Handbook of Private Security Studies, 1st, Edition, 79-89.

Butt, Stephen. Outsourcing Intelligence: The Relationship Between the state and Private Intelligence in Post-Apartheid South Africa, (2010), (17.04.2022). [https://open.uct.ac.za/bitstream/handle/11427/3796/thesis\\_hsf\\_2010\\_butt\\_stephen.pdf;sequence=1](https://open.uct.ac.za/bitstream/handle/11427/3796/thesis_hsf_2010_butt_stephen.pdf;sequence=1),

Campbell, Stephen. (2011). H. A. Survey of the U.S. Market for Intelligence Education, in; International Journal of Intelligence and Counter-Intelligence, no. 2, March 7, 307–337.

Chesterman, Simon . (2008). We Can't Spy, If We Can't Buy!: The Privatization of Intelligence and the Limits of Outsourcing Inherently Governmental Functions, in; European Journal of International Law, Volume 19, Issue 5, November (2008), 1055–1074. Tim Shorrock, Spies for Hire-The Secret World of Intelligence Outsourcing, (New York 2008), Simon and Schuster.

Denécé, Eric. The Revolution in Intelligence Affairs: 1989-2003, in; International Journal of Intelligence and Counterintelligence, (2014), 27(1): 36.

Everett, Terri. (2007). Procuring the Future: 21st Century Acquisition, Office of the Director of National Intelligence, presentation given at conference organised by the DIA, (Colorado), Boulder.

Hansen, Morten. (2014). Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the US Intelligence Community, in; Intelligence and National Security, 29 (1): 58–81.

Hermann, Michael. (1996). *Intelligence Power in Peace and War*, (Cambridge), Cambridge University Press.

Hickley, Walt. 25 Cutting Edge Firms Funded By The CIA, (2012), (09.08.2021) <https://www.businessinsider.com/25-cutting-edge-companies-funded-by-the-central-intelligence-agency-2012-8#biomatrica-works-with-preserving-biological-materials-4>.

Lemieux, Frederic.(2018).The Rise of the Private Intelligence Sector, in; *Intelligence and State Surveillance in Modern Societies*, Emerald Publishing Limited, (Bingley), 191-205. <https://doi.org/10.1108/978-1-78769-171-120181009>.

Liaropoulos, Andrew. A. (2006). "(R)evolution in Intelligence Affairs? In Research of a New Paradigm". RIEAS, Research Paper No.100.

Matey, Gustavo Diaz.(2013).The Use of Intelligence in the Private Sector, in; *International Journal of Intelligence and Counterintelligence*. Routledge Taylor & Francis Group, 26: 276.

Michaels, Jon D. (2008).All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror, in; *California Law Review*. Vol. 96, No. 4, 901-966.

Morrow, Maria A. Robson. (2022). Private sector intelligence: on the long path of professionalization, in; *Intelligence and National Security*. Taylor & Francis Group, DOI: 10.1080/02684527.2022.2029099 p. 6.

Office of the Director of National Intelligence, National Counterintelligence and Security Center, 2015 Report on Security Clearance Determinations, 28 June 2016, p. 5; Office of the Director of National Intelligence, FY 2013 Congressional Budget Justification, Vol. I: National Intelligence Program, February 2012, p. 69.

Palmer, Mick. (2013). Benefits, Challenges, and Pitfalls of Private Intelligence, in; *Salus Journal* Volume: 2, Issue: 1, 3-7.

United Nations Human Rights Special Procedures, Mercenarism and Private Military and Security Companies. Special Rapporteurs, (2018),

(16.09.2021). [www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Members.aspx](http://www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Members.aspx).

Van Puywelve, Damien. (2019). *Outsourcing US Intelligence Contractors and Government Accountability*, Edinburgh University Press Ltd. (Edinburg, UK).

Voelz, Glenn. (2009). *Contractors and Intelligence: The Private Sector in the Intelligence*, in; *International Journal of Intelligence and Counter-Intelligence*, 22, 586-613.

## **Genişletilmiş Özet**

Geçtiğimiz elli yıllık bir dönem süresince, ekonomik ve siyasi küreselleşme, bilişim ve iletişim teknolojisindeki gelişmeler, bilgiye ulaşımın kolaylaşması, internetin insan yaşamına dahil edilmesi (nesnelerin interneti), insanlığı çok farklı bir dünya ile karşı karşıya bırakmıştır. Bu dönüşüm, bireyleri olduğu kadar toplumları da derinden etkilemiş ve üretimden tüketime, sağlıktan eğitime ya da güvenlikten istihbarata kadar, toplumlar tarafından daha önce hiç tecrübe edilmemiş ama daha önce tecrübe edilmemiş farklı bir çevrenin ortaya çıkmasına neden olmuştur. Bu değişim/dönüşüm süreci ise, toplumların aralarındaki rekabet ve mücadele süreçlerini de kavramsal boyutta derinden etkilemiş ve adeta savaş/barış kavramlarına ilişkin temel tanımlamaların, yeniden gözden geçirilmelerini gündeme getirmiştir. Toplumların güvenlik ve istihbarat algılarının temelden değiştiği bu dönemde, “devlet dışı aktörler” olarak ifade edebileceğimiz düzensiz kuvvetlerin de savaş denklemi içerisine entegre edildiği görülmektedir.

Öte yandan, aynı dönemde bilgi çağını yaratan dijital devrim ve iletişim teknolojilerinde gözlenen yenilikler, ulusal ekonomilerin yanı sıra ticari kuruluşların küresel operasyonlarını da derinden etkilemiş, gelişmiş bir organizasyonel yapıya olan ihtiyacı ortaya çıkarmıştır. Bu noktada, yönetim literatüründe uzun yıllardır yaygın olarak kabul gören ve küresel işletmeler tarafından büyük ölçüde kullanılan ‘dış kaynak kullanımı’ kavramını ile karşılaşmaktayız. Bu yönetim eğiliminden özellikle gelişmiş ülkeler daha fazla etkilenmiş ve bazı temel kamu hizmetleri de dahil olmak üzere, neredeyse tüm hizmet alanları tamamen özel teşebbüslere devredilmiştir.

Kamu ve özel kuruluşlar arasındaki hizmet-sunum farklılığının nicel ve nitel sınırları adeta belirsiz olup, özellikle batılı gelişmiş toplumlarda yeni bir güvenlik ve istihbarat yaklaşımının öne çıktığı görülmektedir. Ülkelerin istihbarat teşkilatları arasında yetersiz iletişim ve bilgi paylaşımının yanı sıra istihbarat teşkilatları mensupları arasındaki sınırlı rekabet, ülkeler için ciddi bir güvenlik sorununa yol açmaktadır. Kamu istihbarat teşkilatları arasındaki işbirliğinin istenilen düzeyde olmaması, siyasi karar alıcılara

arz edilen ürünlerin (istihbarat) miktar ve kalite bakımından giderek düşüşüne neden olmaktadır.

Ayrıca, kamu istihbarat teşkilatlarındaki mevcut işgücünün çeşitli nedenlerle (mesleki tükenme, maddi imkanların yetersiz kalması, katı bürokratik uygulamalar vb.) azalan motivasyonu da, istihbarat üretim sürecindeki yönetim performanslarını düşürmüştür. Tüm bu nedenlerle, istihbarat üretim sürecinin kamu istihbarat teşkilatları ve siyasi otoritelerin gözetimi ve idaresi altında, özel yüklenici şirketlere devredilmesi, uluslararası güvenlik ve istihbarat sektörünün gündemine dahil olmuştur. İstihbaratın nitelik ve nicelik olarak tatmin edici olmadığı ya da askeri ve istihbarat makamları arasında istihbarat paylaşımının yetersiz kaldığı durumlarda, siyasi yöneticilerin stratejik karar verme süreçlerinde, üçüncü bir taraftan istihbarat temini etkili bir çözüm olabilmektedir. Bu anlamda, günümüzde faaliyette bulunan özel istihbarat şirketlerinin büyük çoğunluğu, genelde kamu kurumlarında daha önceden istihbarat üretiminde deneyime sahip kişiler tarafından yönetilmektedir.

Yukarıda kısaca ifade edilen dikkat çekici gelişmeler nedeniyle, gelişmiş ülkelerin ve küresel şirketlerin tehdit algıları ciddi bir şekilde değişmiş ve bu durum özel istihbarat şirketlerinin istihbarat toplamada ön plana çıkmasına neden olmuştur. Ancak, ÖİŞ'nin görev kapsamı ve faaliyet sınırları konusunda, yeterli açıklık bulunmamaktadır. Diğer bir deyişle, ÖİŞ'nin hem alanyazında, hem de uygulamada, görev ve sorumlulukları belirsizdir ya da üst üste çakışmaktadır. Bu durumun nedeni, ÖİŞ'nin birçok farklı konuda faaliyet göstermesi ve diğer yüklenici firmalar ile üstlendikleri görevlerin bazen örtüşmesidir. Öte yandan, '2018 BM İnsan Hakları Özel Usulleri, Paralı Askerler ve Özel Askeri/Güvenlik Şirketleri' yönetmeliği, yüklenici firmalarının yetki ve sorumluluklarına ilişkin yeterince açıklayıcı olmaması yanında, uluslararası herhangi bir yasal yaptırımın da bulunmaması, uygulamada ortaya çıkan karmaşıklığın asıl sebebinin oluşturmaktadır.

Bu çalışmada, öncelikle küresel ölçekte faaliyet gösteren ÖİŞ'nin görev, yetki ve sorumluluklarına ilişkin veri ve bilgiler analiz edilmiştir. Bu kap-

samda, özel istihbarat hizmeti sunan şirketler arasından, kayda değer bir pazar payına sahip olan ve kaynak temini mümkün olan toplam 49 ÖİŞ'ne ait veri ve bilgilerden yararlanılmıştır. Bu çalışmanın esas amacı, diğer post-modern askeri tabanlı yüklenici firmalara kıyasla, ÖİŞ'nin kavramsal farklılıklarını vurgulamak ve ÖİŞ'nin kendi aralarındaki görev, yetki ve sorumluluk kapsamının daha iyi açıklığa kavuşturulması için alternative bir model oluşturmaktır. Bu çalışmada, alanyazında ilk kez ÖİŞ'nin faaliyetlerinin kapsamı çerçevesinde temel bir model sunulmaktadır.

Bu anlamda, alanyazındaki kavramsal modelleme araştırmalarının yetersizliği hususundaki eksikleri gidermek amacıyla, ÖİŞ yapısal olarak dört ana başlık ve işlevsellik açısından altı farklı alt başlıkta sınıflandırılmıştır; Teknoloji Tabanlı Hizmetler, Gizli Operasyonlar, Stratejik Bilgi Desteği ve Genel Güvenlik konularında uzmanlaşmış ÖİŞ'leri. Ayrıca bu şirketler, altı alt başlıkta sınıflandırılmıştır; HUMINT Operasyonları, Teknolojiye Dayalı Hizmetler, İhtisas Hizmetleri Sunma, Think-Tank Kuruluşu veya Stratejik Araştırma Merkezleri, Kurumsal İstihbarat ve Yatırım Danışmanlığı, Askeri ve İstihbarat Hizmetlerinin Birleşimi. Bu kavramsal sınıflandırmanın ÖİŞ'leri arasındaki görev, yetki ve sorumluluğa ilişkin belirsizliği ortadan kaldıracağı ve ÖİŞ'lerinin teorik temellerini netleştireceği tahmin edilmektedir.

Dünyada istihbarat hizmetlerinin özel teşebbüslere devri yönünde gözlenen dikkat çekici eğilim, gelişmekte olan ülkelerde de özel istihbarat şirketlerinin ilgi göreceğini göstermektedir. Bu eğilimin işlevselliği ve nihai başarısı, büyük ölçüde ÖİŞ'lerinin görev, yetki ve sorumluluklarının netleştirilmesine ve resmi istihbarat teşkilatları ile uyumlu çalışabilecekleri hukuki bir altyapının oluşturulmasına bağlıdır.