**T.C**

**SAHA İSTANBUL & TÜBİTAK TÜSSİDE**

**SAHA AKADEMİ MBA YÖNETİCİ GELİŞTİRME PROGRAMI**

# Stratejide Yapay Zekâ



**MBA Proje**
**Barış İlker GÖKER**

**Danışman**
**Dr. Uğur TARÇIN**

**İstanbul - 2025**

**ARAŞTIRMA PROJESİ UYGUNLUK FORMU**

**MBA: 2024-2025/03**

**1**. SAHA İstanbul Yönetim Kurulu kararıyla, 2024-2025 eğitim döneminden itibaren SAHA AKADEMİ MBA katılımcılarına "Araştırma Projesi" hazırlama yükümlülüğü getirilmiştir. Bu uygulama; katılımcıların sektörel bilgi, stratejik düşünme ve akademik üretkenlik yetkinliklerini geliştirmeyi hedeflerken, savunma sanayii ekosistemine bilimsel katkıyı artırmayı amaçlamaktadır. Bu girişim, Türk savunma sanayii ekosisteminde bilimsel katkıyı artırmaya yönelik önemli bir adımdır.

**2**. SAHA İstanbul-SAHA AKADEMİ tarafından yayımlanan bu çalışma, ilgili yazar tarafından özgün biçimde hazırlanmış ve beyan edilmiştir. Çalışmada yer alan görüşler yazara ait olup, SAHA İstanbul'un kurumsal görüşünü yansıtmamaktadır. İçerikte sunulan bilgi, yorum ve sonuçların doğruluğu sorumlu yazara aittir. SAHA AKADEMİ; benzerlik oran tespitini yapmıştır.

**3**. Bu çalışma, [ Barış İlker GÖKER ] tarafından hazırlanmıştır. Araştırma Projesi danışman tarafından değerlendirilmiş ve sunumu [ 11 Mayıs 2025 ] tarihinde yeterli görülerek kabul edilmiştir.

**Araştırma Projesi Sunum Jüri Üyeleri**

| | | |
|---|---|---|
| **Başkan** | Dr. Uğur Tarçın (*SAHA AKADEMİ Öğr.Görevlisi)* | *e-imzalıdır* |
| **Üye** | Ayşe Çağın (*SAHA AKADEMİ Yöneticisi)* | *e-imzalıdır* |
| **Üye** | Muzaffer Ünsaldı (*Kurumsal İletişim ve Marka Yöneticisi*) | *e-imzalıdır* |

*(Formun aslı, imzalı olarak ilgili dosyada muhafaza edilmektedir.)*

# İÇİNDEKİLER

# STRATEJİDE YAPAY ZEKÂ

## (Proje- Öneri)

**Barış İlker GÖKER**

Hava Kuvvetleri Komutanlığı

barisilkergoker@gmail.com

### 1. Proje Amacı

Bilindiği üzere toplumsal hayatın her alanında mikro seviyeden makro düzeye kadar strateji kurumların ve kuruluşların yaşam döngüsünde büyük önem arz etmektedir. Daha çok askerî alanlarla bağdaştırılan bu kavram yönetimsel kurguların gelişmesi ile beraber gerek kamu gerekse özel kurumlarda da alacakları kararlar, risk yönetimleri ve çözüm yaklaşımları için vazgeçilmez bir yapı taşı haline gelmiştir. Diğer yandan teknolojik gelişmelerle beraber risk alanları artmış bunun sonucunda ise zaman tüm bu kurumlar için en değerli kavram haline gelmiştir. Kurumların bu gelişmeler karşısında strateji oluştururken yapay zekâ kullanımının zaman tasarrufu, bilgiye hızlı erişim, tecrübe aktarımı konularıyla beraber daha etkili risk senaryolarının oluşturulabileceği ve tüm bu sayılan konuları bilmesi gereken prensibi dahilinde güvenli ve hızlı bir şekilde bağlı bulundukları üst karar mekanizmalarına iletebileceği varsayılmaktadır.

Yukarıda bahsedilen hususlar kapsamında projenin amacını başlıklar halinde ele almak gerekirse;

- **Askerî Strateji Üretimi ve Harp Oyunları:**

Askerî yapının ayrılmaz parçası olan strateji kavramı en temel noktada içinde bulunulan durum

hakkında elde edilen bilgiler ışığında bölgesel, tehdit ve eldeki kabiliyetlerin analizlerinin yapılarak eylem planı oluşturma durumudur.

Günümüzde gerek teknolojik gerekse bölgesel ve küresel gelişmeler karşısında ülkelerin karşı karşıya kaldığı güvenlik riskleri de aynı oranda artmaktadır. Teknolojinin gelişimi ile ortaya çıkan yeni nesil silah sistemleri ve siber tehditler karşısında askerî alanda sürekli olarak yeni stratejiler geliştirilmesi ve bunların bölgesel ve küresel değişkenler ile ele alınarak planlamaların yapılması

hayati bir durum haline gelmiştir. Diğer yandan yeni nesil silah sistemlerinin de yapay zekaya uyumlu olması beklenmektedir.

Proje hayata geçirildikten sonra stratejik karar alma sorumluluğu bulunan birimler için strateji oluşturma safhasında kullanabilecekleri yapay zekâ destekli bir ağ oluşturularak hızlı analiz kabiliyeti ile olası risk senaryolarının oluşturulduğu bir alan oluşturulacaktır. Aynı zamanda bu sistem üzerinden alınan kararlar hem operasyonel alandaki silah sistemlerine hem de yatay ve dikey düzlemdeki diğer komuta kademelerine bilmesi gereken prensibi doğrultusunda güvenli bir şekilde aktarılabilecektir.

Barış zamanı ise yapılan analizler sonucunda ortaya çıkan risk senaryolarına karşı birlikler kendi içlerinde ya da bölgesel olarak harp oyunları düzenleyebilecek bu da hem birliğin kabiliyetinin arttırılması hem de personelin eğitimi açısından faydalı olacaktır, aynı zamanda söz konusu senaryoların eşit seviyede birlikler ile de paylaşımının yapılması sonucunda tecrübe aktarımlarının da pozitif yönde etkileneceği aşikardır.

- **Kamu Kurumlarında Yapay Zekâ Stratejisi:**

Askerî alanda olduğu kadar kamu kurumlarında da risk yönetimi ve doğru strateji oluşturulması önemi bir millî güvenlik konusudur. Özellikle küresel ya da bölgesel seviyede etki alanı oluşturan doğal afetler (Deprem, Yangın, Su baskınları) ile pandemik ve endemik salgınların etkisi son dönemlerde derin yaralar açmıştır. Böyle zamanlarda kritik öneme haiz olan kamu kurumlarının (İtfaiye, arama-kurtarma ekipleri, sağlık kuruluşları, emniyet güçleri) oluşabilecek felaketlerden önce stratejik eylem planlarını sürekli olarak güncellemesi gerekmektedir.

Yaşanacak bahse konu doğa olayları esnasında oluşması beklenen kaos ortamlarında aynı

zamanda duygusal yapıya da sahip olan insanların hem hızlı bir şekilde analiz yapması hem de etkili bir karar alması kolay olmayacaktır.

Projenin hayata geçmesinden sonra yerel yönetimler tarafından sorumluluk bölgeleri ile ilgili verilerin ve kabiliyetlerinin girilmesi sonucunda sistem üzerinden olası risk senaryoları ve çözüm stratejileri oluşturulabilecek ve askerî alanda olduğu gibi bu analizler ve planlar operasyon birimlerinin yanı sıra merkezi yönetim ile de paylaşılabilecektir.

Sonuç olarak ülkece Millî bir güvenlik stratejisi oluşturulabilecek ve böylelikle personel ve teçhizat planlamaları daha planlı bir şekilde yapılabilecektir. Olası risk senaryoları üzerinden ise daha gerçekçi tatbikatlar yapılması sağlanarak toplumsal ve kamusal bilinçlenmenin önü açılacaktır.

## 2. Projenin Kapsamı

- Askerî ve Kamu kuruluşlarında yapay zekâ destekli strateji planlama ile küresel ve bölgesel bazdaki değişkenlere bağlı olarak risk senaryoları oluşturulması,
- Güncel harp oyunu senaryoları eşliğinde kurumsal farkındalık ve personel eğitimlerinin etkinliğinin arttırılması,
- Sistem sayesinde kurumlar arası veya üst ve yatay seviyedeki diğer karar alıcı birimlerle yetkilendirilmiş güvenli ve hızlı veri paylaşımı,
- Sistem üzerinden oluşturulacak stratejik kararların güvenli ağ üzerinden operatif noktalara iletiminin sağlanması,
- Birlikte çalışabilirlik kabiliyetine pozitif yönlü etki,

## 3. Projenin Hedef Kitlesi:

- Türk Silahlı Kuvvetleri,
- Merkezi ve Yerel yönetimler,
- Toplumun güvenliğinden sorumlu kuruluşlar (İtfaiye, Arama Kurtarma Ekipleri, Sağlık birimleri, Emniyet güçleri)

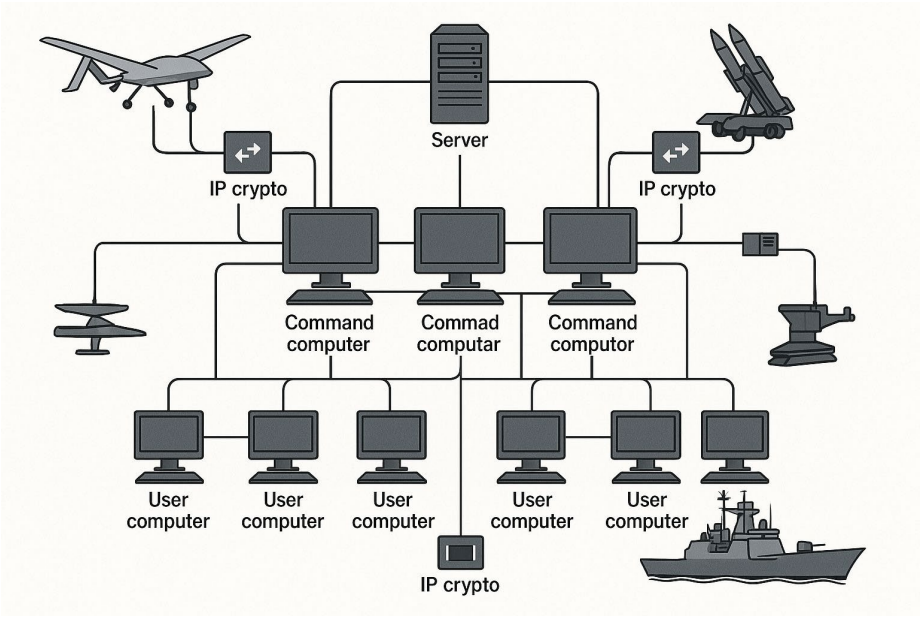
## 4. Projenin Yöntemi ve Çalışma Planı

- **Proje Eylem Planı:**

Projeyi hayata geçirmeyi planlayan kurumlarla beraber öncelikli olarak çalışma grubu oluşturulacak. Oluşturulan çalışma grubu ile beraber eylem planı belirlenerek projeye dahil edilmesi düşünülen firmalar belirlenecek. Sözleşme detayları da netleştirildikten sonra pilot uygulama noktalarının belirlenmesi yapılacak.

Proje öncesi işlemler üzerinde mutabakata varıldıktan sonra proje için tasarlanması planlanan stratejik seviye yetkilendirilmiş ağ sistemi için ilgili kurum isterleri doğrultusunda siber güvenlik ve kullanım kriterlerinin belirlenmesi sağlanacak. Aynı şekilde söz konusu sisteme dahil olması planlanan kullanıcı bilgisayarlarının da teknik kriterlerinin belirlenmesi sağlanacak.

Proje dahilinde söz konusu ağ sisteminin testlerinin yapılabilmesi adına yüklenici firma bünyesinde test alanının oluşturulması sağlanacak. Söz konusu ağın tamamlanması noktasında kullanıcı arayüzünün entegrasyonu ve siber güvenlik kriterlerinin de sürece dahil olması sağlanarak saha test aşamalarına geçiş sağlanacak.




**Tablo-1** Yapay Zeka Tabanlı Ağ Mimarisi(şematiktir)

Proje kabulü ile beraber sözleşme dahilinde ilgili kurumlara teknik ve eğitim alanlarında gerekli destek sağlanacak.

- **Proje Aşamaları:**

  - **Proje Başlangıcı (1 Ay)**

  **.** Yönetici grubu, Kilit paydaşlar ve Çalışma gruplarının oluşturulması ve görev tanımlamalarının yapılması **(2 Hafta)**

. Risk analizi çalışması ve sözleşmenin hazırlanması **(2 Hafta)**

- **Proje Ön Tasarım (2 Yıl)**

. Proje kapsamında kullanılması düşünülen yetkilendirilmiş ağın tasarımı **(3 Ay)**

. Siber güvenlik gereksinimlerinin belirlenmesi ve uygulama aşamasına geçilmesi **(6 Ay)**

. Yapay zekâ tabanlı ara yüz ön tasarım çalışması ve Deep Learning entegrasyonu **(1 Yıl)**

. Kullanıcı bilgisayarlarının isterlerinin belirlenmesi ve siber güvenlik/TEMPEST uyumlamalarının yapılması **(6 Ay)**

. Yetkili kullanıcı etkileşim alanlarının tanımlanması **(2 Ay)**

. Tüm süreçlerin tamamlanmasına müteakip ilk prototipin hazırlanması **(3 Ay)**

. İlk test ve sunum planlamasının yapılması **(1 Ay)**

. Kritik tasarım öncesi isterlerin belirlenmesi **(1 Ay)**

**Not:** Yukarıda bahsi geçen süreçlerden ilk beş sıradaki işlem maddesi eş zamanlı yürütülebileceği düşünüldüğünden Proje Ön Tasarım sürecinin 2 yıl süreceği düşünülmektedir.

- **Proje Son Tasarım ve Test Süreci (18 Ay)**

. Belirlenen isterler sonrası son tasarım sürecinin tamamlanması **(6 Ay)**

. Siber güvenlik test süreçlerinin başlatılması **(6 Ay)**

. Kurumlarda belirlenen bölgeler dahilinde pilot alanların kurulum aşaması **(3 Ay)**

. Yerinde test süreçlerinin icra edilmesi **(1 Ay)**

- **Proje Kapanış ve Teslim (1 Yıl)**

. Sözleşmede belirtilen kriterler doğrultusunda fabrika seviyesi test kriterlerinin yetkilendirilmiş kurul eşliğinde son testleri **(1 Ay)**

- İlgili kurumlardaki saha kurulumlarının yapılması ve saha test aşaması **(6 Ay)**
- Proje kabulünün gerçekleşmesi **(1 Ay)**
- Kullanıcı eğitimlerinin icrası **(3 Ay)**

## 5. Projeden Beklenen Sonuçlar

- Proje sonunda kullanıcılar kendi kabiliyetleri, çevresel faktörler, risk alanları (Karşı kuvvet, doğal felaketler) ve güncel veriler ışığında olası risk alanlarını görebilecek,
- Bu risk alanlarına strateji tasarımı yaparken söz konusu durumlar ile ilgili analizleri en hızlı ve doğru bir şekilde elde edebilecek,
- Olası risk alanları için çeşitli harp oyunu senaryoları üretebilecek,
- Analizleri yetkilendirilmiş stratejik ağ üzerinden yatay ve dikey seviyede diğer karar alıcı makamlarla anlık paylaşabilecek,
- Kurum içerisinde operatif seviyedeki diğer yapay zekâ tabanlı sistemlere görev tanımlaması yapabilecek,



## 6. Proje Bütçesi

- Personel Giderleri 216.000.000 TL (30 Personel – 4 Yıl)
- AR-GE Giderleri 1.000.000.000 TL
- Lojistik/Seyahat Giderleri 10.000.000 TL
- Ekipman/Malzeme Giderleri 100.000.000 TL

**Not:** Söz konusu bütçelendirme 10 kullanıcı tanımlı 2 farklı yerleşkede kullanım yeri olan bir tasarım için belirlenmiştir.

## 7. Riskler ve Önlemler

- **Risk**-1**:** Sistemin içeriğinde hassas bilgilerin dolaşması öngörüldüğünden bilgi güvenliği riski oluşturması,

**Öneri-**1: İçerdiği bilginin hassasiyetine bağlı olarak donanımsal ya da yazılımsal kripto kullanımı ve kullanılacak söz konusu cihazlar için uygun algoritma seçiminin yapılması ve böylelikle siber saldırılara karşı güçlü bir mimariye sahip olması,

- **Risk-**2: Sistem içerisinde dolaşan hassas bilginin içeriğine erişim yetkisi kriterlerinin belirsizliği nedeniyle oluşabilecek sorunlar,

**Öneri-**2: Sistem kurulumu esnasında "Zero Trust Security" kavramına bağlı olarak bir ağ oluşturulması ve bunun yanı sıra kullanıcı profil erişim ve düzenleme yetkisi kontrolünün birden fazla kişi onayı ile belirlenmesi,

- **Risk-**3: Analiz ve harp oyunu senaryolarındaki gerçekleme modellerinin uygulanabilirliği,

**Öneri-**3: Kullanıcı kurumların her birisinde farklı bir çalışma kültürünün olduğu göz önünde bulundurulduğunda senaryo ve analiz yapılarının her kullanıcı kurum için farklı bir şekilde sunulması beklenecektir. Bu ele alınan sorunun "Deep Learning" teknolojisi sayesinde kurumlara özel bir şekilde süreç içinde kendini geliştireceği düşünülmektedir.

## 8. Proje Süresi

Proje tamamlanma süresinin proje kabulünü takiben 4 yıl sonra kullanıma başlanacağı düşünülmektedir.

## 9. Değerlendirme Kriterleri

- Siber güvenlik önlemlerinin Bilgi ve İletişim Güvenliği Tedbirleri Yönergesine uygun olarak tasarlanması,
- Sistem tarafından oluşturulan strateji ve analizlerin gerçeklemeye uygun olarak sunulması,
- Tasarlanacak stratejik ağın bileşenlerinin en az %80 oranında yerli üretim olarak tasarlanması,
- Projenin kurum tarafından belirlenen kullanım kriterleri ile uyumlu olması,

- Sistem üzerinde depolanacak bilgiye ait kullanılması gereken sistemlerin kontrollü bölgelerde tesis edilmesinin sağlanması,
- Sistem mimarisinin "Zero Trust Security" politikasına uygun olarak tasarlanması ve kullanıcı profillerinin bilmesi gereken prensibi doğrultusunda yetki tanımlarının yapılabilmesinin sağlanması,
- Sistem tarafından oluşturulan yatay ve dikey seviyedeki diğer karar mekanizmalarına yetkilendirme politikası kapsamında paylaşımının yapılması,
- Kurumların kullanmış ya da kullanmayı planladığı diğer yapay zekâ tabanlı sistemler ile veri paylaşımının yapılabilmesi için uygun protokollerin sağlanması.

## 10. Sonuç

Proje, yapay zekâ destekli strateji planlamasıyla kurumsal farkındalığın artırılması, değişen küresel ve bölgesel dinamiklere göre risk senaryolarının oluşturulması ve karar alma süreçlerinin daha etkin hâle getirilmesini amaçlamaktadır. Ayrıca, güvenli veri paylaşımı ve stratejik kararların hızlı şekilde operatif birimlere iletilmesi sayesinde birlikte çalışabilirliğe önemli katkı sağlamaktadır.

Projenin hedef kitlesi; Türk Silahlı Kuvvetleri, merkezi ve yerel yönetimler ile toplumsal güvenlikten sorumlu kurumlar (itfaiye, arama-kurtarma ekipleri, sağlık birimleri ve emniyet güçleri) olarak belirlenmiştir. Bu yapılar için stratejik öngörü kabiliyetini güçlendirecek yenilikçi bir destek mekanizması sunulmaktadır.

## 11. Kaynakça


- **Zero Trust Security:**

- Assunção, P. (2019, January, 16-16). A zero trust approach to network security, Proceedings of the Digital Privacy and Security Conference. Portugal, 65-72. https://doi.org/10.11228/dpsc.01.01.00

- Bicakci, K., Uzunay, Y. & Khan, M. (2021, December, 2-3). Towards zero trust: the design and ımplementation of a secure end-point device for remote working, 14th International Conference on Information Security and Cryptology, Ankara, Türkiye, 28-33. https://doi.org/10.1109/iscturkey53027.2021.9654298

- Camphell, M. (2020). Beyond zero trust: Trust is a vulnerability. Computer, 53(10), 110-113. https://doi: 10.1109/MC.2020.3011081

- **Deep Learning:**

- Kunihiko Fukushima, Neocognitron: A Self-organizing Neural Network Model for a Mechanism of Pattern Recognition Unaffected by Shift in Position, 1980, Biol. Cybernetics 36, pp. 193-202.

- Xavier Glorot, Antoine Bordes, and Yoshua Bengio, Deep Sparse Rectifier Neural Networks, 2011, Proceedings of the 14th International Conference on Artificial Intelligence and Statistics, vol. 15 of JMLR. Pp. 315-323.

- **Yapay Zekâ:**

- İyigün, N. Ö. (2021). Yapay Zekâ ve Stratejik Yönetim. TRT Akademi, 6(13), 675-679. https://doi.org/10.37679/trta.1002518

- Al-Suqri, M. N., and Gillani, M. (2022). A Comparative Analysis of Information and Artificial Intelligence Toward National Security. IEEE Access, 10, 64420-64434.

- Boutin, B. (2022). State Responsibility in Relation to Military Applications of Artificial Intelligence. Leiden Journal of International Law, 36(1), 133-150. https://doi.org/10.1017/s0922156522000607