Avrasya İncelemeleri Dergisi
Journal of Eurasian Inquiries

İSTANBUL UNIVERSITY PRESS

Avrasya İncelemeleri Dergisi - Journal of Eurasian Inquiries 13, 1 (2024): 37-60
DOI: 10.26650/jes.2024.1389815
Araştırma Makalesi / *Research Article*

Rekabet İstihbaratı ve Endüstriyel Casusluk: Ulusal Güvenlik Perspektifinden Bir Değerlendirme

Competitive Intelligencea Industrial Espionage: a National Security Perspective

Ali Gök[1], Taner Akçacı[2]

[1]**Sorumlu yazar/Corresponding author:**
Ali Gök (Doç. Dr.),
Gaziantep Üniversitesi, İslahiye İktisadi ve İdari Bilimler Fakültesi, Kamu Yönetimi Bölümü, Gaziantep, Türkiye
E-posta: aligok86@gmail.com
ORCID: 0000-0002-0734-459X

[2]**Taner Akçacı (Prof. Dr.),**
Gaziantep Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası Ticaret ve Lojistik Bölümü, Gaziantep, Türkiye
E-posta: akcaci@gantep.edu.tr
ORCID: 0000-0002-5343-0894

Başvuru/Submitted: 12.11.2023
Revizyon Talebi/Revision Requested: 28.12.2023
Son Revizyon/Last Revision Received: 01.01.2024
Kabul/Accepted: 05.01.2024

Atıf/Citation: Gök, A., Akçacı, T. Competitive Intelligencea Industrial Espionage: a National Security Perspective. *Avrasya İncelemeleri Dergisi - Journal of Eurasian Inquiries 13, 2* (2024): 37-60. https://doi.org/10.26650/jes.2024.1389815

ÖZ

Günümüzde işletmeler ve uluslar, yeni teknolojiler, bilgiler ve yenilikler elde etmeye çalışan aktörler tarafından yasa dışı yöntemlerle her zamankinden daha fazla hedef alınmaktadırlar. Özellikle yüksek teknoloji, askeri uygulamalar ve biyoteknoloji alanında, devletler ile koordineli şekilde faaliyet gösteren işletmeler çok sayıda değerli ticari sırlara ve en son teknolojilere sahip olmaları nedeniyle endüstriyel casusluk için özellikle çekici bir hedeftir. Bu varlıklar, rakipler için milyarlarca dolar değerinde olabilir ve bunların çalınması rakip/düşman devletlere önemli bir askeri ya da ekonomik avantaj sağlayabilir. Bu nedenle bazı devletlerin ya da devlet dışı aktörlerin, gizli iş ayrıntılarını ve teknik bilgileri hedef alması, devletler tarafından ulusal güvenlik kapsamında değerlendirilmekte ve rekabet istihbaratından daha çok özellikle bu tür endüstriyel casusluk faaliyetlerine karşı koyma, istihbarat örgütlerinde "kontrespiyonaj" kapsamına alınmaktadır. Bu çalışma, öncelikle endüstriyel casusluğun kapsamını derinlemesine inceleyerek bu faaliyetlerin çok yönlü boyutlarını ortaya çıkarmayı ve bunun tespiti ve önlenmesine yönelik istihbarat örgütleri ile işletmelerin stratejilerini örnekler üzerinden keşfetmeyi amaçlamaktadır. Ayrıca çalışma, endüstriyel casusluk ve rekabet istihbaratının, ekonomik ve ulusal güvenlik kaygıları ile arasındaki karmaşık etkileşimi araştırmakta ve endüstriyel casusluğa karşı, istihbarat örgütleri ile işletmelerin kurması gereken hassas dengeye ışık tutmaktadır.

Anahtar Kelimeler: Rekabet İstihbaratı, Endüstriyel Casusluk, Ulusal Güvenlik, Ekonomik Güvenlik, İstihbarat Örgütleri, Rusya, Çin

ABSTRACT

Nowadays, companies and nations are being targeted more than ever illegally by actors trying to obtain new technologies, information, and innovations. Companies operating in coordination with governments, particularly in the fields of high technology, military applications, and biotechnology, are particularly attractive targets for industrial espionage because they possess many valuable trade secrets and the latest technologies. These assets can be worth billions of dollars to opponents, and their theft can provide a significant military and economic advantage to rival or enemy states. Therefore, the targeting of confidential business details and technical information by some states or

nonstate actors is considered by states within the scope of national security. In particular, countering such industrial espionage activities, rather than competitive intelligence, is included in the scope of counterespionage in intelligence organizations. This study aimed to examine the scope of industrial espionage in depth, reveal the multifaceted dimensions of these activities, and explore the strategies of intelligence organizations and companies to detect and prevent this through examples. In addition, this study explores the complex interaction between industrial espionage and competitive intelligence with economic and national security concerns and sheds light on the delicate balance that intelligence organizations and companies should establish to decouple from industrial espionage.
Keywords: Competitive Intelligence, Industrial Espionage, National Security, Economic Security, Intelligence Organizations, Russia, China

EXTENDED ABSTRACT

Espionage has entered a new stage of development in the business world at the end of the Cold War and has affected globalization and technology. At this point, the widespread use of cyberspace brings several security risks and threats to companies. The main problem in defining how companies will be affected by these threats is that, in many cases, companies cannot detect incidents or disclose them because of commercial concerns. Companies operating in coordination with governments, particularly in high technology, military applications, and biotechnology, are particularly attractive targets for industrial espionage because they possess many valuable trade secrets and cutting-edge technologies. These assets could be worth billions of dollars to adversaries, and their theft could give rival or enemy states a significant military or economic advantage. In recent years, industrial espionage activities have significantly increased. This is partly due to technology competition with the United States, with China emerging as a major player in the global defense market. China has been accused of systematic industrial espionage against the United States and other Western countries to accelerate its military modernization. In addition to China, Russia, Iran, and North Korea are alleged to be performing these activities. Unauthorized access to confidential data, proprietary technologies, and intellectual property threatens not only the national security of states but also global security. In this context, understanding the dynamics of industrial espionage is becoming increasingly important for policymakers, defense agencies, and researchers engaged in developing national defense capabilities in an increasingly interconnected world. Thus, the targeting of confidential business details and technical information by some states or nonstate actors is considered within the scope of national security by states. In particular, countering such industrial espionage activities, instead of competitive intelligence, is included in the scope of counterespionage in intelligence organizations. As a result, business and commercial objectives are becoming increasingly important for intelligence organizations alongside military or political objectives. In this framework, although competitive intelligence and industrial espionage constitute the subject matter of corporate governance and security studies, they are addressed from the perspective of security studies. In this context, why have intelligence

organizations had to intervene in the fight against such activities, which are a matter of the private sphere and primarily concern the corporate security of companies? In other words, why should intelligence organizations treat industrial espionage activities a security concern? In the fields of high technology, military applications, and biotechnology, the possibility that information, ideas, and trade secrets that should remain confidential could fall into the hands of rival or enemy states is perceived by states as a threat to economic security. From this viewpoint, the corporate security of companies operating in these fields is becoming increasingly important for states; therefore, the scope of the duties and powers of intelligence agencies is expanding to include the corporate security of companies against industrial espionage. Given the inability of national and international legislation to provide a comprehensive legal framework for industrial espionage, the role of intelligence agencies in ensuring corporate security is becoming increasingly important. Although many companies have corporate security departments, few companies have well-planned counterintelligence functions, given the increasing scale of industrial espionage activities. In addition, the fact that intelligence agencies resort to industrial espionage to provide military, economic, and technological advantages to their countries makes the already-weak corporate security departments of companies even more threatening. In addition to the aforementioned situations, the widespread use of cyberspace and the easy transfer of information/data across distances and national borders have resulted in various security risks and threats for companies. At this point, the detection of industrial espionage activities in cyberspace and the development of counter strategies also challenge corporate security departments. Thus, companies must seek support from their country's intelligence agencies to ensure their corporate security. Currently, intelligence agencies and corporations are working together to prevent the threat of critical information and technological innovations being intercepted by other actors. However, this effort must be further developed, particularly by introducing common innovative approaches to detect cyber-attacks and other forms of industrial espionage. Ultimately, states and international organizations/institutions should ensure that severe sanctions and penalties are included in national and international legislation to increase deterrence against industrial espionage.

Giriş

Rekabet istihbaratı ve endüstriyel casusluk faaliyetleri, iş dünyasında uzun zamandır tartışılan konular olmakla birlikte, 21. yüzyılda özellikle teknolojik ilerlemenin etkisiyle iş sırlarını elde etme araçlarının gelişmesi, bu faaliyetleri sadece işletmelerin değil, devletlerin de güvenliklerini ilgilendiren konular haline getirmektedir. Rekabet istihbaratı ve endüstriyel casusluk benzer süreçlere sahip olmalarına rağmen, endüstriyel casusluk, işletmelerden veya kuruluşlardan ticari sırların veya diğer gizli bilgilerin çalınmasını ifade ederken, rekabet istihbaratı, karar vericilere yardımcı olmak ve kuruluşa rekabet avantajı sağlamak amacıyla rakip işletmeler hakkında açık ve yasal kaynaklardan bilgi toplama, işleme ve analiz etme sürecini ifade etmektedir.

Casusluğun iş dünyasında, Soğuk Savaş'ın sona ermesiyle birlikte küreselleşme ve teknolojinin etkisiyle, yeni bir gelişim aşamasına girdiği değerlendirilmektedir. Bu noktada siber alanın kullanımının yaygınlaşması işletmeler için çok çeşitli güvenlik risk ve tehditleri de beraberinde getirmektedir. Söz konusu tehditlerden, işletmelerin nasıl etkileneceğini tanımlamadaki temel sorun, çoğu durumda işletmelerin olayları tespit edememesi veya ticari kaygılardan dolayı açıklayamamasıdır. Özellikle yüksek teknoloji, askeri uygulamalar ve biyoteknoloji alanında, devletler ile koordineli şekilde faaliyet gösteren işletmeler çok sayıda değerli ticari sırlara ve en son teknolojilere sahip olmaları nedeniyle endüstriyel casusluk için özellikle çekici bir hedeftir. Bu varlıklar, rakipler için milyarlarca dolar değerinde olabilir ve bunların çalınması rakip/düşman devletlere önemli bir askeri ya da ekonomik avantaj sağlayabilir. Son yıllarda endüstriyel casusluk faaliyetlerinde önemli bir artış yaşanmaktadır. Bu kısmen, küresel savunma pazarında önemli bir aktör olarak ortaya çıkan Çin'in, ABD ile teknoloji rekabetinden kaynaklanmaktadır. Çin, kendi askeri modernizasyonunu hızlandırmak amacıyla ABD ve diğer Batılı ülkelere karşı sistematik endüstriyel casusluk faaliyetleri yürütmekle suçlanmaktadır. Ayrıca Çin'in yanı sıra Rusya, İran ve Kuzey Kore'nin de bu faaliyetleri yürüttüğü iddia edilmektedir.

Gizli verilere, özel teknolojilere ve fikri mülkiyete yetkisiz erişim, yalnızca devletlerin ulusal güvenliklerini tehdit etmekle kalmamakta, aynı zamanda küresel güvenliğe de tehdit oluşturmaktadır. Bu bağlamda, giderek birbirine bağlanan bir dünyada ulusal savunma yeteneklerini geliştirmekle uğraşan politika yapıcılar, savunma kurumları ve araştırmacılar için endüstriyel casusluğun dinamiklerini anlamak giderek daha önemli hale gelmektedir. Bu nedenle bazı devletlerin ya da devlet dışı aktörlerin, gizli iş ayrıntılarını ve teknik bilgileri hedef alması, devletler tarafından ulusal güvenlik kapsamında değerlendirilmekte ve rekabet istihbaratından daha çok özellikle bu tür endüstriyel casusluk faaliyetlerine karşı koyma, istihbarat örgütlerinde kontrespiyonaj kapsamına alınmaktadır. Sonuç olarak günümüz dünyasında, iş ve ticari hedefler, istihbarat örgütleri için askeri veya siyasi hedeflerin yanında giderek daha önemli hale gelmektedir. Bu kapsamda, bir özel alan konusu olan ve temelde öncelikle işletmelerin kurumsal güvenliğini ilgilendiren bu tür faaliyetlerle mücadeleye istihbarat örgütleri neden

müdahil olmak durumunda kalmışlardır? Bir başka ifadeyle istihbarat örgütleri endüstriyel casusluk faaliyetlerini neden bir güvenlik endişesi olarak ele almalıdır? soruları çalışmanın temel problemini oluşturmuştur. Bu çerçevede rekabet istihbaratı ve endüstriyel casusluk, kurumsal yönetim ve güvenlik çalışmalarının konusunu oluşturmakla birlikte, bu çalışmada güvenlik çalışmaları perspektifinden ele alınacaktır.

Çalışmada ilk bölümde, rekabet istihbaratı ve endüstriyel casusluk faaliyetlerinin benzerlikleri ve farklılıkları üzerine tartışmalara değinilecek olup, akabinde ikinci bölümde endüstriyel casusluğun oluşturduğu tehditler, ulusal güvenlik açısından analiz edilecektir. Son bölümde ise, endüstriyel casusluğa yönelik tarihsel vakalar, güncel zorluklar ve bu çerçevede devletlerin ortaya koyduğu eğilimler üzerinden incelenecektir.

Rekabet İstihbaratı ve Endüstriyel Casusluk: Kavramsal Benzerlik Üzerine Tartışmalar

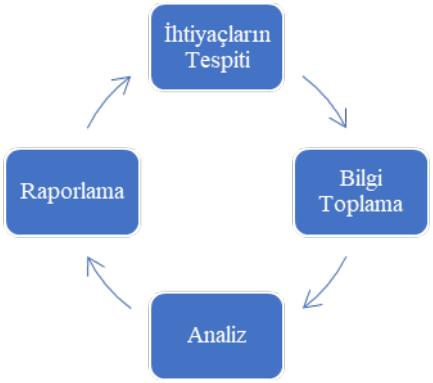
Rekabet istihbaratı ve endüstriyel casusluk kavramları farklı anlamlar taşımalarına rağmen, hem literatürde zaman zaman birbirleri yerine kullanılabilmekte hem de endüstriyel casusluğun bir takım hukuki sonuçlar doğurması sebebiyle, bu tür casusluk faaliyetleri inkâr edilebilirliği sağlayabilmek adına rekabet istihbaratı kapsamında değerlendirilebilmektedir. Bu anlam karmaşasının giderilebilmesi açısından öncelikle her iki kavramın tanımının yapılması ve ikisi arasındaki farkların belirtilmesi gerekmektedir.

Rekabet istihbaratının ve endüstriyel casusluğun ekonomik güvenliğin konusunu oluşturduğu yönünde genel bir kanı bulunmaktadır. Devletler tarafından ekonomik güvenlik, bir ülkenin kendisini savunma yeteneğini doğrudan etkileyen ticaret ve yatırım yönlerine atıfta bulunabilir. Örneğin, silah veya ilgili teknolojiyi edinme yeteneği, askeri lojistik tedarikinin güvenilirliği veya silahlarda teknolojik avantaj elde eden düşmanların neden olduğu tehdit algısı bunlardan bazılarıdır.[1] Rekabet istihbaratı ve endüstriyel casusluk da söz konusu yetenek ve ihtiyaçların temin edilmesini sağlayan bir süreç olarak görülebilmektedir.

Rekabet istihbaratı ve endüstriyel casusluk süreci aşağıda Şekil 1'de belirtildiği gibi genellikle dört aşamaya ayrılmaktadır. Bunlar: 1-ihtiyaçların tespiti, 2- bilgi toplama, 3- analiz ve 4- raporlama(yayma) olarak sıralanabilir. Tüm bu süreç genellikle istihbarat döngüsü ya da istihbarat çarkı olarak adlandırılır.[2]

1 Vincent Cable, "What is International Economic Security?", *International Affairs*, 71/2, 1995, 306.

2 Dirk Vriens, "The Role of Information and Communication Technology in Competitive Intelligence", *Idea Group Inc*.,2004. Erişim 07 Eylül 2023, https://repository.ubn.ru.nl/handle/2066/139628.



Şekil. 1. İstihbarat Çarkı

Şekil 1'de belirtilen temel istihbarat döngüsünü ve bunun sonucunda ortaya çıkan analiz kullanılarak işletmelere yönelik bilgiler -örneğin alt yüklenici firmalar, tedarikçiler, iş yapılan ekipman imalatçıları ve müşteri bilgileri- öğrenilebilmektedir.[3]

Rekabet istihbaratı ve endüstriyel casusluk benzer süreçlere sahip olmalarına rağmen, rekabet istihbaratı, karar vericilere yardımcı olmak ve kuruluşa rekabet avantajı sağlamak amacıyla iç, dış veya rekabet ortamından bilgi toplama, işleme ve analiz etme sürecidir.[4] Bir başka ifadeyle bilgilerin açık ve yasal bir şekilde toplanmasına rekabet istihbaratı adı verilmektedir. Rekabet istihbaratı, rekabet avantajı kazanmak amacıyla rakipler, tedarikçiler, müşteriler ve belirli bir sektör hakkında bilgi toplamak için organize bir şekilde koordineli bir çabadır.[5] Herhangi bir rakip analizinin temel amacı, işletmenizin rekabet ettiği kategorinin dinamiklerini anlamaktır. Kısaca, işletmenizin en yakın rakiplerine göre konumunu belirleyebilmektir.[6]

Günümüzde işletmelerin faaliyet gösterdiği belirsiz ve dinamik ortam göz önüne alındığında, işletme sınırları dışındaki pazar yerinin analiz edilmesi zorunlu hale gelmektedir. İşletmelerin bu ortamda devamlılıklarını sağlayabilmek için mevcut ve gelecekteki rekabet ortamlarını değerlendirmesi gerekmektedir. Rekabet istihbaratı bu ihtiyaç ekseninde, işletmelere gelecekte neler olacağına dair öngörüler sağlayarak, becerilerini ve bilgilerini geliştirmelerine ve rakiplerinden daha hazırlıklı olmalarına yardımcı olur. Bu nedenle, bir işletmenin planlarını ve kararlarını etkileyebilecek bilgilerin toplanması, analiz edilmesi ve yönetilmesi için sistematik ve etik bir süreç olarak tanımlandığı şekliyle rekabet istihbaratı, işletmeler için stratejik bir rol oynar.[7]

3 Carl Roper, *Trade Secret Theft Industrial Espionage, and the China Threat*, (Boca Raton: Taylor & Francis Group,2014), 101.

4 Hamid Tahmasebifard, "The Role of Competitive Intelligence and Its Sub-Types on Achieving Market Performance", *Cogent Business & Management*, 5/1, 2018, 1-16.

5 Douglas Bernhardt, *Competitive Intelligence: How to Acquire and Use Corporate Intelligence and Counter-Intelligence*, (Edinburgh: Prentice Hall, 2003), 87.

6 Higgs, Bronwyn, "Industrial espionage: The Legal Way", *Marketing Magazine*, 76, 2005.

7 Francesca Labonia, "The Strategic Role of Competitive Intelligence: A Study of The Brazilian Market", 2018, 15. Erişim 10 Eylül 2023, https://repositorio.usp.br/directbitstream/b7e691e0-ca07-4bb3-9a88-5966e8754b46/FRANCESCA%20LABONIA%20-%20PRO18.pdf; Oana – Antonia Colibasanu, "Between Intelligence and Espionage in the Contemporary Business Environment", *Ekonomika a Management Prague University of Economics and Business*, 4, 2008, 2.

Rekabet istihbaratının odak noktası, bilgilerin kaynaklardan yasal ve etik olarak toplanmasıdır.[8] Ancak endüstriyel casuslukta bu durum farklılaşmaktadır. Endüstriyel casusluk, rakipler hakkındaki özel bilgilerin toplanmasıdır.[9] Ticarette ağırlık, bilgi ve teknolojiye dayalı ürünlere geçmiştir. Bu durumun fikri mülkiyeti, dünya ticaretinin daha büyük bir bileşeni haline getirmektedir. Bu çerçevede fikri mülkiyet kapsamına giren özel bilgiler, bir işletmenin giderek en değerli varlığı olarak kabul edilmektedir.[10]

Endüstriyel casusluk, genellikle hırsızlık, rüşvet, şantaj gibi yasa dışı eylemlerden ve bazen de gözetim gibi gizli operasyonlardan oluşur. Endüstriyel casusluğun temel amacı, bir rakibi sabote etmektir.[11] Rekabet avantajı kazanmaya çalışmak çoğu iş araştırmasının doğasında vardır. Ancak endüstriyel casusluğa izin verilmez ve hoş karşılanmaz. Özetle; rekabet istihbaratı, endüstriyel casusluğun daha hafif bir "kötülüğü" olarak kabul edilir.[12]

Aslında bu iki kavram arasındaki fark, kullanılan kaynaklara ve bilgi edinmek için kullanılan araçlara bağlı olarak çok ince olabilir. Ancak yasal olarak elde edilen bilgiler, bir kuruluş için yasa dışı kaynaklardan elde edilen veriler kadar zararlı (veya yararlı) da olabilir.[13]

Rekabet istihbaratında kullanılmak istenilen verilerin çoğu kamusal alanda bulunabilir. Bunlar; çoğunlukla iş rehberleri, gazete makaleleri, ticari basın vb. gibi geleneksel açık kaynaklardır. Mağaza ziyaretleri, rastgele fiyat kontrolleri ve ticari fuarlara katılım gibi yöntemler de önemli miktarda bilgi sağlayabilir.[14]

Son zamanlarda, ağ tabanlı sistemlerin ortaya çıkışı ise bilgiye ulaşımı daha da kolaylaştırmıştır. Özellikle çeşitli ilgi gruplarına sahip insanlara çevrimiçi iletişim kurma olanağı sunan birçok farklı web sitesi ve sosyal medya platformunun ortaya çıkışı ve bu insanların bilgi yaymaya istekli olması, rekabet istihbaratı açısından işletmelere önemli katkı sağlamaktadır. Bu faaliyet alanına sosyal medya istihbaratı adı verilmektedir.[15] Bir başka ifadeyle değişen iletişim ortamı sosyal medyayı, "sosyal casusluk" yoluyla rakip firmalar

8 Bernhardt, *Competitive Intelligence: How to Acquire and Use Corporate Intelligence and Counter-Intelligence,* 87; Phillip C. Wright, Géraldine Roy, "Industrial Espionage and Competitive Intelligence: One You Do; One You Do Not", *Journal of Workplace Learning*, 11/2, 1999, 54; Miroslava Brazdilova, "Competitive Intelligence and Competitive Abilities of Enterprises", *Ekonomika A Management*, 2005.

9 Temitope Toriola, "Industrial Espionage or Competitive Intelligence: Two Sides of the Same Coin", *Purdue University*, 2011, 3. Erişim 12 Eylül 2023, https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2011-10-report.pdf.

10 Bernhardt, *Competitive Intelligence: How to Acquire and Use Corporate Intelligence and Counter-Intelligence,* 87

11 Toriola, "Industrial Espionage or Competitive Intelligence: Two Sides of the Same Coin", 3.

12 Sergey Vladimirovich Shaitura, Konstantin Vasilievich Ordov, Irina Georgievna Lesnichaya, Yulia Dmitrievna Romanova, Seda Seiranovna Khachaturova, "Services and Mechanisms of Competitive Intelligence on The Internet", *ESPACIOS*, 39/45, 2018, 1-7.

13 Wright, Roy, "Industrial Espionage and Competitive Intelligence: One You Do; One You Do Not", 54.

14 Bronwyn, "Industrial espionage: The Legal Way", 77; Tsanko V. Ivanov, "Competitive Intelligence and Counterintelligence – Modern Tools For Generating Proactive Corporate Security", *International Scientific Journal Security & Future*, 1/1, 2017, 7.

15 Shaitura, Ordov, Lesnichaya, Romanova, Khachaturova, "Services and Mechanisms of Competitive Intelligence on The Internet"

hakkında rekabet istihbaratı elde etme kaynağı haline getirmektedir.[16]

Sonuç olarak rekabet istihbaratı ile endüstriyel casusluk faaliyetlerinin birbirinden ayrılmasını sağlayan toplanan verilerin kaynağıdır. Bu kaynaklar, "beyaz bilgi, gri bilgi ve siyah bilgi" olmak üzere üç türdür. Söz konusu türler detaylı açıklanacak olursa:[17]

- Birçoğu yukarıda listelenen çeşitli veri kaynaklarında bulunabilen açık kaynak bilgileri "beyaz" olarak kategorileşmektedir;
- Ticari fuarlar ve rakipler tarafından sıklıkla göz ardı edilen diğer yayınlar gibi özel alan verilerini içeren gri bilgiler; aynı zamanda kısıtlı bilgi olarak da adlandırılabilir;
- Siyah bilgiler etik kuralların ötesinde toplanabilir; bilgisayar korsanlığı, kurumsal casusluk, telefon dinleme vb. yoluyla yasa dışı olarak elde edilen bilgilerdir.

Ancak "kaynaklar arasındaki çizgi nasıl çizilebilir?" sorusu problem teşkil etmektedir. Kaynaklar arasındaki farkın tanımlanması o kadar basit olmamakla birlikte, aslında siyah ile beyaz arasında bir "gri alan" vardır ve siyahın griye, beyazın da griye karıştığı yer genellikle kişisel muhakeme ve karar meselesidir. Genel bir görüş birliği ya da evrensel olarak kabul edilmiş bir standart yoktur.[18] Sonuç olarak, beyaz ve gri bilgiler rekabet istihbaratı kapsamında değerlendirilebilirken, siyah bilgilerin elde edilmesi endüstriyel casusluk kapsamında değerlendirilebilmektedir.

Pek çok kişi, endüstriyel casuslukta bir çalışanın bir tür özel veriyi bir evrak çantası içinde işyerinden gizlice çıkardığını ve daha sonra rakibin temsilcisiyle bir kafede buluştuğunu ve çaldığı bilgileri belirli bir miktar somut değer karşılığında teslim ettiğini düşünür.[19] Bu durum kısmen doğru olmakla birlikte, endüstriyel casusluk, bir işletmenin gizli veya korunan bilgilerinin bir rakip veya yabancı ülke tarafından kullanılmak üzere çalınmasıdır. Bu sebeple rekabet istihbaratından farklı olarak korunan bilgileri, ticari sırları, müşteri listelerini ve diğer kamuya açık olmayan bilgileri içerebilir.[20]

Reid, endüstriyel casusluğu bir tür "hile"ye benzetmektedir ve bu tür casusluk, devlet destekli yabancı bir kuruluşun araştırma ve geliştirme (Ar-Ge) aşamasını atlamasına (veya en azından süreci hızlandırmasına) ve doğrudan işletmeye geçmesine yardımcı olmak amacıyla bir işletmeden ticari sırların çalınmasıdır. Reid'a göre, casusluğu "hile" yapan şey, bir yabancı ülkenin ticari sırlarından mahrum kalması, diğerinin ise rakibinden faydalanmasıdır.[21]

Bu açıdan bazı devletlerin, rekabet dengesini kendi lehlerine çevirmek için endüstriyel casusluğu kullandıkları görülmektedir. Bu çerçevede yenilikleri geliştirmek yerine, rakibine

16 Joni Salminen ve William Degbey, "Social Media Espionage – A Strategic Grid", *New Technology-Based Firms in the New Millennium*, Haz. Gary Cook (Emerald Group Publishing Limited, 2015), 261–274.

17 Ivanov, "Competitive Intelligence and Counterintelligence – Modern Tools For Generating Proactive Corporate Security", 7.

18 Peter Heims, *Countering Industrial Espionage* (Surrey: Century Security Education Ltd, 1982), 4.

19 Toriola, "Industrial Espionage or Competitive Intelligence: Two sides of the same coin", 3.

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

21 Melanie Reid, "A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat?", *University of Miami Law Review*, 70/757, 2016, 761.

karşı endüstriyel casusluk yöntemlerine başvurmanın önemli avantajları vardır. Elde edilen gizli materyaller yalnızca askeri veya teknolojik yeteneklerin geliştirilmesine katkıda bulunmakla kalmaz, aynı zamanda tasarruf edilen para da sosyo-ekonomik projelere yeniden tahsis edilebilir.[22]

Endüstriyel casusluk yalnızca etik dışı olmakla kalmaz, aynı zamanda birçok ülkede ceza kanunlarına göre önemli bir suçtur. Ancak buna rağmen yıllar geçtikçe bir dizi endüstriyel casusluk vakası yaşanmaya da devam etmektedir.[23]

Sonuç olarak, 21. yüzyılın bilgi temelli toplumun varlığıyla karakterize edildiği göz önüne alındığında, dünya çapında faaliyet gösteren işletmeler, iyi bir pazar konumu sağlayan ve özellikle endüstriyel casusluk girişimlerine karşı koruma sağlayan yeterli miktarda bilgiyi elde etmek için kalkınma çerçeveleri oluşturarak bu gerçekliğe uyum sağlamak zorundadır.[24] Ancak bu korumayı devletlerin ve onların istihbarat örgütlerinin desteği olmadan yapabilmeleri zordur.

Ayrıca bazı devletlerin ya da devlet dışı aktörlerin ve işletmelerin-özellikle de savunma alanında faaliyet gösteren işletmelerin- gizli olarak değerlendirdiği iş ayrıntılarının ve teknik bilgilerin hedef alınması, devletler tarafından ulusal güvenlik kapsamında değerlendirilmektedir.

Bu duruma ek olarak, ticari sırlara yönelik casusluk faaliyetleri, ekonomik büyüme ve istikrar açısından ana tehditler arasındadır. Bu açıdan endüstriyel casusluk hem kamuyu hem de özel sektörü etkileyen, askeri, siyasi ve ekonomik etkileri olan bir konudur.[25]

Bir sonraki bölümde endüstriyel casusluğun ulusal güvenlik açısından nasıl bir tehdit oluşturduğu incelenecektir.

Ulusal Güvenlik Açısından Endüstriyel Casusluk ve İstihbarat Örgütleri

Küreselleşmenin etkisiyle birlikte iletişimde yaşanan teknolojik ilerleme, sermaye akışı ve ticaret sayesinde tüm ekonomiler birbirine daha bağımlı hale gelmektedir. Bu çerçevede neoliberal bir uluslararası ekonomik sistemde, ekonomik olaylara karşı kırılganlık ve "yabancılara" bağımlılık, küresel pazarlarda yer almanın normal bir sonucudur. Bu nedenle bireyler, işletmeler ve devletler için güvensizlik duygusu giderek hâkim olmaya başlamıştır.[26] Böyle bir sistemde ekonomik güvenlik kavramı da askeri güvenliğin yanında öne çıkmaktadır.

Başka bir ifadeyle, Soğuk Savaş'ın sona ermesi jeopolitik bir dönüm noktası olmuş, ekonomik rekabet ivme kazanmış ve devletler küresel arenaya uyum sağlamak için yeni stratejilere başvurmuştur. Nitekim küreselleşme, uluslararası politika üzerinde önemli bir etkiye sebep olmuş, küresel aktörler arasında karşılıklı bağımlılığın artmasına yol açmış, dolayısıyla

22 Massimo Pellegrino, "The Threat of State-Sponsored Industrial Espionage", European Union Institute for Security Studies, 26, 2015. Erişim 15 Eylül 2023, https://op.europa.eu/en/publication-detail/-/publication/9de4b721-6256-43f0-b7df-988e3c4c9451; Shahar Argaman ve Gabi Siboni. "Commercial and Industrial Cyber Espionage in Israel", *Military and Strategic Affairs*, 6/1, 2014, 46.

23 Benny, *Industrial Espionage Developing a Counterespionage Program, 2-3.*

24 Colibasanu, "Between Intelligence and Espionage in the Contemporary Business Environment", 1.

25 Giancarlo Senatore, Fabio Lorenzo, Giovanna Galasso ve Federica Magna, "Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber", European Commission, 2019. Erişim 16 Eylül 2023, https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf.

26 Cable, "What is International Economic Security?", 305-306.

geleneksel Vestfalya sisteminden bir paradigma değişimi yaşanmıştır. Neticede de ekonomik boyut uluslararası ilişkilerin baskın vektörü olarak ortaya çıkmıştır. Nitekim devletlerarasındaki rekabet, askeri alandan ekonomik alana kaymış, askeri silahların yerini mali araçlar almaya başlamış ve savaş alanı piyasa rekabetine doğru kaymıştır. Bu durumun bir sonucu olarak da ulusal güvenlik ve ekonomik güvenlik giderek iç içe geçmiş iki kavram haline gelmiştir.[27]

Bu bağlamda Soğuk Savaş sonrası dönemde artan uluslararası ekonomik rekabet, endüstriyel casusluğun konumunu da yeniden şekillendirmiştir. Bu bakımdan endüstriyel casusluğun devletlerin hem ulusal varlıklarını korumaları hem de ulusal işletmelerin uluslararası düzeyde rekabetçi hale gelmeleri açısından vazgeçilmez bir yöntem haline gelmiştir.

Gizli kalması gereken ticari sırlar ya da işletme bilgilerinin rakip devletin eline geçme ihtimali, ekonomik güvenliğe yönelik bir tehdit olarak algılanırken, bu güvensizlik ortamında istihbarat örgütlerinin, askeri tehditlerin yanında endüstriyel casusluk ve bu casusluğa karşı koyma faaliyetlerini de içerecek şekilde görev ve yetkilerinin kapsamı da genişlemektedir.[28]

Günümüzde işletmeler ve uluslar, çok çeşitli alanlarda yeni teknolojiler, bilgiler ve yenilikler elde etmeye çalışan aktörler tarafından yasa dışı yöntemlerle her zamankinden daha fazla hedef alınmaktadırlar. Bu saldırıların hedefinde daha çok yüksek teknoloji, askeri uygulamalar ve biyoteknoloji yer almaktadır. Bu açıdan söz konusu alanlarda faaliyet gösteren işletmelerin kurumsal güvenliği, endüstriyel casusluğun önlenmesi ve mücadele edilmesinde giderek daha önemli hale gelmektedir. İstihbarat örgütleri de, kendi ülkelerinin önemli endüstrilerine yönelik casusluk çabalarıyla mücadele ederken, küreselleşmenin giderek hızlandığı bir çağda, özel sektörün de iyileştirilmiş ve yoğunlaştırılmış kurumsal güvenlik yoluyla bu zorluğa göğüs germesine destek olmaktadırlar.[29] Bir başka ifadeyle istihbarat örgütleri, kritik bilgilerin ve teknolojik yeniliklerin diğer aktörler tarafından ele geçirilmesi tehdidini önlemek amacıyla bu verileri yabancı rakiplerden korumaya yönelik çaba göstermektedirler.[30]

Örneğin ABD'de Federal Soruşturma Bürosu (Federal Bureau of Investigation-FBI) ve Merkezi Haberalma Teşkilatı (Central Intelligence Agency-CIA) endüstriyel tehdit bilgilerini, özellikle de casusluk tehdidini özel sektöre ve karar vericilere iletmeye yönelik en yetkili kurumlardandır. Özellikle FBI, ofislerinin bölgelerinde bulunan işletmelerle düzenli irtibat halindedir ve özel sektörün kendilerine yönelik casusluk tehditlerini anlamasına ve tanımasına yardımcı olmak için brifingler, broşürler ve diğer materyalleri sağlar. Sağlanan brifinglerin ve materyallerin içeriği, her işletmenin özel ihtiyaçlarına ve kaygılarına göre uyarlanır. CIA ise, idari emirlere uygun olarak kullanılmak üzere FBI'ya bilgi sağlar. Bazen CIA, ABD'li işletme yetkililerine, ABD işletmelerinin karşı karşıya olduğu yabancı istihbarat tehditleri

27 Andrea Binanti, "Economic Intelligence and Industrial Espionage", Luiss, Department of Political Science Master's Degree, 2019.

28 Edwin Fraumann, "Economic Espionage: Security Missions Redefined", *Public Administration Review*, 57/4, 1997, 303.

29 Lauri Holmström, "Industrial Espionage and Corporate Security: The Ericsson Case", Reports of the Police College of Finland, 87, 2010, 11-17. Erişim 16 Eylül 2023, https://www.theseus.fi/bitstream/handle/10024/86735/Rapotteja_87_holmstrom.pdf?sequence=1.

30 Binanti, "Economic Intelligence and Industrial Espionage", 45.

hakkında doğrudan bilgi verir. Uygun olduğu takdirde CIA, bir ABD işletmesine hedefin kendisi olduğunu bildirmeden önce diğer ABD Hükümeti kurumlarıyla, özellikle de FBI ile koordinasyon sağlar.[31]

Sonuç olarak, uluslararası mevzuatın endüstriyel casusluğa yönelik kapsamlı bir yasal çerçeve sağlamadaki yetersizliği göz önüne alındığında, küresel ağların genişliği, fikri mülkiyetler üzerindeki devlet kontrolünün garanti altına alınmasını zorlaştırmaktadır. Gerçekten de endüstriyel casusluk konusu son yüzyılda ivme kazanmış, istihbarat örgütleri için yeni zorluklara yol açmış ve ulusal güvenlik açısından ekonomik suçların/tehditlerin önemi artmıştır.[32]

İstihbarat örgütlerinin bu tehditlerle mücadele kapsamında karşılaştığı en önemli zorluk bilgi teknolojilerindeki gelişimdir. Casuslar için bilgisayar kullanımı, bizzat etrafı gözetlemekten çok daha güvenli ve daha az risklidir. Bir evrak çantasını çalmak yerine kişisel bir bilgisayardan kopyalama yapıldığında, iz bırakma ihtimali zayıf olmakta, dolayısıyla bu çekici bir casusluk şekli haline gelmektedir. Ayrıca siber alanda "iyi" niyetli insanları "kötü" niyetli insanlardan ayırmak da zordur, bu da söz konusu alanı aldatma planları için doğal bir ortam haline getirmektedir.[33]

İstihbarat örgütlerinin karşılaştığı bir diğer zorluk, endüstriyel casusluk faaliyetlerinin çok uluslu işletmelerin yaygınlaşmasıyla birlikte giderek daha fazla küreselleşmesidir. Rakip aktörler, belirli bir işletmeyi, kendi ulusundan başka bir ülkedeki şubesini hedef alabilmekte veya herhangi bir ürünü/teknolojiyi kendi ülkesinde üretmek için patent haklarına sahip olan başka bir işletmeyi hedefleyebilmektedir. Söz konusu durumlarda aynı veya benzer bilgilerin koruyucu güvenlik önlemlerinin çok sıkı olmadığı başka bir ülkeden alınması daha kolaydır. Başka bir ifadeyle, bilgiyi tutan işletmenin farklı güvenlik standartlarına sahip olması nedeniyle aynı bilgiyi yabancı ülkede hedeflemek daha kolaydır.[34] Sonuç olarak, söz konusu durumlarda istihbarat örgütlerinin karşı koyma faaliyetleri coğrafi sınırlar nedeniyle giderek zorlaşmaktadır.

İstihbarat örgütlerinin dikkat etmesi gereken hem teknik hem de teknik olmayan alanlarda genel olarak endüstriyel casusluk yöntemleri şu şekilde sınıflandırılabilir:[35]

- Siber saldırılar: Yukarıda da ifade edildiği gibi, siber saldırılar endüstriyel casusluğun az riskli ve çok yaygın bir yöntemidir. Bir saldırganın hedef işletmenin ağına saldırı

31 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 1995. Erişim 16 Eylül 2023, https://sgp.fas.org/othergov/indust.html#four.

32 Binanti, "Economic Intelligence and Industrial Espionage", 45.

33 Søilen K. Solberg, "Economic and Industrial Espionage at the Start of The 21st Century – Status quaestionis", *Journal of Intelligence Studies in Business*, 6/3, 2016, 52.

34 Roper, *Trade Secret Theft Industrial Espionage, and the China Threat*, 23.

35 Sharad Sinha, "Understanding Industrial Espionage For Greater Technological and Economic Security", *Digital Object Identifier*, 2012, 39-40.; Bernhardt, *Competitive Intelligence: How to Acquire and Use Corporate Intelligence and Counter-Intelligence,* 90-91; Fraumann, "Economic Espionage: Security Missions Redefined", 304; Gillian Dempsey, "Industrial Espionage: Criminal or Civil Remedies", *Australian Institute of Criminology*, No 106, 1999, 2. Erişim 17 Eylül 2023, https://www.aic.gov.au/sites/default/files/2020-05/tandi106.pdf; Santiago A. Cueto, "Spies, Lies and Secrets: 37 Industrial Espionage Tactics that Threaten to Kill Your International Business", 2013. Erişim 18 Eylül 2023, https://internationalbusinesslawadvisor.com/37-industrial-espionage-tactics-that-threaten-to-kill-your-international-business/.

başlatması ile gerçekleşebilir. Bu, ağa izinsiz giriş, kimlik avı, kimlik hırsızlığı veya truva atı yerleştirme şeklinde olabilir.

- Elektronik gözetim: Hedef işletmenin çalışanları teknik gözetim altına alınır. Bu, yasadışı telefon dinlemeyi, teknik takibi veya e-posta hesaplarına yasa dışı erişimi içerebilir.
- Tersine mühendislik: Bu yöntemde saldırgan, bir rakibin ürününde tersine mühendislik yaparak o ürünün tasarımı hakkında fikir sahibi olur. Hem donanım hem de yazılıma yöneliktir.
- Sızma ajan: İçeriden bir personelin satın alınması veya bir ajanın sızması.
- Çöp bidonuna dalma: Bir işletme tarafından atılan çöp kâğıtlarının başka bir işletme tarafından toplandığı bir bilgi toplama yöntemidir. Bu kâğıtlar, değerli bilgiler bulmak için incelenir ve analiz edilir. Bu faaliyet önemsiz görünebilir, ancak işletmelerin yüzlerce belge oluşturduğu ve bunların çoğunun zaman zaman çöp kutularına gittiği göz önüne alındığında önem kazanmaktadır.
- Ortak araştırma ve iş olanaklarından yararlanılması: Ortak araştırma ve iş faaliyetleri, iki tarafı yakınlaştırır ve her iki tarafta da gizli verilerin paylaşılmasına yol açar. Bu tür bilgilere erişim, bir tarafın, diğerine üstünlük sağlaması için kullanılabilir.
- Konferanslar, kongreler ve ticari fuarlar: İşletmeler rutin olarak konferanslara, kongrelere ve ticari fuarlara katılır. Farklı işletmelerin çalışanları, büyük ölçüde gayri resmi bir atmosferde birbirleriyle etkileşime girer. Bu ortam, bir işletme tarafından, çalışanlarıyla konuşarak diğer işletmeler hakkında önemli bilgiler toplamak için kullanılabilir.
- Dış Kaynak Kullanımı/Yerelleşme: Yabancı dış kaynak kullanımı yöntemleri, süreçleri veya bilgileri istismar edebilir. Lisans altında yerelliğin dışına çıkmak, genellikle telif hakkı veya ticari marka yasalarıyla sınırlı olmayan ülkelerde güvenlik kaybına yol açar.
- Paravan işletmeler ve kuruluşlar: Bazı işletmeler, rakiplerin ticari sırlarına erişmek için yazılım satıcısı veya hatta kâr amacı gütmeyen kuruluşlar gibi davranabilirler.
- Ortak girişim ve ihale süreci: Yabancı alıcılar, işletmelerin ihale sürecinde büyük miktarda veri sağlamasını isteyebilir ve bu da değerli özel bilgilerden ödün verilmesine neden olabilir.
- Yakınlık: Ortak girişimler ve stratejik ittifaklar, bir personeli işletmenin kilit personeli veya teknolojisiyle yakınlaştırabilir.
- Birleşmeler ve satın almalar: Birleşmeler ve satın almalar genellikle yeni bir işletmenin daha önce sahip olmadığı belirli teknolojileri edinmesine olanak tanır.

Sungur'a göre, söz konusu yöntemler çerçevesinde uluslararası sistemdeki ekonomik, siyasi ve askeri rekabetin "acımasız doğası" değişmemekle birlikte, kullanılan araç ve yöntemler teknolojik yeniliklerle orantılı bir şekilde giderek daha da karmaşık hale gelmekte ve çeşitlilik kazanmaktadır.[36]

36 Bülent Sungur, *Endüstriyel Casusluğun Soğuk Savaş Sonrası Küresel Rekabet Ortamındaki Yeri*, Yayımlanmamış Yüksek Lisans Tezi, (İstanbul: Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü Müdürlüğü, 2012).

Teknolojik yenilikler endüstriyel casuslukta etkili olmakla birlikte, hala en büyük tehdit, bir rakip için çalışan "sızma ajan"dır. Sızma ajan, rakiplerin rekabet avantajlarını artırmak için kayıtlara, dosyalara, belgelere, ürünlere, ekipmanlara, stratejik planlara ve müşteri ve satış kayıtlarına erişmesine olanak tanır. Personelin casusluk yapma veya sırları çalma nedenleri genellikle karışıktır ve maddi, duygusal ve/veya ideolojik nedenlerden de kaynaklanabilir. Casusluk motivasyonu, statüye ilişkin derin bir tatminsizlik, güvensizlik, bir azınlık grubuna üye olmak, aşırı hırslı veya fanatik olmaktan kaynaklanabileceği gibi bazı takıntılardan da kaynaklanabilir. Alkol, uyuşturucu, kumar ve diğer zafiyetler kolaylıkla takıntıya dönüşebilecek kötü alışkanlıklardan sadece birkaçıdır. Para genellikle bireylerin yozlaşmasında büyük bir rol oynar, ancak öfke ve intikam, özellikle bireylerin terfi için göz ardı edildiği veya katkılarının özel olarak tanınmadığını hissettiği durumlarda motivasyon faktörleridir.[37]

Bir işletmede herhangi birisi sızma ajan olarak kullanılacağı gibi, aşağıda altı kategoriye ait çalışanların casusluk faaliyetlerine katılma olasılığı daha yüksektir. Bunlar:[38]

- Bilim adamları/mühendisler, büyük ticari değere sahip olan önemli ürün tasarımı ve geliştirme ayrıntılarına erişebilirler.
- Uygulama mühendisleri, yardımcı oldukları ürün grubuyla ilgili mühendislik bilgisinin yanı sıra müşteriler, çalışma alanları ve teknik sorunları hakkında bilgi sahibidir.
- İşletme avukatları bekleyen patent başvuruları, birleşmeler ve satın almalar ve diğer gizli hukuki konularla ilgili bilgiye sahiptir.
- Teknik yazarlar kullanıcı kılavuzları, sürüm notları ve uygulama notları hazırlar ve dolayısıyla farklı ürün serileriyle ilgili kritik mühendislik bilgilerine erişebilirler.
- Satış personeli farklı ürünlere ilişkin satış tahminleri ve satış rakamları hakkında bilgi sahibi olur.
- Yöneticilerin ürün lansman planlarına, ürün genişletme planlarına ve stratejik bilgilere erişimi vardır.

Yukarıda bahse konu olan endüstriyel casusluk yöntemlerinin kullanımı geçmiş zamanlara dayanmakla birlikte, sıklıkla imparatorlukların yükselişinin "suç ortaklarından" biridir. Klasik Yunan şehirlerinden modern ABD işletmelerine kadar ticari sırların çalınması, neredeyse kan dökülmesi kadar rutin bir şekilde güç aktarımına işaret etmektedir.[39]

Endüstriyel casusluk faaliyetlerinin çoğunlukla teknoloji odaklı işletmelerde yaşandığı görülmektedir. Bu durumun temel nedenleri hem devletlerarasında askeri caydırıcılık temelli bir silahlanma yarışının yaşanması hem de teknoloji araştırma ve geliştirme faaliyetlerinin önemli miktarda maliyetli olmasıdır. Çoğunlukla hedef alınan işletme kolları arasında bilgisayar, yazılım, elektronik, havacılık, enerji, otomotiv, sağlık vb. yer alsa da örnekler incelendiğinde endüstriyel casusluk faaliyetlerinin özellikle savunma sanayi ve Ar-Ge çalışmaları üzerine yapıldığı görülmektedir.

37 Bernhardt, *Competitive Intelligence: How to Acquire and Use Corporate Intelligence and Counter-Intelligence,* 90-91.

38 Sinha, "Understanding Industrial Espionage For Greater Technological and Economic Security", 38.

39 Mara Hvistendahl, Valerio Pellegrini, "The Oldest Game", *Foreign Policy*, 232, 2019, 32.

Bir sonraki bölümde endüstriyel casusluğun tarihsel gelişimi ve ulusal güvenliği tehdit etmiş olan endüstriyel casusluk örnekleri incelenecektir.

Endüstriyel Casusluğun Tarihsel Gelişimi ve Ulusal Güvenliği Tehdit Eden Endüstriyel Casusluk Örnekleri

Yöntemler insan istihbaratına dayalı casusluktan siber saldırılara evrilen bir gelişim gösterse de, geçmişten günümüze endüstriyel casusluğun ana motivasyon kaynağı maddi kazancı siyasi çıkara dönüştürmek olarak aynı kalmıştır.

M.S. 550'de Bizans tarihçisi Procopius'a göre İmparator Justinianus, ipeğin sırrını getirmek için Nasturi Hıristiyan rahiplerini Çin'e göndermiş ve söz konusu rahipler Bizans'a, gizlenmiş ipekböceği yumurtalarıyla dönmüşlerdir. Daha sonra ise ipekböcekleri yumurtalarından çıkmış ve Çin'in bu alanda tekeli kırılmıştır.[40] Söz konusu olay endüstriyel casusluğun ilk örneklerinden biri olmuştur.

Bir başka örnek ise, Venediklilerin cam ve ayna gibi teknolojik yenilikler elde etmek için tüccar olarak denizaşırı seyahatlere çıkmaları ve söz konusu yenilikleri kendi ülkelerine getirme arayışlarıdır.[41] Diğer bir örnek de, 1712'de bir Cizvit rahibinin Çin'in porselen üretimine ilişkin sırları ele geçirmesidir. Rahip, üretim ayrıntılarını ve malzeme örneklerini Avrupa'ya göndererek Avrupalı tüccarlarla paylaşılmasını sağlamıştır.[42] Kısa bir süre içerisinde de Fransa'nın Sevres kentindeki bir porselen fabrikası, Çin ürünleriyle aynı seviyede sert hamurlu porselen üretmeye başlamıştır. Daha ileri bir gelişme olarak İngilizler, Fransızların sırlarını çalmayı başarmış ve Britanya'nın kendi üst düzey porselen endüstrisini kurmuşlardır.[43]

Endüstriyel casusluğun bir başka önemli örneği, 18. Yüzyılın sonlarında Fransa'nın, Büyük Britanya'nın endüstriyel gücüyle rekabet edebilmek için, İngiliz demir-çelik tersanelerine çıraklar yerleştirme faaliyetidir.[44] Britanya'da büyük ölçekli endüstriyel gelişme, Avrupa Kıtası'ndan çok daha erken gerçekleşmiş, Fransa'nın ilerlemesi ise, kısıtlayıcı loncalar, ağır vergiler ve ticaret ve seyrüsefer üzerindeki bürokratik kısıtlamaların yanı sıra, kömür ve diğer temel hammadde kıtlığı nedeniyle sekteye uğramıştır.[45] Bu nedenle Fransa'nın yürüttüğü endüstriyel casusluk faaliyetleri, planların doğrudan çalınmasından İngiliz zanaatkârlarını Fransa'ya getirmeye yönelik ortak çabalara kadar her şeyi içermiştir. Bu girişimler sonuç vermiş ve 1771'de tekstilde kullanılan iplik üretimini büyük ölçüde artıran bir makine olan "eğirme makinesinin" ayrıntılı planları ele geçirilebilmiştir. Bu olaydan sonra İngilizler, 18.

40 Hvistendahl, Pellegrini, "The Oldest Game"
41 Binanti, "Economic Intelligence and Industrial Espionage", 45-46.
42 Michael Disotell, "The Spies Who Loved Me (And My Trade Secrets): A Brief History of Industrial Espionage", 2013. Erişim 20 Eylül 2023, https://blogs.orrick.com/trade-secrets-watch/2013/09/18/the-spies-who-loved-me-and-my-trade-secrets-a-brief-history-of-industrial-espionage.
43 Stephen Mihm, "China Didn't Invent Industrial Espionage", Bloomberg, 2015. Erişim 21 Eylül 2023, https://www.bloomberg.com/view/articles/2015-05-26/china-didn-t-invent-industrial-espionage.
44 Disotell, "The Spies Who Loved Me (And My Trade Secrets): A Brief History of Industrial Espionage"
45 Margaret Bradley, "Examples of Industrial and Military Technology Transfer in the Eighteenth Century", *Documents pour l'histoire des techniques*, 2010, 87-88.

yüzyıl boyunca insanların ve fikirlerin akışını durdurmayı amaçlayan çeşitli önlemler aldılar. Örneğin bir yasa çıkartılarak, vasıflı İngiliz işçileri işe almaya çalışan baştan çıkarıcıların cezalandırılması amaçlanmış ve bu şekilde ayartılan her Britanyalı için 500 pound para cezası verilmesi kararı alınmıştır.[46]

18. yüzyılda ABD ise, endüstriyel casusluğu benzer maksatla kullanarak, bu alanda önemli bir başlangıcı teşkil etmiştir. Alexander Hamilton, Avrupa'nın teknik bilgisini çalmanın gerekliliğini vurgularken, Benjamin Franklin, İngiliz zanaatkârlarını açıkça Amerika'ya göç etmeye ve dolaylı olarak İngiliz makinelerini yanlarında getirmeye teşvik etmiştir.[47]

19. ve 20. yüzyılda ise dünya çapındaki çatışmalar politika yapıcıların gündemini işgal etmiş ve ulusal meselelerin odağı silah endüstrisi ve askeri güvenlik etrafında yoğunlaşmıştır.[48] Bu çerçevede İkinci Dünya Savaşı'na kadar endüstriyel casusluk gerilimleri Avrupa merkezli yaşanırken, İkinci Dünya Savaşı'ndan sonra işgücü gerilimleri azaldıkça daha çok ABD ve Sovyetler Birliği arasında yaşanmaya başlamıştır.[49]

Soğuk Savaş dönemi, iki blok arasındaki ekonomik asimetriler, endüstriyel casusluğun önemini artırmış; öyle ki Sovyetler Birliği, teknolojik boşluklar nedeniyle ekonomik geri kalmışlığını düzeltmek için endüstriyel casusluk faaliyetlerine başvurmuştur.[50] Hatta Soğuk Savaş sırasında, ABD'li işletmelerin hem Sovyet casuslarının hem de çok uluslu rakiplerin tehditleriyle karşı karşıya kalması nedeniyle, endüstriyel casusluk küresel bir mücadele alanı haline gelmiştir.[51]

Soğuk Savaş'ın sona ermesi, ulusal güvenliğin kapsamında değişikliğe neden olmuştur. Soğuk Savaş sırasında bloklar arası tehdit, ulusal güvenliğin odak noktasıydı ve istihbarat faaliyetleri bu tehdidin izlenmesine yoğunlaşmıştı. Soğuk Savaş sonrası ise ulusal güvenlik, askeri yeteneğin yanında ekonomik güç unsurlarını da içermeye başlamıştır.[52] Nitekim Soğuk Savaş'ın bitimiyle birlikte de askeri üstünlüğün yanında, ekonomik üstünlüğün artan önemi ile küresel ticarette büyük kazançlar elde etmek bazı ülkelerin temel hedefi haline gelmiştir. Bu mücadelede kendi işletmelerinin ulusal çıkar adına daha fazla kazanç sağlamasını isteyen devletler, istihbarat örgütlerini de geçmişte çok kullanmadıkları bir saha olan endüstriyel alanda kullanmaya başlamışlardır.[53]

Söz konusu durum, bir işletmenin başka bir işletme hakkında rekabet istihbaratına başvurması gibi basit bir yöntemden farklı bir alanı teşkil etmektedir. İstihbarat örgütleri, yurt dışındaki işletmelere yönelik casusluk yapma konusunda kendi ülkelerindeki işletmelere denizaşırı

46 Mihm, "China Didn't Invent Industrial Espionage"
47 Hvistendahl, Pellegrini, "The Oldest Game", 32.
48 Binanti, "Economic Intelligence and Industrial Espionage", 45-46.
49 Disotell, "The Spies Who Loved Me (And My Trade Secrets): A Brief History of Industrial Espionage"
50 Binanti, "Economic Intelligence and Industrial Espionage", 46; Mihm, "China Didn't Invent Industrial Espionage"
51 Disotell, "The Spies Who Loved Me (And My Trade Secrets): A Brief History of Industrial Espionage"
52 Diane C. Snyder, Sean Gregory, "Economic Intelligence in the Post-Cold War Era: Issues for Reform", 1997. Erişim 21 Eylül 2023, https://irp.fas.org/eprint/snyder/economic.htm.
53 Sungur, *Endüstriyel Casusluğun Soğuk Savaş Sonrası Küresel Rekabet Ortamındaki Yeri.*

operasyonlarda yardımcı olmaya başlamışlardır. Örneğin Çin ve Rusya, Almanya'da geliştirilen hassas ve yüksek değerli teknolojilere erişim sağlamak amacıyla kendi işletmelerine (Alman işletmeleri hakkında casusluk yaparak) yardım etmekle suçlanmıştır.[54]

Benzer faaliyetleri Fransa'nın istihbarat örgütü Dış Güvenlik Genel Müdürlüğü'nün de (Direction Generale de la Securite Exterieure-DGSE), yürüttüğü görülmektedir. DGSE, ABD menşeli çok uluslu işletmelerin yabancı ofislerine sızmaya çalışmış, bu girişim 1993 yılında, aralarında Boeing, IBM ve Texas Instruments'ın da bulunduğu birçok ABD şirketinin değerli hedefler olarak listelendiği Fransız hükümetine ait bir belgenin gazetelere sızdırılmasıyla açığa çıkmıştır.[55]

Casusluk faaliyetlerinin açığa çıkması güven kaybına ve işletmelerin hisse fiyatının düşmesine neden olacağından, bu tür faaliyetler istihbarat örgütleri ya da işletme çalışanları tarafından kasıtlı sızdırılmadıkça kamuoyu tarafından nadiren bilinmektedir.[56] Bu nedenle açık kaynaklarda yer alan örnekler de sınırlıdır.

Sonuç olarak kamuoyu tarafından bilinen 21. yüzyıldaki endüstriyel casusluk örnekleri incelendiğinde, artan askeri rekabetin ve bu durumdan kaynaklı güvensizlik hissinin doğası gereği, endüstriyel casusluk faaliyetlerinin savunma sanayi ve Ar-Ge çalışmaları üzerinde yoğunlaştığı görülmektedir.

Savunma sanayi, yapısı gereği ulusal güvenliği ilgilendiren inovasyonların gerçekleştirildiği ve bu çerçevede devletler açısından en ileri teknolojik atılımlar için yüksek öncelikli ve stratejik bir alandır.[57]

Savunma endüstrileri, devletlerin tehditleri caydırmasına ve güç kullanmasına olanak sağladığından dolayı önemli görülmelidir. Ama aynı zamanda ekonomik ve teknolojik bir öneme de sahiplerdir. Örneğin İngiltere, Fransa ve ABD'de savunma ekipmanları, toplam üretimin yaklaşık yüzde onunu temsil etmektedir. Yurt içi ve yurt dışından verilen ekipman siparişleri İngiltere'de yaklaşık 500.000, Fransa'da 300.000 ve ABD'de iki milyondan fazla kişiye istihdam sağlamaktadır.[58]

Dünyanın önde gelen devletleri, güvenlik ve askeri stratejilerini ve askeri organizasyon yapılarını yeniden dizayn etmekte ve askeri rekabette stratejik komuta avantajını sağlayabilmek için yeni türde araç-gereç (uzun menzilli hassas, akıllı, gizli veya insansız silah ve teçhizat geliştirmeye yönelik yaygın bir eğilim var) geliştirmektedirler. Örneğin ABD ve Rusya, mutlak askeri üstünlük arayışı içinde teknolojik ve kurumsal yeniliklere odaklanmakta, İngiltere, Fransa, Almanya, Japonya ve Hindistan askeri kuvvetlerinin yapısını teknolojik olarak yeniden dengelemekte ve optimize etmektedir. Sonuç olarak uluslararası askeri rekabet tarihi değişimler

54 Sinha, "Understanding Industrial Espionage For Greater Technological and Economic Security", 38.
55 Snyder, Gregory, "Economic Intelligence in the Post-Cold War Era: Issues for Reform"
56 Solberg, "Economic and Industrial Espionage at the Start of the 21st Century – Status Quaestionis", 52.
57 Erdal Akdeve ve Erman Benli, "Rekabet İstihbaratı ve Risklerin Tespiti", ThinkTech, 2020, 7. Erişim 22 Eylül 2023, https://thinktech.stm.com.tr/tr/rekabet-istihbarati-ve-risklerin-tespiti.
58 Trevor Taylor, "Defence Industries in International Relations", *Review of International Studies*, 16/1, 1990, 59.

geçirmekte ve savaşlar, "akıllı" savaşlara doğru evrilmektedir.[59]

Söz konusu yeni rekabette aktörlerin, birbirlerine karşı avantaj sağlayabilmek ya da nasıl bir tehditle karşı karşıya kaldıklarını öğrenebilmek adına geçmiş dönemlere göre daha yoğun bir şekilde casusluk faaliyetlerine başvurdukları görülmektedir.

Özellikle Rusya ve Çin, son dönemlerde rekabet dengesini kendi lehlerine çevirmek için endüstriyel casusluğu sıklıkla kullanmaktadırlar. Çin'de fikri mülkiyet hakları başka yerlerde olduğu kadar savunulmamaktadır. Üstelik özel sektör ile kamu sektörü arasında çok az ayrım olduğu göz önüne alındığında hem hükümet hem de işletmeler genellikle bu tür eylemlerden faydalanmaktadır. Her ne kadar Çin yavaş yavaş "inovasyon takipçisi" olmaktan "inovasyon lideri" konumuna geçse de ekonomik büyümedeki yavaşlama bu sürecin finanse edilmesini daha da zorlaştırmaktadır. Sonuç olarak, gerekli teknolojinin gizlice edinilmesi daha da cazip hale gelmektedir. Bu tehdit özellikle yüksek askeri teknolojili ürünler sunan, genellikle denizaşırı üretime başvuran ve bilimsel bilgi birikiminin bir kısmını Çinli ortaklara aktaran ABD ve Avrupa menşeli işletmeler için ciddidir.[60]

Çin'in, hassas ticari sırları ve özel bilgileri içerecek şekilde ABD teknolojisini elde etmek için kapsamlı çabaları bulunmaktadır. Stratejik kalkınma hedeflerini (bilim ve teknoloji ilerlemesi, askeri modernizasyon ve ekonomik politika hedefleri) desteklemek için özellikle siber casusluğu kullanmaya devam etmektedir.[61]

Geçtiğimiz otuz yıl boyunca ve özellikle son birkaç yılda, medyada çıkan çok sayıda haberler ve devam eden davalar ve tutuklamalar, Çin'in artan endüstriyel casusluk becerisini ortaya koymaktadır.[62] Lewis ve Wray'in ifadesine göre, Çin'in özellikle ABD'ye karşı yürüttüğü endüstriyel casusluk faaliyetleri benzeri görülmemiş düzeylerde ve Çinli istihbarat toplayıcılarına yönelik davalar şu anda Adalet Bakanlığı casusluk vakalarının yaklaşık yüzde doksanını oluşturmaktadır.[63]

Yakın zamandaki en önemli örnek, 2009 yılında Pentagon'un, F-35 Savaş Uçağı Projesi'nin kimliği belirsiz kişiler tarafından saldırıya uğramasıdır. Yeni nesil savaş uçağının milyarlarca dolarlık projesi, iki yıl boyunca koordineli siber casusluk saldırılarına maruz kalmış, saldırganlar, elektronik ve dahili bakımla ilgili büyük miktarda veriyi çalmak için Çin'de bulunan bilgisayarları kullanmışlardır.[64] Bu saldırıdan hareketle Çin'in, ABD'nin kritik altyapısına sızma ve ABD

59 Anthony H. Cordesman, Arleigh A. Burke, Max Molot, "China's Rising Military Technology and Industrial Base", *Strategic and International Studies*, 2019, 228.

60 Pellegrino, "The Threat of State-Sponsored Industrial Espionage"

61 National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace", 2018, 5. Erişim 22 Eylül 2023, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

62 Roper, *Trade Secret Theft Industrial Espionage, and the China Threat*, 33.

63 James Andrew Lewis, "Counterespionage", *Center for Strategic and International Studies*, 2019; Christopher Wray, "Responding Effectively to the Chinese Economic Espionage Threat", FBI, 2020. Erişim 24 Eylül 2023, https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat.

64 Pierluigi Paganini, "10 Biggest Cyber Espionage Cases", 2017. Erişim 28 Eylül 2023, https://securityaffairs.com/66617/hacking/cyber-espionage-cases.html.

Donanması'nın Pasifik bölgesindeki iletişimini bozma yeteneğine sahip olduğu yönünde genel bir düşünce bulunmaktadır.[65] Segal, ABD ve Çin arasındaki bir güvenlik meselesi haline gelen rekabeti "teknoloji soğuk savaşı" olarak tasvir etmektedir.[66]

Bu "teknoloji soğuk savaşında" gerilimi arttıran başka gelişmeler de yaşanmıştır. 2018 yılında üç Çin vatandaşı, uluslararası işletmelerden veri çalmak için kimlik avı dolandırıcılığı ve kötü amaçlı yazılım kullanan bir siber güvenlik şirketi işletmekle suçlanmıştır. Açıklanan iddianamede, söz konusu kişilerin hedeflerinin arasında Siemens AG, New York'taki Moody's Analytics ve Sunnyvale, California'daki Trimble Inc. yer aldığı belirtilmektedir. Başka bir vakada, Çinli siber aktörler ile CCleaner olarak bilinen ticari yazılıma girişe izin veren bir arka kapı arasında bağlantılar bularak, Google, Microsoft, Intel ve VMware'in de bulunduğu ABD işletmelerini hedef almışlardır.[67]

Endüstriyel casusluk faaliyetleri, benzer şekilde Rusya'nın da modernizasyon çabalarının uygulanabilir bir bileşenidir. Hatta Pellegrino'nun ifadesine göre, Rus istihbarat örgütleri, "ülkelerinin ekonomik kalkınmasını ve bilimsel ve teknik ilerlemesini desteklemek için" yasalar ve direktifler çerçevesinde bu faaliyetleri yürütmekle yetkilidirler.[68]

Rusya'nın, teknoloji gibi sektörlere yönelik ekonomik çeşitlendirmeyi de içeren yapısal reformları gerçekleştirebilmek için Rus istihbarat örgütlerinin, hassas ABD iş ve teknoloji bilgilerini toplamak adına karmaşık ve büyük ölçekli casusluk operasyonları gerçekleştirdiği belirtilmektedir.[69]

Rus istihbarat örgütlerinin bu maksatla kullandığı bilinen yöntemleri şunlardır:[70]

- Batı ile etkileşime giren Rus ticari ve akademik girişimlerinin kullanılması;
- İleri teknik becerilere sahip Rus göçmenlerin Rus istihbarat servisleri tarafından işe alınması;
- Hükümetin sanayiden hassas teknik bilgiler elde etmesine olanak tanıyan Rus istihbaratının kamu ve özel kuruluşlara sızması.

Örneğin, 1999 yılında Newsweek, ABD'deki askeri teknolojilere yönelik ilk koordineli siber casusluk vakasını ortaya çıkarmıştır. Kimliği belirsiz kişiler, Wright Patterson Hava Kuvvetleri Üssü'nün ağına sızarak, askeri araştırma kurumlarına bağlanmış ve binlerce belgeyi ele geçirebilmişlerdir. Ayışığı Labirenti olarak belirtilen bu saldırılarda Rusya suçlanmış ancak kanıtlanamamıştır.[71] Örnekler sadece ABD'ye yönelik olmamakla birlikte, Rusya, destekli bir

65 Michael G. Mclaughlin, William J. Holstein, "A Long March: China's Military-Industrial Espionage", 2023. Erişim 21 Eylül 20223, https://asiatimes.com/2023/06/a-long-march-chinas-military-industrial-espionage/.

66 Adam Segal, "The Coming Tech Cold War With China", Foreign Affairs, 2020. Erişim 02 Ekim 20203, https://www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-china.

67 The Associated Press, "How China, Russia, Iran Target US With Economic Espionage", 2018. Erişim 02 Ekim 2023, https://apnews.com/united-states-government-general-news-bc0d920ef35d4c8296f79cebb1a9bd6f.

68 Pellegrino, "The Threat of State-Sponsored Industrial Espionage", 1-2.

69 National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace", 8.

70 National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace", 8.

71 Paganini, "10 Biggest Cyber Espionage Cases"; Dick O'Brien, "A Short History Of Cyber Espionage", 2017. Erişim 14 Ekim 2023, https://medium.com/threat-intel/cyber-espionage-spying-409416c794ec.

aktör olarak tanımlanan "Yusufçuk (Dragonfly)" (Vahşi Ayı olarak da bilinir) 2010 yılından bu yana elektrik üretimi ve enerji şebekesi yönetimi alanlarında Avrupalı firmaları hedef alan casusluk kampanyaları yürütmektedir.[72] Ayrıca APT28 olarak bilinen Rus devleti destekli siber yapının, 2007 yılından bu zamana ABD ve Avrupa'nın savunma kurumları hakkında istihbarat topladığı iddia edilmektedir.[73]

Benzer şekilde İran'ın da müdahil olduğu endüstriyel casusluk vakaları bulunmaktadır. Özellikle son dönemlerde, İran Devrim Muhafızları'na bağlı birim ve aktörlerin başta İsrail ve ABD'nin hükümet ve ticari kurumlarını hedef alabilme noktasında gittikçe tecrübelendiği görülmektedir.

Çin'in aksine İran'ın, çalıntı fikri mülkiyeti kullanabilecek bir endüstriyel üretim sektörünün bulunmaması nedeniyle ticari casusluğu kullanımı sınırlıdır. Bu nedenle İran'ın endüstriyel casusluk faaliyetleri, daha çok havacılık, savunma sanayi, telekomünikasyon, enerji ve madencilik alanlarını hedef alarak, askeri teknolojik gücünü artırmaya hizmet etmektedir.[74]

Örneğin 2020 yılında, İran bağlantılı "Gelişmiş Kalıcı Tehdit (Advanced Persistent Threat/ APT33)" birim, elektrik hizmetlerinde, imalatta ve petrol rafinerilerinde kullanılan endüstriyel kontrol sistemlerinin tedarikçilerini ve imalatçılarını giderek daha fazla hedef almaya başlamıştır. APT33'ün endüstriyel kontrol sistemleri için ekipman tedarikçilerini ve yazılım sağlayıcılarını hedeflemesi, özellikle enerji, petrol ve gaz, denizcilik ve imalat sektörlerinde bu tür sistemleri dünya çapında kullanan kuruluşlar için sonuçlar doğurmaktadır. Orta Doğu'da, özellikle de Suudi Arabistan, BAE ve Bahreyn'e bu tür endüstrilerde güçlü varlığı veya bağlantıları olan kuruluşlar, ilgili APT33 faaliyetlerinden dolayı daha yüksek bir tehditle karşı karşıyadır.[75] İran Devrim Muhafızları ile bağlantısı olduğuna inanılan Rocket Kitten adlı İranlı bir hacker grubu da, İran'ın füze ve uzay programlarını geliştirmesine yardımcı olmak için önemli ABD savunma işletmelerini hedef almaktadır.[76]

Sonuç

Devletler, uluslararası sistemde rekabet üstünlüğünü korumaya çabalarken, endüstriyel casusluk faaliyetleri, özellikle savunmayla ilgili araştırma, geliştirme ve inovasyonun bütünlüğüne yönelik tehditler oluşturan zorlu bir mücadele alanı olmuştur. Bu nedenle rekabet istihbaratından daha çok özellikle bu tür endüstriyel casusluk faaliyetleri devletler tarafından ulusal güvenlik

72 Pellegrino, "The Threat of State-Sponsored Industrial Espionage", 2.

73 The Associated Press, "How China, Russia, Iran Target US With Economic Espionage"

74 Collin Anderson, Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage and Revenge", *Carnegie Endowment for International Peace*, 2018. Erişim 17 Eylül 2023, https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf.

75 Control Risks. "Iranian Cyber Espionage Group Targets Suppliers of Industrial Control Systems", 2020. Erişim 03 Ekim 20203, https://www.controlrisks.com/our-thinking/insights/iranian-cyber-espionage-group-targets-suppliers-of-industrial-control-systems?utm_referrer=https://www.google.com; Andy Greenberg, "A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems", 2019. Erişim 12 Ekim 2023, https://www.wired.com/story/iran-apt33-industrial-control-systems/.

76 The Associated Press, "How China, Russia, Iran Target US With Economic Espionage"

kapsamında değerlendirilmiş ve bu faaliyetlere karşı koyma, istihbarat örgütlerinin görev ve yetki alanı kapsamına alınmıştır.

Yüksek teknoloji, askeri uygulamalar ve biyoteknoloji alanında gizli kalması gereken bilgilerin, fikirlerin ve ticari sırların rakip/düşman devletlerin eline geçme ihtimali, devletler tarafından ekonomik güvenliğe yönelik bir tehdit olarak algılanmaktadır. Bu açıdan söz konusu alanlarda faaliyet gösteren işletmelerin kurumsal güvenliği, devletler açısından giderek daha önemli hale gelmekte ve bu nedenle de istihbarat örgütlerinin görev ve yetkilerinin kapsamı da endüstriyel casusluğa karşı işletmelerin kurumsal güvenliklerine ihtiyaç verecek şekilde genişlemektedir. Özellikle, ulusal ve uluslararası mevzuatların endüstriyel casusluğa yönelik kapsamlı bir yasal çerçeve sağlamadaki yetersizliği göz önüne alındığında, kurumsal güvenliği sağlamada istihbarat örgütlerinin rolünün giderek önemli bir hal aldığı düşünülmektedir.

Günümüzde birçok işletmenin kurumsal güvenlik departmanları olmasına rağmen, örneklerden yola çıkarak endüstriyel casusluk faaliyetlerinin artan boyutları göz önünde bulundurulduğunda, çok az işletme iyi planlanmış bir karşı istihbarat fonksiyonuna sahiptir. Ayrıca, istihbarat örgütlerinin de kendi ülkelerine askeri, ekonomik ve teknolojik avantaj sağlayabilmek adına bizzat endüstriyel casusluğa başvurmaları, işletmelerin zaten zayıf olan kurumsal güvenlik departmanlarını daha da tehdit eder hale getirmektedir. Söz konusu durumlara ek olarak siber alanın kullanımının yaygınlaşması ve bilginin/verinin, mesafe ve ulusal sınırları aşarak, kolay bir şekilde aktarılması, işletmeler için çok çeşitli güvenlik risk ve tehditleri de beraberinde getirmiştir. Bu noktada siber alanda gerçekleşen endüstriyel casusluk faaliyetlerinin tespiti ve karşı koyma stratejilerinin geliştirilmesi de işletmelerin kurumsal güvenlik departmanlarını zorlamaktadır. Söz konusu nedenler göz önüne alındığında, işletmelerin kurumsal güvenliklerini sağlamada kendi ülkelerinin istihbarat örgütlerinden destek almaları bir zorunluluk teşkil etmektedir.

Endüstriyel casusların kullandığı yöntemler ve bu faaliyetlerin yürütülmesi için angaje edilen kişilerin seçilmesinde kullanılan motifler, istihbarat örgütlerinin geleneksel tehditlerin tespit edilmesinde kullandığı yöntemlerle benzerdir. Bu sebeple endüstriyel casusluğa karşı koyma yöntemleri belirlenirken, casusluğu önlemek için kullanılan karşı önlemler referans alınabilir. Bu noktada işletmelerin, istihbarat örgütleri ile işbirliği yapmalarının yanında, onlardan öğreneceği çok şey bulunmaktadır.

İstihbarata karşı koyma (İKK), yabancı istihbarat örgütlerinin oluşturduğu tehdidin tanımlanması, etkisiz hale getirilmesi ve bu servislerin manipüle edilmesi olarak tanımlanabilir. İKK'nın en temel amacı, bilgiyi, almaya yetkili olmayan kişilerden korumak, potansiyel tehditlere karşı koymak ve güvenliği arttırmaktır. Endüstriyel casusluğa karşı koyma kapsamında, yalnızca saldırgan ve yasa dışı bilgi toplamaya karşı koruma sağlamamalı, aynı zamanda bir işletmeye zarar verebilecek ve işletmenin pazarda rekabet etme yeteneğini etkileyebilecek açık ve yasal toplama çabalarına karşı da koruma sağlamalıdır. Ayrıca İKK faaliyetleri, elektronik dinleme gibi yasa dışı faaliyetleri önleyecek, bir işletmenin kendisi hakkında yayınladığı kritik

bilgileri dikkatle kontrol edecek ve rakiplerin bilgi toplamasını zorlaştırarak ticari istihbarat ve casusluk çabalarına karşı savunmasız olan alanları koruyacaktır.[77]

Bu kapsamda, endüstriyel casusluğa karşı koymak için istihbarat örgütlerinde olduğu gibi işletmelerin de birbirini geliştiren ve destekleyen dört bölümü olmalıdır. Bunlar: Teknik, operasyonel, fiziksel ve personel güvenliği olarak sıralanabilir. Teknik güvenlik önlemleri elektronik sistemlerde mevcut olan güvenlik açıklarını azaltır. Karşı önlemler de bilgisayar sistemleri ve ağlarının gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlar. Operasyonel güvenlik, bir işletme tarafından kullanılan ve teknik olmayan yollarla bilgileri tehlikeye atabilecek iş süreçlerini ele alır. Örneğin, yalnızca "bilinmesi gerekenler" esasına göre bilgi erişimine ilişkin istihbarat örgütlerinin prensibi, bilgilerin gereksiz yayılmasının önlenmesine yardımcı olur. Fiziksel güvenlik için ise, tesislere fiziksel erişim dikkatle düzenlenmeli ve kontrol edilmelidir. Bu, kendi çalışanlarınızın yanı sıra ziyaretçilerin ve yüklenicilerin erişiminin sınırlandırılmasını da içerir. Hiç kimsenin tüm kurumsal tesislerde serbestçe dolaşmasına izin verilmemelidir. Personel güvenliği için ise, özellikle hassas bilgilere erişme potansiyeli olan tüm kişiler hakkında kapsamlı bir soruşturma yapılmalıdır. Bilgilerin çoğu bir kuruluş içindeki farklı departmanlar için hassas olabileceğinden, muhtemelen tüm çalışanların özgeçmiş kontrolünün yapılması genel bir politika olmalıdır.[78]

Günümüzde istihbarat örgütleri ile işletmeler kritik bilgilerin ve teknolojik yeniliklerin diğer aktörler tarafından ele geçirilmesi tehdidini önlemek amacıyla ortak işbirliği içerisinde çaba göstermektedirler. Ancak bu çabanın daha fazla geliştirilmesi, özellikle siber saldırıları ve diğer endüstriyel casusluk türlerinin tespitinde ortak yenilikçi yaklaşımların ortaya konması gerekmektedir. Ayrıca devletler ve uluslararası örgütler/kurumlar tarafından ulusal ve uluslararası mevzuatlarda, endüstriyel casusluk suçuna karşı caydırıcılığı arttırıcı ağır yaptırımların ve cezaların yer alması sağlanmalıdır.

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazarlar çıkar çatışması bildirmemiştir.
Finansal Destek: Yazarlar bu çalışma için finansal destek almadığını beyan etmiştir.
Yazar Katkıları: Çalışma Konsepti/Tasarım- A.G., T.A.; Veri Toplama- A.G., T.A.; Veri Analizi/Yorumlama- A.G., T.A.; Yazı Taslağı- A.G., T.A.; İçeriğin Eleştirel İncelemesi- A.G., T.A.; Son Onay ve Sorumluluk- A.G., T.A.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The author has no conflict of interest to declare.
Grant Support: The author declared that this study has received no financial support.
Author Contributions: Conception/Design of Study- A.G., T.A.; Data Acquisition- A.G., T.A.; Data Analysis Interpretation- A.G., T.A.; Drafting Manuscript- A.G., T.A.; Critical Revision of Manuscript- A.G., T.A.; Final Approval and Accountability- A.G., T.A.

77 Bernhardt, *Competitive Intelligence: How to Acquire and Use Corporate Intelligence and Counter-Intelligence,* 88.

78 Ira S. Winkler, "Case Study of Industrial Espionage Through Social Engineering", 1996, 4-6. Erişim 20 Eylül 2023,https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=e01cfb43fd2df7bb751aefff10ed79f58342e255.

Kaynakça/References

Akdeve, Erdal, Erman Benli, "Rekabet İstihbaratı ve Risklerin Tespiti.", *ThinkTech*. 2020. Erişim 22 Eylül 2023. https://thinktech.stm.com.tr/tr/rekabet-istihbarati-ve-risklerin-tespiti.

Anderson, Collin, Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage and Revenge.", *Carnegie Endowment for International Peace*. 2018. Erişim 17 Eylül 2023. https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf.

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage. 1995. Erişim 16 Eylül 2023. https://sgp.fas.org/othergov/indust.html#four.

Argaman, Shahar, Gabi Siboni. "Commercial and Industrial Cyber Espionage in Israel.", *Military and Strategic Affairs*. 6/1, 2014. 43-58.

Benny, Daniel J. *Industrial Espionage Developing a Counterespionage Program*. Boca Raton: Taylor & Francis Group, 2014.

Bernhardt, Douglas. *Competitive Intelligence: How to Acquire and Use Corporate Intelligence and Counter-Intelligence*. Edinburgh: Prentice Hall, 2003.

Binanti, Andrea. "Economic Intelligence and Industrial Espionage.", Luiss, Department of Political Science Master's Degree. 2019.

Bradley, Margaret. "Examples of Industrial and Military Technology Transfer in The Eighteenth Century.", *Documents pour l'histoire des techniques*. 2010. 87-95.

Brazdilova, Miroslava. "Competitive Intelligence and Competitive Abilities of Enterprises.", *Ekonomika A Management*. 2005.

Bronwyn, Higgs. "Industrial espionage: The Legal Way.", *Marketing Magazine*. 76, 2005. 76-77.

Cable, Vincent. "What is International Economic Security?.", *International Affairs*. 71/2, 1995. 305-324.

Colibasanu, Antonia. "Between Intelligence and Espionage in the Contemporary Business Environment.", *Ekonomika a Management Prague University of Economics and Business*. 4, 2008. 1-13.

Control Risks. "Iranian Cyber Espionage Group Targets Suppliers of Industrial Control Systems.", 2020. Erişim 03 Ekim 20203. https://www.controlrisks.com/our-thinking/insights/iranian-cyber-espionage-group-targets-suppliers-of-industrial-control-systems?utm_referrer=https://www.google.com.

Cordesman, Anthony H., Arleigh A. Burke, Max Molot, "China's Rising Military Technology and Industrial Base.", *Strategic and International Studies*. 2019.

Cueto, Santiago A. "Spies, Lies and Secrets: 37 Industrial Espionage Tactics that Threaten to Kill Your International Business.", 2013. Erişim 18 Eylül 2023. https://internationalbusinesslawadvisor.com/37-industrial-espionage-tactics-that-threaten-to-kill-your-international-business/.

Dempsey, Gillian. "Industrial Espionage: Criminal or Civil Remedies.", *Australian Institute of Criminology*. No 106, 1999. Erişim 17 Eylül 2023. https://www.aic.gov.au/sites/default/files/2020-05/tandi106.pdf.

Disotell, Michael. "The Spies Who Loved Me (And My Trade Secrets): A Brief History of Industrial Espionage.", 2013. Erişim 20 Eylül 2023. https://blogs.orrick.com/trade-secrets-watch/2013/09/18/the-spies-who-loved-me-and-my-trade-secrets-a-brief-history-of-industrial-espionage.

Fraumann, Edwin. "Economic Espionage: Security Missions Redefined.", *Public Administration Review*. 57/4, 1997. 303-308.

Greenberg, Andy. "A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems.", 2019. Erişim

12 Ekim 2023. https://www.wired.com/story/iran-apt33-industrial-control-systems/.

Heims, Peter. *Countering Industrial Espionage*. Surrey: Century Security Education Ltd, 1982.

Holmström, Lauri. "Industrial Espionage and Corporate Security: The Ericsson Case.", *Reports of the Police College of Finland*. 87, 2010. 11-17. Erişim 16 Eylül 2023. https://www.theseus.fi/bitstream/handle/10024/86735/Rapotteja_87_holmstrom.pdf?sequence

Hvistendahl, Mara, Valerio Pellegrini, "The Oldest Game.", *Foreign Policy*. 232, 2019. 32-33.

Ivanov, Tsanko V. "Competitive Intelligence and Counterintelligence – Modern Tools For Generating Proactive Corporate Security.", *International Scientific Journal Security & Future*. 1/1, 2017. 7-10.

Labonia, Francesca. "The Strategic Role of Competitive Intelligence: A Study of The Brazilian Market.", 2018. Erişim 10 Eylül 2023. https://repositorio.usp.br/directbitstream/b7e691e0-ca07-4bb3-9a88-5966e8754b46/FRANCESCA%20LABONIA%20-%20PRO18.pdf.

Lewis, James Andrew. "Counterespionage.", *Center for Strategic and International Studies*. 2019.

Mclaughlin, Michael G., William J. Holstein, "A Long March: China's Military-Industrial Espionage.", 2023. Erişim 21 Eylül 20223. https://asiatimes.com/2023/06/a-long-march-chinas-military-industrial-espionage/.

Mihm, Stephen. "China Didn't Invent Industrial Espionage.", Bloomberg, 2015. Erişim 21 Eylül 2023.https://www.bloomberg.com/view/articles/2015-05-26/china-didn-t-invet-industrial-espionage.

National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace.", 2018. Erişim 22 Eylül 2023. https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

O'Brien, Dick. "A Short History of Cyber Espionage"., 2017. Erişim 14 Ekim 2023. https://medium.com/threat-intel/cyber-espionage-spying-409416c794ec.

Paganini, Pierluigi. "10 Biggest Cyber Espionage Cases.", 2017. Erişim 28 Eylül 2023. https://securityaffairs.com/66617/hacking/cyber-espionage-cases.html.

Pellegrino, Massimo. "The Threat of State-Sponsored Industrial Espionage.", *European Union Institute for Security Studies*. 26, 2015. Erişim 15 Eylül 2023. https://op.europa.eu/en/publication-detail/-/publication/9de4b721-6256-43f0-b7df-988e3c4c945.

Reid, Melanie. "A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat?.", *University of Miami Law Review*. 70/757, 2016. 757-829.

Roper, Carl. *Trade Secret Theft Industrial Espionage, and the China Threat*. Boca Raton: Taylor & Francis Group, 2014.

Salminen, Joni, William Degbey. "Social Media Espionage – A Strategic Grid.", *New Technology-Based Firms in the New Millennium*, Haz. Gary Cook. Emerald Group Publishing Limited, 2015. 261–274.

Segal, Adam. "The Coming Tech Cold War With China", Foreign Affairs. 2020. Erişim 02 Ekim 20203.https://www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-china.

Senatore, Giancarlo, Fabio Lorenzo, Giovanna Galasso ve Federica Magna. "Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber.", *European Commission*. 2019. Erişim 16 Eylül 2023. https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf.

Shaitura, Sergey Vladimirovich, Konstantin Vasilievich Ordov, Irina Georgievna Lesnichaya, Yulia Dmitrievna Romanova, Seda Seiranovna Khachaturova. "Services and Mechanisms of Competitive Intelligence on The Internet.", *ESPACIOS*. 39/45, 2018. 1-7.

Sinha, Sharad. "Understanding Industrial Espionage For Greater Technological and Economic Security.",

Digital Object Identifier. 2012. 37-41.

Snyder, Diane C., Sean Gregory, "Economic Intelligence in the Post-Cold War Era: Issues for Reform.", 1997. Erişim 21 Eylül 2023. https://irp.fas.org/eprint/snyder/economic.htm.

Solberg, Søilen K. "Economic and Industrial Espionage at The Start of The 21st Century – Status Quaestionis.", *Journal of Intelligence Studies in Business*. 6/3, 2016. 51-64.

Sungur, Bülent. *Endüstriyel Casusluğun Soğuk Savaş Sonrası Küresel Rekabet Ortamındaki Yeri*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü Müdürlüğü, 2012.

Tahmasebifard, Hamid. "The Role of Competitive Intelligence and Its Sub-Types On Achieving Market Performance.", *Cogent Business & Management*. 5/1, 2018. 1-16.

Taylor, Trevor. "Defence Industries in International Relations.", *Review of International Studies*. 16/1, 1990. 59-73.

The Associated Press, "How China, Russia, Iran Target US With Economic Espionage.", 2018. Erişim 02 Ekim 2023. https://apnews.com/united-states-government-general-news-bc0d920ef35d4c8296f79cebb1a9bd6f.

Toriola, Temitope. "Industrial Espionage or Competitive Intelligence: Two Sides of the Same Coin.", *Purdue University*. 2011. Erişim 12 Eylül 2023. https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2011-10-report.pdf.

Vriens, Dirk. "The Role of Information and Communication Technology in Competitive Intelligence.", *Idea Group Inc*, 2004. Erişim 07 Eylül 2023. https://repository.ubn.ru.nl/handle/2066/139628.

Winkler, Ira S. "Case Study of Industrial Espionage Through Social Engineering.", 1996, 4-6. Erişim 20 Eylül 2023. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=e01cfb43fd2df7bb751aefff10ed79f58342e255.

Wray, Christopher. "Responding Effectively to the Chinese Economic Espionage Threat.", *FBI*. 2020. Erişim 24 Eylül 2023. https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat.

Wright, Phillip C., Géraldine Roy, "Industrial Espionage and Competitive Intelligence: One You Do; One You Do Not.", *Journal of Workplace Learning*. 11/2, 1999. 53-59.