YAPAY ZEKÂ ÇAĞINDA SİBER GÜVENLİK VE TÜRKİYE'NİN STRATEJİK ÖNCELİKLERİ

RA-POR

NİSAN 2026

Milli İstihbarat Akademisi

YAPAY ZEKÂ ÇAĞINDA SİBER GÜVENLİK
VE TÜRKİYE'NİN STRATEJİK ÖNCELİKLERİ

RAPOR / NİSAN 2026

Milli İstihbarat Akademisi

Milli İstihbarat Akademisi

Telif

Yayın Tarihi: Nisan 2026

Millî İstihbarat Akademisi
E-Posta: bilgi@mia.edu.tr

"Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 5'inci maddesinin 2'nci fıkrası çerçevesinde bandrol taşıması zorunlu değildir."

RAPOR / Nisan 2026

YAPAY ZEKÂ ÇAĞINDA SİBER GÜVENLİK VE TÜRKİYE'NİN STRATEJİK ÖNCELİKLERİ

İÇİNDEKİLER

İNFOGRAFİK

GRAFİK

ŞEKİL

TABLO

KISALTMALAR

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
BDM	Büyük Dil Modeli
BT	Bilişim Teknolojileri
CISA	ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı
DDoS	Dağıtık Hizmet Engelleme Saldırısı
ENISA	Avrupa Birliği Siber Güvenlik Ajansı
ML	Makine Öğrenmesi
NATO	Kuzey Atlantik Antlaşması Örgütü
NIS2	AB Ağ ve Bilgi Sistemleri Direktifi 2
NIST	ABD Ulusal Standartlar ve Teknoloji Enstitüsü
OECD	Ekonomik İşbirliği ve Kalkınma Örgütü
OT	Operasyonel Teknolojiler
OWASP	Açık Web Uygulama Güvenliği Projesi
SCADA	Denetleyici Kontrol ve Veri Toplama Sistemi
SGB	Siber Güvenlik Başkanlığı
SOME	Siber Olaylara Müdahale Ekibi
UNICRI	Birleşmiş Milletler Bölgelerarası Suç ve Adalet Araştırmaları Enstitüsü
USOM	Ulusal Siber Olaylara Müdahale Merkezi
YZ	Yapay Zekâ

ÖN SÖZ

Dijital teknolojilerde yaşanan hızlı gelişmeler, güvenlik anlayışını ve risk ortamını derinden dönüştürmektedir. Bu dönüşümün merkezinde yer alan yapay zekâ; kamu yönetiminden özel sektöre, kritik altyapılardan gündelik hizmet süreçlerine kadar geniş bir alanda yeni imkânlar sunmaktadır. Verimlilik artışı, hız, otomasyon ve karar destek kapasitesi gibi önemli avantajlar sağlayan bu teknoloji, aynı zamanda yeni güvenlik açıklarını da beraberinde getirmektedir. Özellikle siber tehditlerin; niteliği, kapsamı ve etkisi, yapay zekâ uygulamalarının yaygınlaşmasıyla birlikte daha karmaşık bir hâle gelmiştir.

Günümüzde siber güvenlik, yalnızca teknik sistemlerin korunmasıyla sınırlı bir mesele değildir. Veri güvenliği, kurumsal süreklilik, kamu hizmetlerinin aksamadan yürütülmesi, toplumsal güvenin korunması ve ulusal kapasitenin güçlendirilmesi gibi çok boyutlu unsurları da içermektedir. Dolayısıyla yapay zekâ destekli siber tehditler; yönetişim, kurumsal koordinasyon, hukuk, insan kaynağı ve stratejik planlama başlıklarıyla birlikte değerlendirilmesi gereken stratejik bir konu olarak öne çıkmaktadır.

Tüm bunlar göz önünde bulundurulduğunda yapay zekâ destekli tehditlerin ortaya çıkardığı yeni risk alanlarının, büyük dil modeli tabanlı sistemlerin güvenlik boyutunun, kritik altyapılar üzerindeki etkilerinin, kurumsal karar alma süreçlerine yönelik olası tehditlerin ve Türkiye açısından öne çıkan yapısal ihtiyaçların değerlendirilmesi elzemdir. Bu rapor da teknik ayrıntıları stratejik bir çerçeveye yerleştirerek konuya ilişkin daha net, anlaşılır ve uygulanabilir bir değerlendirme sunmayı amaçlamaktadır.

Bugün esas ihtiyaç, teknolojik gelişmelere uyum sağlamak kadar söz konusu gelişmelerin doğurabileceği riskleri önceden görmek ve gerekli kurumsal tedbirleri zamanında almaktır. Bu çerçevede Türkiye'nin önünde duran temel görev, dijital dönüşümü desteklerken güvenlik, düzenleme, koordinasyon ve insan kaynağı alanlarında eş zamanlı bir ilerleme sağlamaktır. Bu ilerlemenin; kamu kurumları, özel sektör, akademi ve sivil toplumu kapsayan güçlü bir güvenlik ekosistemiyle desteklenmesi büyük önem taşımaktadır.

RA -
POR

Çalışmanın, ortak bir kavramsal zemin oluşturarak politika geliştirme süreçlerine ve kurumsal hazırlık kapasitesine katkı sunması amaçlanmaktadır. Raporun hazırlanmasında emeği geçen tüm uzmanlara teşekkür eder; çalışmanın, ülkemizin çıkarları doğrultusunda daha hazırlıklı, daha dirençli ve daha bütüncül bir güvenlik yaklaşımının geliştirilmesine katkı sağlamasını temenni ederim.

Prof. Dr. Talha Köse
Millî İstihbarat Akademisi Başkanı

YÖNETİCİ ÖZETİ

- Yapay zekâ (YZ), siber güvenlik alanında yeni bir araç olmanın ötesine geçerek saldırı ölçeğini, savunma hızını ve düzenleyici gereksinimleri aynı anda dönüştüren stratejik bir güç çarpanı hâline gelmiştir. Bu nedenle konu, teknik güvenlik önlemlerin yanında ulusal kapasite, yönetişim ve stratejik hazırlık meselesi olarak da ele alınmalıdır.
- YZ; kamu, özel sektör ve kritik altyapılara hızla girmektedir. Güvenlik, denetim ve yönetişim mekanizmaları ise aynı hızda gelişmemekte; bu durum da verimlilik artışıyla birlikte kırılganlıkları ve dijital bağımlılığı büyütmektedir.
- Saldırgan YZ kullanımı; akıllı oltalama, derin sahte içerik üretimi, hedefe özel sosyal mühendislik ve otomatik keşif faaliyetleri üzerinden saldırı maliyetini düşürmekte ve tehditlerin ölçeklenmesini kolaylaştırmaktadır. Bu durum, görece sınırlı kapasiteye sahip aktörlerin dahi daha etkili, daha ikna edici ve daha yoğun saldırılar düzenleyebilmesini mümkün kılmaktadır.
- Hasmane YZ kullanımı kapsamında, YZ sistemlerini doğrudan hedef alan adversarial (çekişmeli) saldırılar; veri zehirleme, model çıkarımı, üyelik çıkarımı, tersine mühendislik ve hassas bilgi ifşası gibi yöntemleri içermektedir. Bu tür saldırılar model performansını bozmakla kalmaz, aynı zamanda karar destek sistemlerini yanıltarak kurumsal süreçleri saptırabilir ve güven kaybına da yol açabilir.
- Büyük dil modeli (BDM) tabanlı sistemler; istem enjeksiyonu, güvensiz çıktı işleme, hassas bilgi sızıntısı, tedarik zinciri zafiyetleri, aşırı yetki ve aşırı güven gibi yeni riskler üretmektedir. Bu riskler; veri yönetişimi, denetim, hesap verebilirlik ve kurumsal karar kalitesi sorunları olarak değerlendirilmelidir.
- YZ destekli siber tehditlerin etkisi yalnızca teknik sistemlerle sınırlı değildir. Bu tehditler; ulusal güvenlik, kritik altyapılar, kurumsal kapasite ve toplumsal güven üzerinde doğrudan sonuç üretmektedir. Özellikle derin sahte ve sentetik medya; bilgi ekosistemini bozma, kurumsal meşruiyeti aşındırma ve kriz anlarında kamu güvenini zayıflatma potansiyeli taşımaktadır.
- Türkiye açısından öncelikli risk alanları; enerji, finans, telekomünikasyon, savunma tedarik zinciri ve kamu dijitalleşmesi başlıklarında yoğunlaşmaktadır. Bu sektörlerdeki yüksek dijital

bağlılık, YZ destekli tehditlerin operasyonel süreklilik, karar kalitesi ve dış teknoloji bağımlılığı üzerinde daha ağır etkiler üretmesine neden olmaktadır.

- YZ çağında en büyük risk, teknolojiye erişim eksikliğinden ziyade yönetişim, koordinasyon, insan kaynağı ve veri/model yönetimi eksikliğidir. Bu nedenle etkili yanıt; daha fazla teknoloji yatırımının yanında daha güçlü kurumsal çerçeve, daha net sorumluluk zinciri ve daha sıkı denetim mekanizmaları gerektirmektedir.
- Kısa vadede öncelik, merkezî koordinasyonun güçlendirilmesi ve YZ envanterinin çıkarılmasıdır. Sistemlerin; veri, yetki ve dış bağımlılıkları görünür hâle getirilmelidir. BDM ve ajan tabanlı sistemler için asgari güvenlik kuralları belirlenmelidir.
- Orta vadede öncelik; standart, denetim ve sektörel dayanıklılık mekanizmalarının kurumsallaştırılmasıdır. Kamu alımları, kayıt tutma, olay raporlama ve tedarik güvenliği şartları netleştirilmelidir. Siber Olaylara Müdahale Ekibi (SOME) yapılanması ve tehdit istihbaratı paylaşımı güçlendirilmelidir.
- Uzun vadede hedef, dış teknoloji bağımlılığını yönetebilen güçlü bir ulusal kapasite oluşturmaktır. Test, sertifikasyon, denetim ve uzman insan kaynağı kapasitesi geliştirilmelidir. Yerli ekosistem ile toplumsal farkındalık birlikte güçlendirilmelidir.

GİRİŞ

Yapay zekâ (YZ) destekli siber tehditler; siber güvenliği, yeni araçlar ve saldırı türlerinin yanında saldırı maliyeti, savunma hızı, karar süreçleri ve teknoloji bağımlılıkları üzerinden de dönüştürmektedir. Bu dönüşüm, konuyu klasik bilgi güvenliği tartışmasının ötesine taşımaktadır. Ulusal güvenlik, kurumsal dayanıklılık, kamu hizmetlerinin sürekliliği ve toplumsal güven; bu yeni risk alanının temel unsurlarıdır.

Günümüzde tartışmanın odağı, YZ'nin yalnızca yeni tehditler üretmesi değildir. Asıl mesele; kamu kurumları, özel sektör ve kritik altyapıların YZ'yi iş süreçlerine hızla entegre etmesine rağmen güvenlik, denetim ve yönetişim mekanizmalarının bu dönüşüme aynı hızda eşlik edememesidir. Bu durum, verimlilik artışı ile yeni kırılganlıkların eş zamanlı büyümesine yol açmaktadır. **Bu nedenle YZ destekli siber riskler; regülasyon, veri yönetişimi, tedarik zinciri güvenliği, insan denetimi ve kurumsal koordinasyon boyutlarıyla birlikte ele alınmalıdır.**

Devletlerin ve kurumların; enerji, sağlık, ulaşım, bankacılık, telekomünikasyon ve kamu hizmetleri gibi kritik işlevleri giderek daha fazla dijital altyapıya dayanmaktadır. Dijitalleşme arttıkça saldırı yüzeyi de genişlemektedir. Buna bağlı olarak siber tehditlerin ulusal güvenlik üzerindeki etkisi daha görünür hâle gelmektedir. Son yıllarda YZ'deki hızlı gelişme, bu tabloyu daha da değiştirmiştir. Nitekim YZ; artık yalnızca verimlilik sağlayan bir araç olmaktan çıkıp saldırıları hızlandıran, sosyal mühendisliği güçlendiren, karar destek sistemlerini etkileyen ve dış teknoloji sağlayıcılarına bağımlılığı artıran stratejik bir etken hâline gelmiştir. Bu nedenle YZ çağında siber güvenlik; yönetişim, düzenleme, denetim ve stratejik özerklik başlıklarıyla birlikte değerlendirilmelidir.

Söz konusu dönüşümün bugün daha kritik hâle gelmesinin birkaç nedeni vardır. İlk olarak YZ artık sınırlı kullanım alanlarında kalan deneysel bir teknoloji değildir. Kamu kurumları, özel sektör şirketleri ve kritik altyapı işletmecileri; üretken YZ, BDM'ler, karar destek sistemleri ve otomatik analiz araçlarını giderek daha fazla kullanmaktadır. İkinci olarak tehdit ortamı hızla değişmektedir. Akıllı oltalama, derin sahte içerikler, sentetik kimlikler ve hedefe özel saldırılar; tehditlerin daha hızlı ve daha ölçekli hâle gelmesine neden olmaktadır. Üçüncü olarak saldırı yüzeyi artık yalnızca ağlar, cihazlar ve uygulamalarla sınırlı değildir. Veri, model, bağlam, çıktı işleme, eklenti, ajan ve bulut katmanları

da bu yüzeyin parçası hâline gelmiştir. Son olarak YZ kullanımı hızla artarken veri sınıflandırması, insan denetimi, kayıt tutma ve üçüncü taraf bağımlılıklarının yönetimi gibi temel mekanizmalar aynı hızda gelişmemektedir.

Bahsi geçen gelişmeler, siber güvenliğin temel mantığını da değiştirmektedir. Geleneksel yaklaşım; daha çok yetkisiz erişimi engellemek, ağları korumak ve sistemleri yedeklemek üzerine kuruluydu. YZ çağında ise güvenlik; modele hangi verinin girdiği, modelin hangi bağlamda çalıştığı, hangi kararlara etki ettiği ve çıktılarının nasıl doğrulandığı gibi unsurları da kapsamaktadır. Bu nedenle esas mesele, siber alanın işleyiş mantığının değişmesidir. Saldırılar; daha otomatik, daha kişiselleştirilmiş ve daha ikna edici hâle gelmektedir. Buna karşılık savunma tarafında; daha fazla görünürlük, daha güçlü denetim ve daha etkili koordinasyon ihtiyacı doğmaktadır.

Türkiye açısından bu dönüşüm daha da önemlidir. Kamu dijitalleşmesinin yaygınlaşması, e-Devlet uygulamalarının genişlemesi, kritik altyapıların dijital bağımlılığı, finansal sistemlerin yoğun bağlantılı yapısı ve savunma sanayisi tedarik zincirinin hassasiyeti riskleri artırmaktadır. Bu nedenle YZ destekli siber tehditler; teknik açıkların yanında kamu hizmetlerinde aksama, kurumsal karar kalitesinde zayıflama, bilgi ekosisteminde manipülasyon, toplumsal güven kaybı ve dış teknoloji bağımlılığının derinleşmesi gibi sonuçlar da üretmektedir.

Türkiye açısından temel risk; YZ'nin yeni saldırı araçları üretmesinden çok kamu dijitalleşmesi, kritik altyapılar ve kurumsal karar süreçleri üzerinde dış bağımlılık ve denetim zafiyeti yaratmasıdır. Bu risk; veri egemenliği, kurumsal koordinasyon, kriz yönetimi ve ulusal hazırlık kapasitesi ile doğrudan ilişkilidir. **Bu nedenle çözüm sadece daha fazla teknoloji yatırımı yapmak değildir. Asıl ihtiyaç; kurumlar arası koordinasyonu güçlendirmek, veri ve model yönetişimini netleştirmek, insan denetimini sistematik hâle getirmek, yüksek riskli alanlarda hesap verebilirlik mekanizmaları kurmak ve kritik tedarik bağımlılıklarını stratejik düzeyde yönetmektir.**

Bu rapor, YZ destekli siber tehditleri yalnızca teknik ayrıntı düzeyinde değil; ulusal güvenlik, kurumsal kapasite, regülasyon ve stratejik özerklik boyutlarıyla da ele almaktadır. Raporun amacı, bu risklerin Türkiye açısından doğurduğu stratejik sonuçları ortaya koymak ve politika önceliklerini belirlemektir.

BÖLÜM 1

YAPAY ZEKÂ VE SİBER ALANIN DÖNÜŞÜMÜ

Yapay zekâ (YZ), siber alanı birçok farklı bağlamda ve köklü bir biçimde dönüştürmektedir. Bu noktada söz konusu dönüşümü analiz ederken yeni tehdit türlerini sıralamaktan çok bu dönüşümün güvenlik ortamını nasıl yeniden şekillendirdiğini ortaya koymak gerekmektedir.

Bu doğrultuda altı kritik başlık öne çıkmaktadır:

- **Otomasyon ve Ölçek:** YZ'nin en belirgin etkilerinden biri, saldırı süreçlerini hızlandırmasıdır. Hedef seçimi, açık kaynak taraması, sahte içerik üretimi ve saldırı planlaması artık daha kısa sürede yapılabilmektedir. Bu durum, saldırıların daha düşük maliyetle ve daha geniş ölçekte yürütülmesini kolaylaştırmaktadır. Bu değişim, yalnızca güçlü aktörlere avantaj sağlamamaktadır. Sınırlı kapasiteye sahip aktörler de daha etkili kampanyalar yürütebilmektedir. Sonuç olarak savunma tarafı; daha sık, daha hızlı ve daha uyarlanabilir tehditlerle karşı karşıya kalmaktadır.
- **Karar Süreçlerine Etki:** YZ başlangıçta daha çok destek aracı olarak kullanılmaktaydı. Bugün ise birçok kurumda doğrudan karar süreçlerini etkileyen bir katman hâline gelmiştir. Tehdit önceliklendirme, olay analizi ve risk değerlendirmesi gibi alanlarda YZ çıktıları giderek daha fazla önem kazanmaktadır. Bu gelişme verimlilik sağlayabilir. Ancak karar desteği ile karar verme arasındaki sınır her zaman açık değildir. İnsan onayı, sorumluluk ve denetim kuralları netleşmezse teknik kolaylık yönetişim açığına dönüşebilir.
- **Saldırı Yüzeyinin Genişlemesi:** YZ, siber güvenlikte korunması gereken alanları genişletmektedir. Artık yalnızca ağlar, cihazlar ve uygulamalar değil; veri kümeleri, modeller, eğitim süreçleri, istemler, eklentiler, vektör veri tabanları ve bulut servisleri de risk alanına dâhildir. Bu nedenle güvenlik değerlendirmesi daha kapsamlı yapılmalıdır. Modele hangi verinin girdiği, modelin hangi sistemlerle entegre olduğu ve ürettiği çıktının nerede kullanıldığı önem taşımaktadır. Güvenlik; erişim kontrolü meselesi olmanın ötesine geçerek veri, model ve uygulama zincirinin birlikte yönetilmesini gerektirmektedir.
- **Saldırgan ve Savunan Arasındaki Dengenin Değişmesi:** Siber alanda saldırgan ile savunan arasında her zaman bir asimetri olmuştur. YZ, bu farkı daha görünür hâle getirmektedir. Saldırganlar düşük maliyetle içerik üretebilmekte, hedefe özel manipülasyon yapabilmekte ve saldırılarını hızlı biçimde çoğaltabilmektedir. Savunma tarafında ise durum daha farklıdır. YZ sistemlerinin güvenli biçimde kullanılması için test, kayıt tutma, denetim, insan onayı ve hukuki uyum gerekmektedir. Bu nedenle saldırı tarafı daha hızlı hareket ederken savunma tarafı daha kontrollü ilerlemek zorunda kalmaktadır.
- **Bilgi Ekosistemi ile Siber Alanın Etkileşimi:** YZ, siber güvenliği teknik alanın dışına taşımaktadır. Bilgi manipülasyonu, sentetik medya, otomatik propaganda ve dezenformasyon faaliyetleri artık siber risk ortamının bir parçası olarak değerlendirilmelidir. Bir saldırının etkisi yalnızca sistemleri durdurmakla sınırlı kalmamakta; kurumsal güveni, kriz iletişimini ve toplumsal algıyı da etkileyebilmektedir. Bu durum; özellikle kamu kurumları, seçim süreçleri, finansal güvenlik ve kritik hizmetler açısından önemlidir. YZ ile üretilen sahte içerikler; yanlış bilgi yayabilir, kurumsal

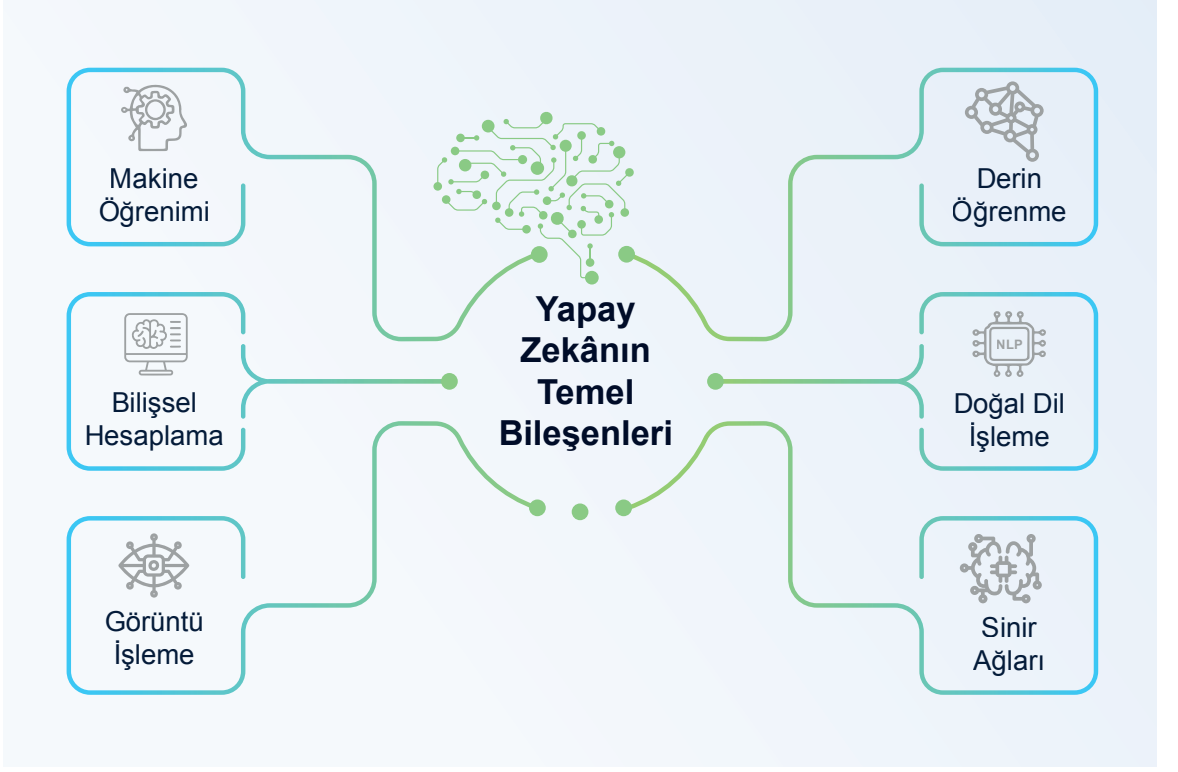
otoriteyi taklit edebilir ve toplumsal güveni zedeleyebilir. Bu nedenle bilgi doğrulama kapasitesi, siber güvenliğin tamamlayıcı unsuru hâline gelmiştir.

- **Bağımlılık ve Stratejik Etki:** YZ'nin bir diğer önemli etkisi, teknoloji bağımlılıklarını artırmasıdır. YZ sistemleri; veri, model, yazılım kütüphanesi, bulut altyapısı, işlem gücü ve dış servis sağlayıcıları gibi çok katmanlı bileşenlere dayanmaktadır. Bu bileşenler, sınırlı sayıda aktörde toplandığında, güvenlik riski yalnızca teknik düzeyde kalmamaktadır. Özellikle kritik altyapılar ve kamu sistemleri için bu bağımlılıkların stratejik sonucu vardır. Verinin dış bulutta işlenmesi, sistem kayıtlarına erişimin sınırlı olması veya güncelleme süreçlerinin dış aktörlerce belirlenmesi, kurumsal kontrolü zayıflatabilir. Bu nedenle YZ çağında güvenlik, aynı zamanda dijital egemenlik ve kriz anında süreklilik meselesidir.

Bu dönüşüm, siber güvenliğin artık yalnızca teknik savunma araçlarıyla ele alınamayacağını göstermektedir. Daha geniş, daha disiplinli ve yönetişim odaklı bir yaklaşım gerekmektedir.

İnfografik 1'de YZ'nin temel bileşenleri görülmektedir. Sanayi 4.0 ile dijitalleşme, otomasyon ve ağ bağlantılı sistemlerde büyük ilerlemeler sağlanmıştır. Ancak bu gelişmeler, siber saldırı yüzeyini de genişletmiş ve YZ temelli saldırıların artmasına neden olmuştur.[1] Siber güvenlik perspektifinden YZ'yi; hasmane YZ kullanımı, saldırgan YZ kullanımı ve savunma amaçlı YZ kullanımı olmak üzere üç ana kategoriye ayırmak mümkündür.[2]

İnfografik 1: Yapay Zekânın Temel Bileşenleri

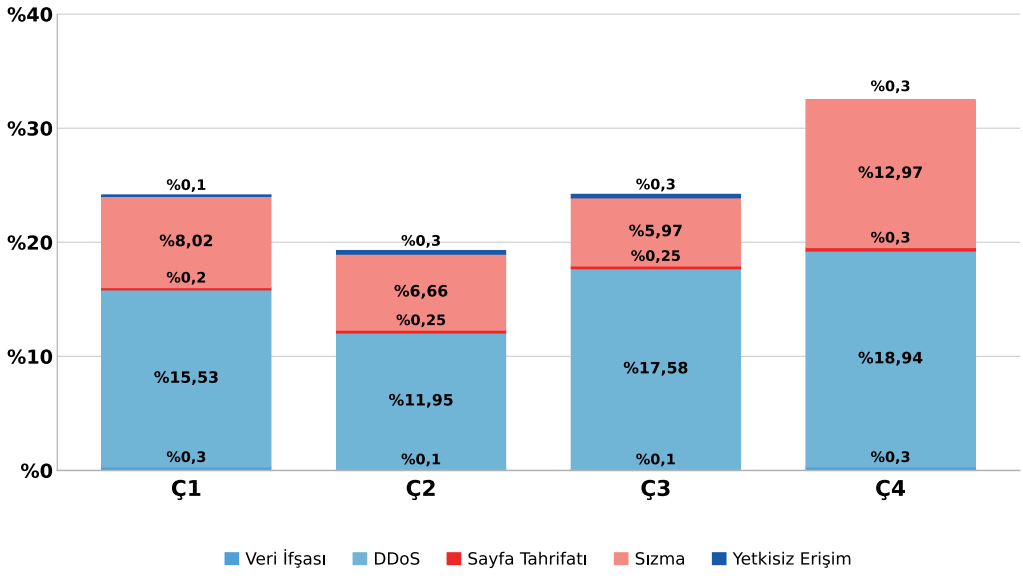


Saldırgan YZ kullanımının stratejik etkisi, saldırı kalitesini tek başına yükseltmesinden çok saldırı maliyetini düşürüp ölçeği büyütmesinden kaynaklanır. Sonuç olarak saldırgan YZ kullanımı, siber tehdit ortamını daha yoğun, daha hızlı uyarlanan ve daha ikna edici hâle getirmektedir.[3] Bu tehdidin en görünür biçimlerinden biri YZ destekli sosyal mühendisliktir. 2025 itibarıyla YZ destekli oltalama saldırıları küresel sosyal mühendislik saldırılarının büyük bölümünü oluşturmaktadır. BDM'ler; daha ikna edici e-postalar, ses oltalama senaryoları ve sahte içerikler üretmek için kullanılmaktadır. Üretken BDM'lerin ses klonlama ve yüz değiştirme araçlarının; oltalama, sesli oltalama ve taklit saldırılarında kullanımının katlanarak artacağı öngörülmektedir.[4]

Hasmane YZ kullanımı, YZ'nin bir saldırı aracı olarak kullanılmasından farklı olarak doğrudan modelin kendisini hedef almaktadır. Bu kapsamda amaç; kararları yanıltmak, performansı düşürmek, gizli verileri çıkarmak veya modeli ele geçirmektir.[5] ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) bu alanı; veri zehirleme, girdi manipülasyonu, model çıkarımı, üyelik çıkarımı, tersine mühendislik ve gizlilik ihlalleri gibi başlıklarda sınıflandırmaktadır.[6] Söz konusu riskler, motivasyon sahibi düşmanların kasıtlı eylemleri olarak tanımlanmakta olup özellikle kimlik doğrulama, anomali tespiti, içerik filtreleme, otonom karar desteği ve kritik altyapı izleme gibi alanlarda ciddi sonuçlar doğurabilmektedir.

MITRE ATLAS da hasmane YZ kullanımı kapsamında, YZ sistemlerine yönelik adversarial saldırıları; gerçek dünya saldırı gözlemleri ve güvenlik araştırmalarına dayanan, savunma ekiplerinin tehdit modellemelerine dâhil etmesi gereken bir tehdit alanı olarak ele alır.[7] Bu saldırı türü; özellikle kamu kurumları ve kritik altyapılarda karar destek sistemlerini yanıltabilir, modelin beslendiği veri ortamını bozabilir ve model davranışı üzerinden hassas bilgi sızıntısına yol açabilir.[8] Grafik 1'de 2024 yılında Avrupa Birliği'nde (AB) kamu kurumlarını hedef alan saldırıların dağılımı verilmiştir.

Grafik 1: 2024 Yılında AB'de Kamu Yönetimi Sektörüne Yönelik Tehdit Dağılımı



Kaynak: ENISA.

Savunma amaçlı YZ ise siber güvenlikte tehdit tespiti, anomali analizi, erken uyarı ve otomatik müdahale için kullanılan YZ uygulamalarını ifade etmektedir.[9] NIST siber güvenlik çerçevesine göre bu kullanım; tanımlama, tespit, koruma, tepki ve iyileştirme başlıkları altında ele alınmaktadır.[10] Ağ trafiğini, erişim örüntülerini ve kullanıcı davranışlarını analiz ederek olağan dışı hareketleri belirleyebilir. Bu alanda; erişim doğrulama, ağ ve davranış izleme, anormal trafik tespiti gibi konularda önemli ilerlemeler sağlanmıştır.[11] İnfografik 2'de YZ'nin savunma amacıyla kullanım alanları görülmektedir.

İnfografik 2: Siber Güvenlikte Yapay Zekâ Araçlarının Savunma Amaçlı Kullanımı

BÖLÜM 2

YAPAY ZEKÂ VE YENİ TEHDİT MANZARASI

Bölüm 1'de anlatılanlar göz önüne alındığında, söz konusu dönüşümün getirdiği risk ve tehditler kurumsal ve stratejik sonuçları bakımından analiz edilmelidir. Nitekim tehditleri; ikna ve kimlik manipülasyonu, otomasyon ve ölçeklenme, model bütünlüğü ve veri güvenliği, kritik altyapı ve hizmet sürekliliği, kurumsal karar alma süreçlerine sızma olmak üzere beş ana kümeye ayırmak mümkündür. BDM temelli riskler ise bu kümelerin birden fazlasını kesen yatay bir risk alanı olarak ele alınmalıdır. Böylece hangi riskin hangi kurumsal sonucu ürettiği görünür kılınabilir.

İkna ve Kimlik Manipülasyonu Tehditleri

Bu tehdit kümesi; saldırganın hedef sistemi doğrudan teknik olarak sömürmesinden önce insanı, kurumsal güven ilişkisini ve kimlik doğrulama zincirini manipüle etmesini ifade etmektedir. Akıllı oltalama, derin sahte ses ve görüntüler, sentetik kimlikler, sahte yönetici talimatları ve hesap devralma girişimleri bu başlık altında yer alır.

OpenAI'ın 2025 tarihli kötüye kullanım raporu; bazı aktörlerin ChatGPT'yi kullanarak sahte öz geçmiş üretimi, ABD merkezli görünen personel kimlikleri oluşturma, iş başvurularını otomatikleştirme ve uzaktan çalışma süreçlerini manipüle etme girişimlerini belgelemektedir. Rapora göre aktörler yalnızca sahte profil üretmekle kalmamış, aynı zamanda şirket tarafından çalışanlara tahsis edilen dizüstü bilgisayarlara uzaktan erişimi kolaylaştıracak yöntemler ve araçlar hakkında da model desteği kullanmıştır.[12]

Yine ABD Federal Soruşturma Bürosu, Mayıs ve Aralık 2024'te yayımladığı kamu uyarılarında, suçluların üretken yapay zekâyı (YZ) kullanarak daha inandırıcı e-postalar, sesli/video mesajlar, sahte sosyal medya profilleri ve dolandırıcılık siteleri ürettiklerini belirtmiştir.[13] Buna göre YZ, dil hatalarını azaltarak ve içeriği kişiselleştirerek dolandırıcılık şemalarının inandırıcılığını artırmakta ve aynı zamanda suçluların daha geniş kitlelere daha kısa sürede ulaşmasına olanak tanımaktadır.

Buradaki temel dönüşüm, saldırının artık sadece kandırmaya değil, ikna ve inandırmaya dayanmasıdır. Üretken YZ sayesinde saldırılar; daha iyi kurgulanmış, hedefe özel, zamanlaması daha doğru ve bağlama daha uygun hâle gelmektedir. Bu durum; kimlik doğrulama, yönetici onayı, tedarikçi iletişimi veya vatandaş ile kurum temas noktaları gibi güvene dayalı süreçleri daha kırılgan hâle getirmektedir. Finans sektöründe sosyal mühendislik saldırılarının kişisel/kurumsal veri hırsızlığına, dolandırıcılığa ve büyük ölçekli finansal suçlara yol açtığını gösteren AB Siber Güvenlik Ajansı (ENISA) değerlendirmeleri, bu tehdidin yalnızca bireysel kullanıcı sorunu olmaktan çıktığını ve kurumsal risk boyutuna ulaştığını ortaya koymaktadır.[14]

Akıllı oltalama saldırılarında sosyal medya ve e-postalar üzerinden hedefin davranışları analiz edilerek kişiye özel sahte mesajlar üretilir. Temel motivasyon, kimlik bilgileri ve finansal verileri ele geçirmektir. Derin sahte saldırıları ise bir kişinin, yüzü veya sesinin YZ ile taklit edilerek gerçekte söylemediği ya da yapmadığı şeyleri yapıyormuş gibi gösterilmesidir. Üst düzey bir yöneticinin sesinin taklit edilerek büyük ölçekli dolandırıcılıkta kullanılmasıyla güvenlik boyutu daha görünür hâle gelmiştir.[15] Bu nedenle akıllı oltalama ve derin sahte saldırılarının yalnızca farkındalık eğitimiyle ele alınması mümkün değildir.

Bu saldırılar; kurumsal savunma, kimlik doğrulama mimarisi, işlem onayı tasarımı, tedarikçi iletişim güvenliği, kamu iletişimi doğrulama protokolleri ve sentetik medya doğrulama kapasitesiyle ilişkilidir. Özellikle kamu kurumları, kritik hizmet işletmecileri ve finansal kuruluşlar açısından bu tehditler, toplumsal güveni ve kurumsal meşruiyeti aşındırabilecek niteliktedir.[16]

Otomasyon ve Ölçeklenme Tehditleri

Bu tehdit kümesi; YZ'nin saldırıları daha hızlı, daha ucuz ve daha geniş ölçekte yürütülebilir hâle getirmesiyle ilgilidir. Kötü amaçlı yazılımların uyarlanması, zafiyet tarama süreçlerinin otomasyonu, botnet koordinasyonu, dağıtık hizmet engelleme saldırısının (DDoS) optimize edilmesi ve eş zamanlı sosyal mühendislik kampanyaları bu sınıfta yer almaktadır.

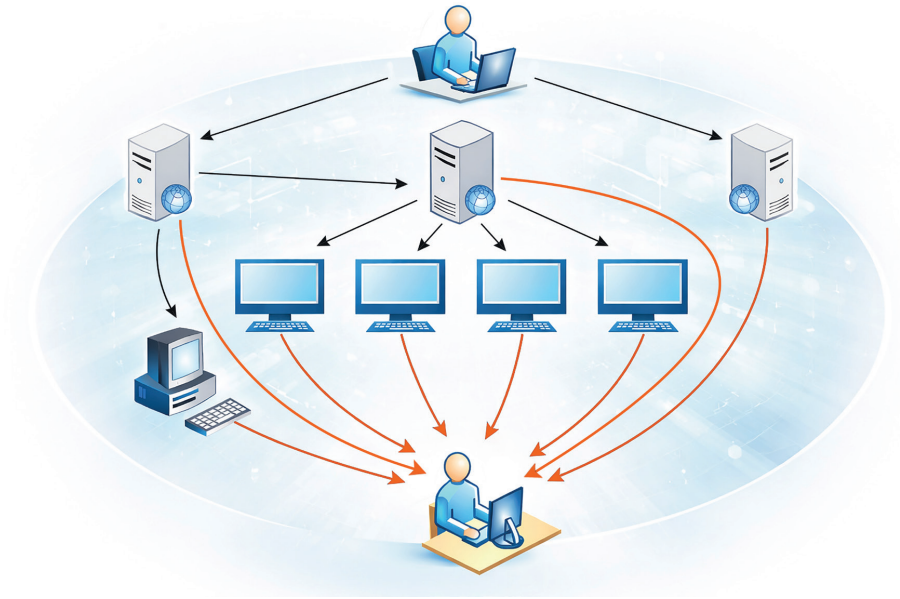
Buradaki temel değişim, saldırganların daha zeki olmasından çok operasyonel olarak daha ölçekli hareket edebilmesidir. Kötü amaçlı yazılımlar artık yalnızca bulaşan kod şeklinde değil; hedefe göre davranışını değiştiren, tespitten kaçınan ve dağıtımını optimize eden saldırı zincirlerinin parçası olarak ortaya çıkmaktadır. Benzer şekilde DDoS ve hizmet bozma saldırıları da trafik hacmi sorunu olmaktan çıkıp uygun hedefi ve zayıf noktayı seçebilen otomatik kampanyalara dönüşmektedir.[17] Bu nedenle otomasyon ve ölçeklenme tehditlerine karşı sadece uç nokta koruma yeterli değildir. Artık merkezî görünürlük, hızlı yama disiplini, davranışsal analiz, oran sınırlama, otomatik sınıflandırma ve ihtiyaç durumuna göre kontrollü otomatik müdahale mekanizmaları gerekmektedir. Bu noktada kurumlar, YZ'yi güvenli biçimde benimserken aynı zamanda YZ'nin saldırı yüzeyini genişletebileceklerini göz önünde bulundurmalıdır. Bu sebeple kritik altyapılarda dayanıklılık odaklı yaklaşım ön plana çıkmaktadır.[18]

OpenAI,[19] bazı tehdit aktörlerinin YZ'yi; komut dosyalarını uyarlama, sistem yapılandırmalarında hata ayıklama, port tarama araçları geliştirme, FTP'ye yönelik kaba kuvvet saldırısı betikleri hazırlama ve BDM'leri ağ keşif ve tarama aracı çıktılarıyla birlikte kullanarak sızma testi benzeri iş akışlarını otomatikleştirme amacıyla kullandığını göstermektedir. Bu kullanım hem teknik keşif hem de sosyal medya otomasyonu gibi farklı fazlara yayılmıştır.

Söz konusu tehditler, kimlik doğrulama alanında da etkilidir. CAPTCHA aşma, parola tahmini, kaba kuvvet saldırılarının hız kazanması ve tuş kaydedici zararlı yazılımların kullanımı; kullanıcı adı-parola temelli sistemleri daha kırılgan hâle getirmektedir. Bu nedenle çok faktörlü kimlik doğrulama, güçlü parola politikaları, şifre yöneticileri ve biyometrik doğrulama gibi kontroller öne çıkmakta ve YZ destekli biyometrik sistemler de anormal erişimlerin tespitine katkı sağlamaktadır.[20]

Kurumsal açıdan savunma ekipleri artık tekil olay mantığıyla değil, yüksek hacimli ve hızlı uyarlanan saldırı kampanyaları mantığıyla hareket etmek zorundadır. Yalnızca uç nokta koruma yeterli değildir. Merkezî görünürlük, hızlı yama disiplini, davranışsal analiz, oran sınırlama, otomatik sınıflandırma ve ihtiyaç hâlinde kontrollü otomatik müdahale mekanizmaları gereklidir. YZ tabanlı anomali tespiti ve saldırı tespit sistemleri; özellikle DDoS, fidye yazılımı ve kötü amaçlı yazılım tespitinde giderek daha etkili hâle gelmektedir.[21] Şekil 1'de DDoS saldırılarının yapısı gösterilmektedir.

Şekil 1: DDoS Saldırı Örneği



Model Bütünlüğü ve Veri Güvenliği Tehditleri

Bu tehdit kümesi, YZ sistemlerinin kendini hedef alan saldırılar ile bu sistemleri besleyen veri, model ve entegrasyon katmanlarına yönelik riskleri kapsamaktadır. Veri zehirleme, model çıkarımı, üyelik çıkarımı, tersine mühendislik, model hırsızlığı, hassas bilgi ifşası ve istem enjeksiyonu bu başlık altında değerlendirilir. NIST[22] ile MITRE ATLAS[23] yaklaşımları; bu saldırıları veri, model, platform ve çevre katmanları üzerinden sistematik biçimde sınıflandırmaktadır.

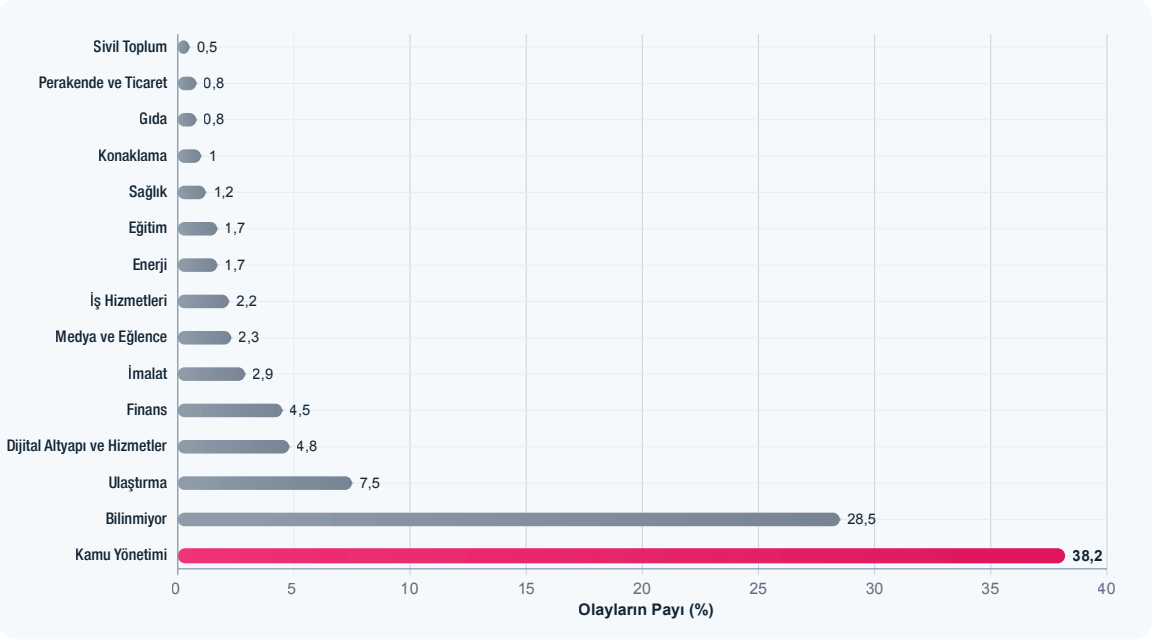
Eğitim verisi veya kurumsal bilgi tabanı manipüle edildiğinde model yanlış kararlar üretebilir. **Hassas bilgi ifşası ise kurumsal sırların ve stratejik bilgilerin dışa taşınmasına yol açabilir. Bu tehdidin sonucu ise yanlış tahminle sınırlı değildir. Asıl kritik sonuçlar; yanlış yönlendirilmiş kurumsal işlem, veri sızıntısı, hatalı güvenlik kararı ve güven kaybıdır.** Bu nedenle veri kaynağı doğrulaması, model yaşam döngüsü denetimi, giriş/çıkış filtreleme, kayıt tutma ve üçüncü taraf model/eklenti denetimi temel yönetişim ihtiyacı hâline gelmektedir.

Kritik Altyapı ve Hizmet Sürekliliği Tehditleri

Kritik altyapılar açısından YZ destekli tehditler, yalnızca bilişim teknolojileri (BT) sistemlerinin ihlal edilmesi anlamına gelmemektedir. Bu tehditler; enerji, telekomünikasyon, ulaşım, finans ve kamu hizmetleri gibi alanlarda operasyonel süreklilik, emniyet ve toplumsal istikrar üzerinde doğrudan sonuç üretebilir. Grafik 2, siber saldırıların sektörel bazda dağılımını göstermektedir. DDoS, Operasyonel Teknolojiler (OT)/Denetleyici Kontrol ve Veri Toplama Sistemi (SCADA) ortamlarına dolaylı etki, yanlış alarm üretimi, bakım ve arıza sınıflandırmasında manipülasyon, tedarik zinciri üzerinden kritik

sistemlere sızma ve YZ ile desteklenen hizmet bozma kampanyaları bu kümede yer almaktadır. MITRE'nin kritik altyapılar için YZ siber riskini azaltma ilkeleri; YZ'nin ölçek ve hız nedeniyle fiziksel zarar, mülkiyet kaybı ve çevresel etkiler doğurabileceğini vurgulamaktadır.[24] ABD Siber Güvenlik ve Altyapı Güvenliği Ajansının (CISA) kritik altyapı ve YZ odaklı yaklaşımı da YZ entegrasyonlarının güvenli yapılmaması hâlinde yeni kırılganlıklar doğurabileceğini ve dayanıklılık odaklı güvenlik tasarımı gerektiğini belirtmektedir.[25] Bu nedenle kritik altyapı ve hizmet sürekliliği tehditleri, siber güvenliği klasik BT güvenliği çerçevesinden çıkararak sistemin; doğru çalışması, doğru karar destek üretmesi ve kriz anında dış bağımlılıklar nedeniyle devre dışı kalmaması gibi önlemleri içeren bir noktaya getirmektedir. **Hizmet sürekliliği; artık veri bütünlüğü, model güvenilirliği, tedarik zinciri güvenliği ve insan-YZ iş bölümü ile bir arada düşünülmelidir.**

Grafik 2: 2025 Yılında AB'de Gerçekleşen Siber Saldırıların Sektörel Dağılımı



Kaynak: ENISA.

Kurumsal Karar Alma Süreçlerine Sızma Tehditleri

En kritik dönüşümlerden biri, YZ destekli tehditlerin doğrudan kurumsal karar alma süreçlerine sızabilmesidir. **Burada saldırı, sistemleri kapatmak veya veri çalmak kadar kurumu yanlış karar almaya, yanlış önceliklendirme yapmaya veya yanlış güven ilişkileri kurmaya zorlamak şeklinde ortaya çıkmaktadır.**[26] BDM tabanlı asistanların manipüle edilmesi, güvenlik operasyon merkezlerinde üretilen özetlerin yanlış yönlendirilmesi, sahte risk raporları, tedarik ve satın alma süreçlerinde hatalı öneri üretimi, personel süreçlerinde YZ çıktısına aşırı güven ve ajan tabanlı YZ sistemlerine gereğinden fazla yetki verilmesi bu başlık altında değerlendirilmektedir.

Söz konusu tehdit alanında teknik zafiyet, hızla yönetişim açığına dönüşmektedir. Aşırı yetki verilmiş bir ajan tabanlı YZ, yanlış bağlamla işlem başlatabilir. Aşırı güvenilen BDM çıktısı, denetlenmeden kurumsal akışa girebilir ve yanlış veriyle beslenen bir karar destek sistemi, güvenlik veya operasyon önceliklerini bozabilir. Sonuç olarak tehdit, kurumun teknik varlıklarından çok karar kalitesini ve denetim zincirini hedef alır.[27]

Kurumsal karar alma süreçlerine sızma tehditleri bu nedenle siber güvenlik ekipleriyle birlikte üst yönetim, hukuk, uyum, iç denetim ve diğer birimlerin de konusu olmalıdır. Çünkü burada korunan şey; yalnızca ağ veya veri değil kurumsal muhakeme, hesap verebilirlik ve işlem bütünlüğüdür. Tablo 1'de tüm saldırı türlerinin sınıflandırılması verilmiştir.

Birleşmiş Milletler Bölgelerarası Suç ve Adalet Araştırmaları Enstitüsü (UNICRI);[28] derin sahte teknolojisinin içerik manipülasyonu başta olmak üzere işletmeleri, finans birimlerini ve güvene dayalı iş süreçlerini istismar etmek için de giderek daha elverişli hâle geldiğini vurgulamaktadır. Aynı rapor, YZ'nin CAPTCHA atlatma, hedefli manipülasyon ve kurumsal süreçlerde sahte güven oluşturma gibi alanlarda kötüye kullanım potansiyeline dikkat çekmektedir.

Tablo 1: Yapay Zekâ Destekli Siber Tehdit Türlerinin Analitik Sınıflandırması

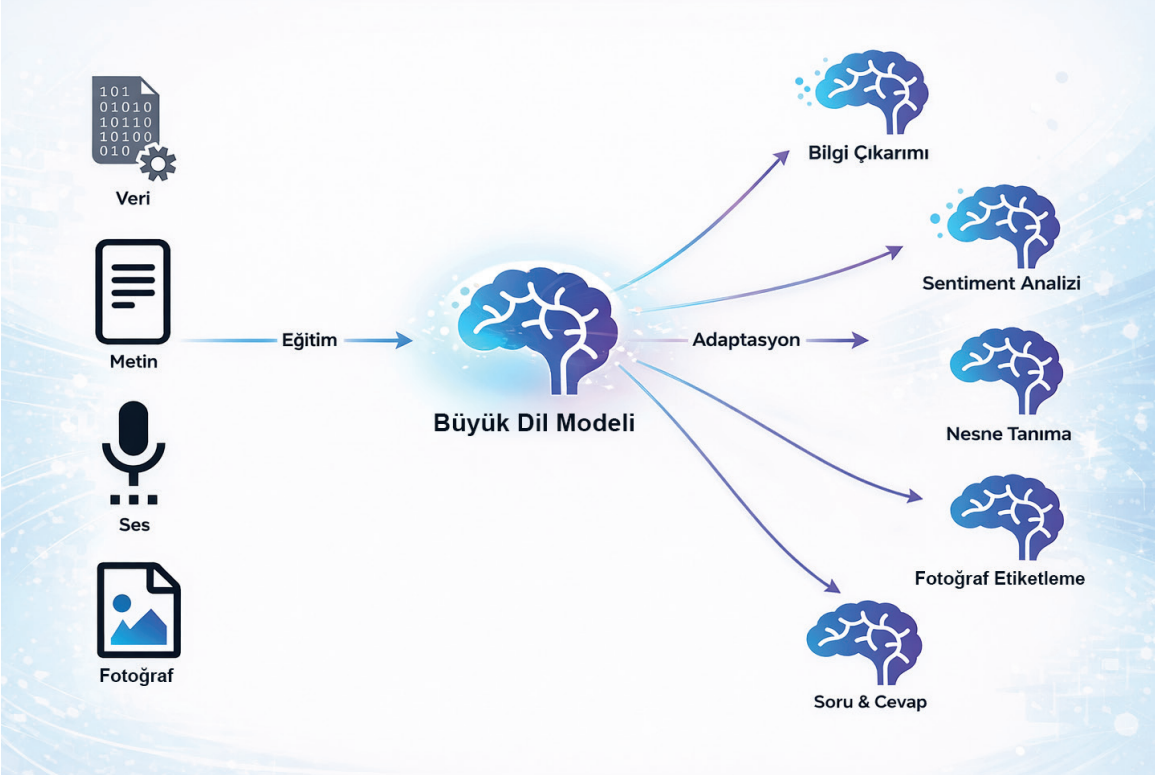
Saldırı/Tehdit Türü	Ana Kategori
YZ destekli oltalama	İkna ve kimlik manipülasyonu tehditleri
Derin sahte içerik	İkna ve kimlik manipülasyonu tehditleri
Kötü amaçlı yazılım	Otomasyon ve ölçeklenme tehditleri
Fidye yazılımı	Kritik altyapı ve hizmet sürekliliği tehditleri
Kimlik bilgisi doldurma yoluyla hesap ele geçirme	İkna ve kimlik manipülasyonu tehditleri
CAPTCHA aşma/otomatik kimlik doğrulama atlatma	Otomasyon ve ölçeklenme tehditleri
Dağıtık hizmet engelleme saldırısı	Kritik altyapı ve hizmet sürekliliği tehditleri
Botnet tabanlı saldırılar	Otomasyon ve ölçeklenme tehditleri
Veri zehirleme	Model bütünlüğü ve veri güvenliği tehditleri
Model hırsızlığı	Model bütünlüğü ve veri güvenliği tehditleri
Üyelik çıkarımı	Model bütünlüğü ve veri güvenliği tehditleri
İstem enjeksiyonu	Kurumsal karar alma süreçlerine sızma tehditleri
Hassas bilgi ifşası	Model bütünlüğü ve veri güvenliği tehditleri
Aşırı yetki/aşırı otonomi	Kurumsal karar alma süreçlerine sızma tehditleri
Aşırı güven	Kurumsal karar alma süreçlerine sızma tehditleri
Tedarik zinciri zafiyeti/tedarik zinciri ihlali	Model bütünlüğü ve veri güvenliği tehditleri
Anomali tespit sistemlerinin manipülasyonu	Model bütünlüğü ve veri güvenliği tehditleri
Otomatik güvenlik yanıtlarının suistimali	Kurumsal karar alma süreçlerine sızma tehditleri

BÖLÜM 3

BÜYÜK DİL MODELLERİ VE GÜVENLİK RİSKLERİ

BDM'ler, her ne kadar yapay zekâ (YZ) tehditleri bağlamında değerlendirilebilecek olsa da analiz edilmesi gereken alan hem yetenek hem de tehdit bağlamında oldukça farklı, geniş ve derindir. Bu sebeple diğer tehdit başlıklarından ayrışmaktadır. Nitekim bu modeller; soru yanıtlama, içerik üretme, çeviri, özetleme ve kod yazma gibi çok çeşitli görevleri yerine getirebilen oldukça güçlü üretken YZ sistemleridir. İnfografik 3'te BDM'lerin genel yapısı görülmektedir. Bu modeller; kurumsal iş akışlarına hızla entegre oldukça veri güvenliği, yönetişim ve karar kalitesi açısından da yeni riskler doğurmaktadır.[29]

İnfografik 3: Büyük Dil Modeli Genel Yapısı

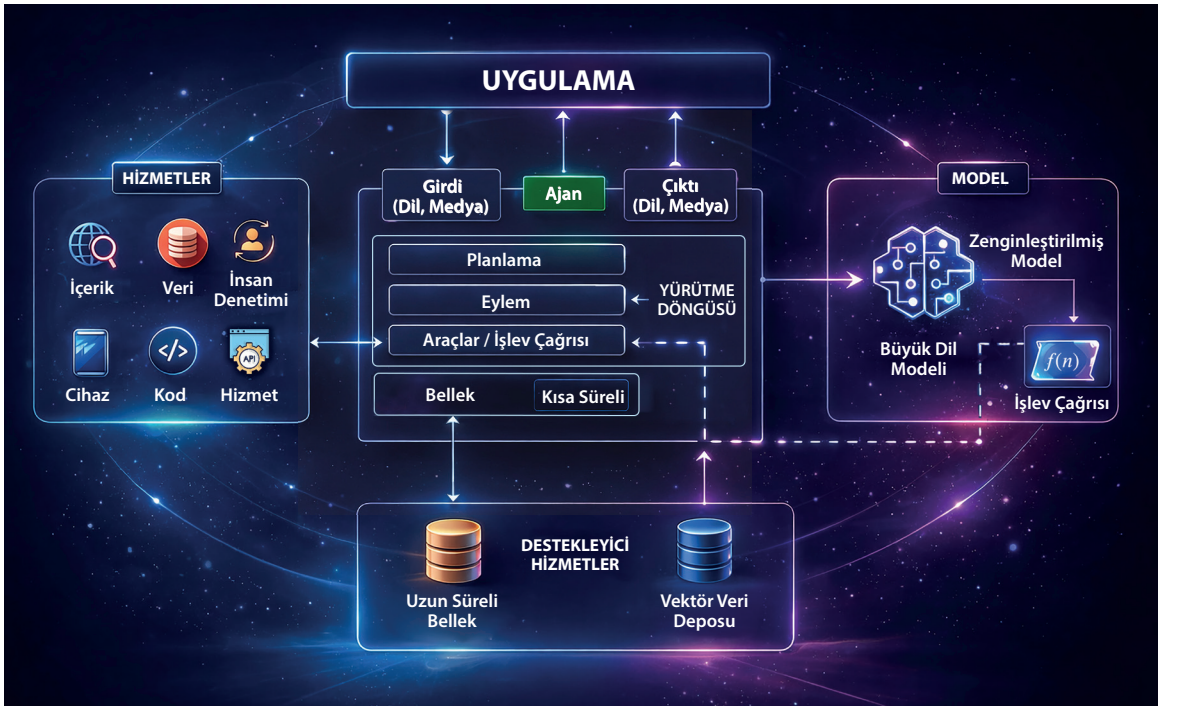


Bahsi geçen riskler arasında; özellikle istem enjeksiyonu, hassas bilgi ifşası, tedarik zinciri zafiyetleri, güvensiz çıktı işleme, aşırı yetki ve modele aşırı güven öne çıkmaktadır.[30] Bu nedenle BDM güvenliği, tüm uygulama ekosistemi ve yaşam döngüsü boyunca ele alınması gereken bir konudur.

BDM'lerin; kamu hizmetlerinden savunma tedarikine, kritik altyapılardaki yardımcı YZ asistanları ve ajan tabanlı YZ uygulamalarından kurumsal bilgi işleme süreçlerine kadar giderek daha fazla karar, erişim ve iş akışına bağlanmasına İnfografik 4 ve 5'te gösterilen ajan tabanlı YZ sistemleri örnek gösterilebilir. İnfografiklerde de görüleceği üzere ajan tabanlı YZ sistemleri; model kullanımı, veri tabanı, hafıza kullanımı, vektör veri tabanı, dış sistemler ile entegrasyon gibi birden fazla saldırı yüzeyine sahiptir.[31]

BDM riskleri üç düzlemde okunmalıdır. Birinci düzlem; modelin manipüle edilmesi, yanlış çıktı üretmesi veya hassas bilgiyi açığa vurması gibi operasyonel risklerdir. İkinci düzlem; iş akışlarının, tedarik süreçlerinin ve karar destek mekanizmalarının güvenli olmayan biçimde BDM'lere bağlanması gibi kurumsal risklerdir. Üçüncü düzlem ise kamu kurumlarının, kritik altyapı işletmecilerinin ve savunma tedarik zincirlerinin dış modellere, dış bulut altyapılarına ve denetlenemeyen üçüncü taraf bileşenlere bağımlı hâle gelmesi gibi stratejik risklerdir.[32]

İnfografik 4: Tek Ajanlı Mimari

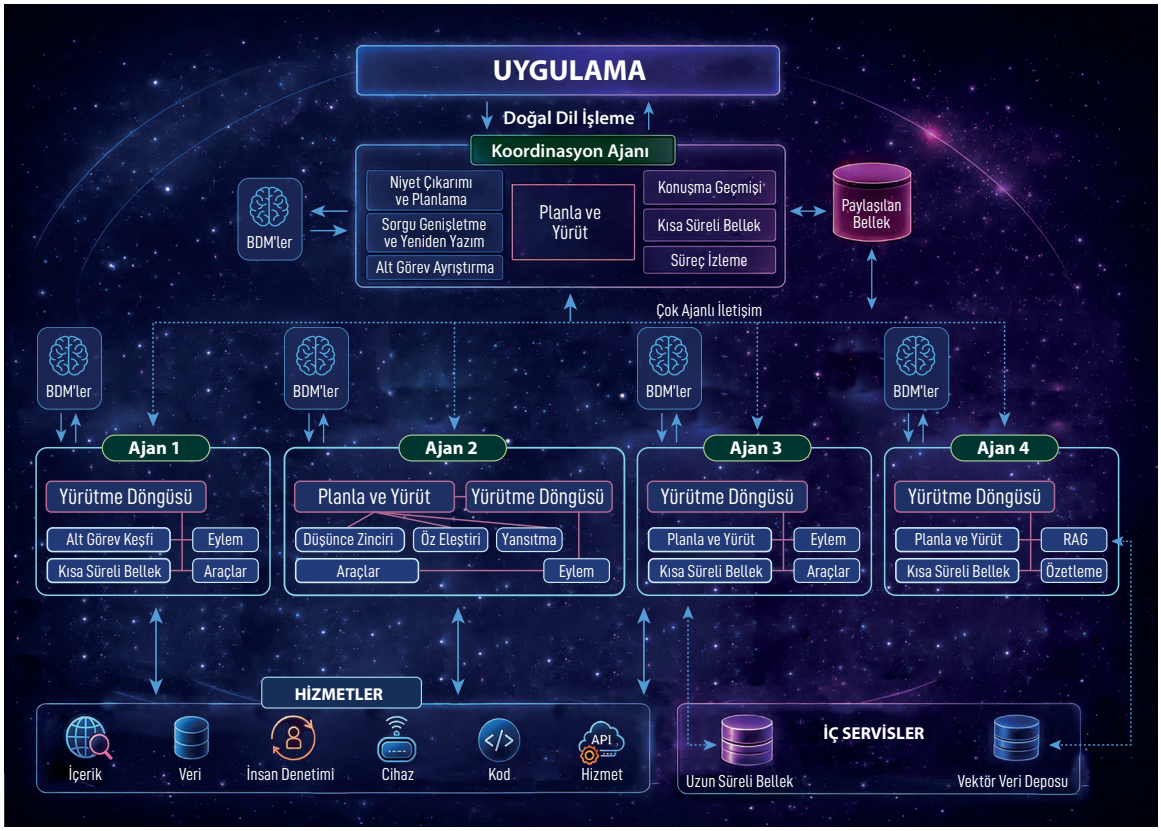


Kaynak: OWASP.

Kamu sektöründe, YZ'nin verimlilik ve duyarlılık sağlama potansiyeli olduğu ancak şeffaflık eksikliği ve hatalı otomasyonun hesap verebilirliği zayıflatabileceği, Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) tarafından açık biçimde belirtilmektedir.[33] Örneğin İnfografik 6'da yapısı gösterilen istem enjeksiyonu saldırıları; doğrudan idari hata, kamu hizmetinin bozulması ve kurumsal hesap verebilirlik sorunu üretmektedir.

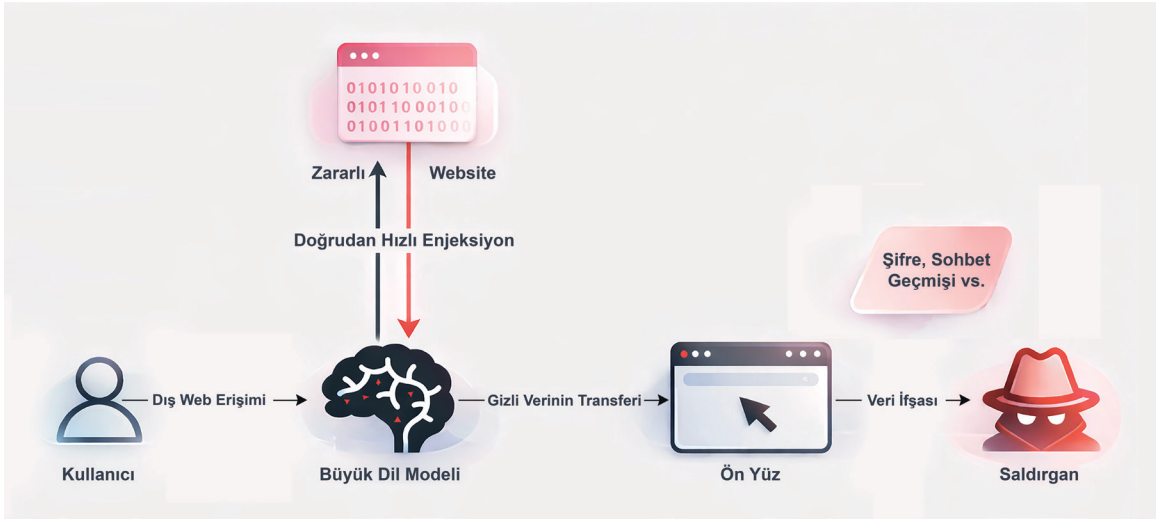
Hassas bilgi ifşası, kamu kurumlarında ve savunma tedarik süreçlerinde çok daha yüksek etki doğurmaktadır. Kurum içi belgelerin, tedarik tekliflerinin, teknik çizimlerin, kullanıcı kayıtlarının veya kritik altyapı operasyon verilerinin dış BDM servislerine taşınması; veri sızıntısı dışında, egemenlik ve tedarik zinciri güvenliği sorunları da yaratmaktadır. Kurumsal sonuç açısından bu risk; veri koruma ihlali, tedarik gizliliğinin kaybı, güvenlik soruşturması gerektiren sızıntılar ve kamu güveninin aşınması anlamına gelmektedir.[34]

İnfografik 5: Çok Ajanlı Mimari



Kaynak: OWASP.

İnfografik 6: İstem Enjeksiyonu Saldırısı Örneği



Kurum; hangi verinin modele girebileceğini, hangi verinin dış servise çıkamayacağını, hangi çıktının kayıt altına alınacağını ve hangi kullanımın yasak olduğunu netleştirmeden BDM kullanımını genişletirse veri güvenliği denetim dışına çıkacaktır.

Tedarik zinciri zafiyetleri, savunma sanayisi ve kritik altyapılar için belki de en stratejik BDM risklerinden biridir. Açık Web Uygulama Güvenliği Projesi'ne (OWASP) göre bu risk, yazılım bağımlılıklarının ötesine uzanmaktadır. Haricî veri kaynakları, açık kaynak modeller, ince ayar veri setleri, eklentiler ve üçüncü taraf bulut altyapıları; tedarik zincirinin temel bileşenleri arasında yer almaktadır. Bu yapı, zafiyetlerin farklı düzlemlerde ortaya çıkmasına neden olmaktadır. Modele aktarılan veriler manipüle edilebilir. Dış hizmet sağlayıcılar yetkisiz erişime maruz kalabilir. Güncellemeler arka kapı veya davranış değişikliği yaratabilir. Hizmet sürekliliği tek taraflı biçimde kesintiye uğrayabilir ve denetim izi zayıflayabilir. OWASP, bu tür bağımlılıkların; eğitim verisinin, modellerin ve dağıtım platformlarının bütünlüğünü zedeleyebileceğini açıkça ortaya koymaktadır.

Savunma tedarik süreçlerinde; BDM destekli sözleşme analizi, teklif karşılaştırma, teknik gereksinim türetme veya lojistik destek planlaması gibi kullanım örnekleri düşünüldüğünde, dış modele veya dış aracı bileşene aşırı bağımlılık hem bilgi sızıntısı hem de manipülasyon riskini büyütmektedir. Böyle bir bağımlılık, hassas ihale verilerinin üçüncü taraf sistemlere açılması, model çıktılarının belirli tedarikçileri avantajlı gösterecek şekilde sapması, teknik gereksinimlerin yanlış türetilmesi veya operasyonel planlamanın hatalı önceliklendirilmesi gibi sonuçlar doğurabilir. OECD'nin YZ altyapısında bulut bilişim yoğunlaşmasına ilişkin bulguları, bu tür bağımlılıkların yalnızca teknik bir mesele olmadığını, aynı zamanda pazar gücü ve stratejik özerklik meselesi olduğunu da göstermektedir.

Veri ve model zehirleme, eğitim verilerinin manipüle edilerek ve araya kötü niyetli veriler eklenerek modelin yanlış eğitilmesidir. Özellikle kurum içi veri tabanlarıyla beslenen yardımcı YZ asistanı ve getirim artırılmış üretim mimarilerinde kritik hâle gelmektedir.[35] Kritik altyapılarda bakım önerisi veren yardımcı YZ asistanı, arıza sınıflandırması yapan ajan tabanlı YZ sistemleri veya olay müdahalesine destek olan BDM araçları yanlış veriyle beslendiklerinde operasyonel riske dönüşebilir.[36]

OECD;[37] YZ'nin kamu verimliliği, duyarlılığı ve hesap verebilirliği artırma potansiyelini kabul ederken bunun veri yönetimi, dijital altyapı, beceri ve yönetişim ön koşullarına bağlı olduğunu vurgulamaktadır. Bu bağlamda OWASP riskleri kamu kurumlarında üç yönetişim sorusunu beraberinde getirmektedir: **Birincisi, karar destek ile karar verme arasındaki sınır nedir? İkincisi, vatandaş ve kurum verisi hangi kurallarla modele açılabilir? Üçüncüsü, yanlış ya da manipüle edilmiş bir BDM çıktısının sorumluluğu kimdedir? Bu sorular yanıtlanmadan BDM'lerin kamu süreçlerine yayılması, verimlilikten çok kurumsal kırılganlık üretme riski taşır.**

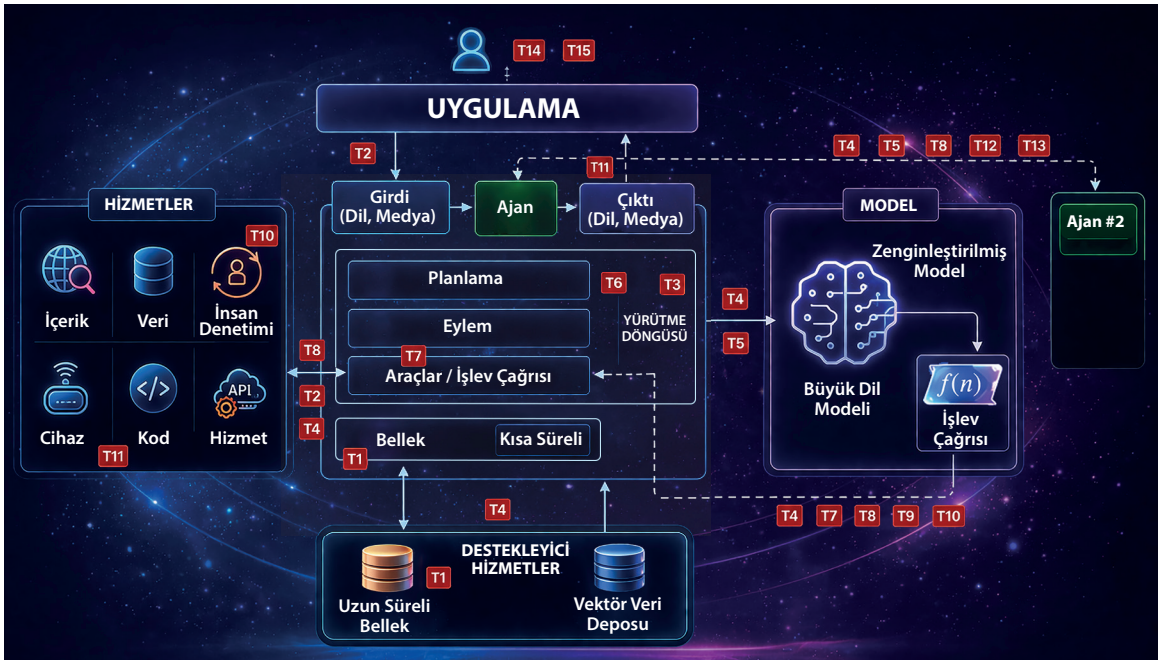
Kritik altyapılarda BDM tabanlı yardımcı YZ asistanları ve ajan tabanlı YZ uygulamalarının yayılması, tehdit manzarasını niteliksel olarak değiştirmektedir. Enerji, telekomünikasyon, ulaşım veya kamu hizmetlerinde yardımcı YZ asistanları; operatörlere arıza açıklaması, olay özeti, bakım önerisi veya belge bazlı karar desteği verebilir. Ajan tabanlı YZ ise belirli koşullarda eylem zincirleri başlatabilir, görev planlayabilir veya farklı sistemler arasında veri taşıyabilir.[38] Bu nedenle kritik altyapılarda BDM riski, doğrudan emniyet ve hizmet sürekliliği sorunu üretmektedir. Yetki sınırları doğru tanımlanmamış

bir yardımcı YZ asistanı ve ajan tabanlı YZ düzeni; yanlış alarmları büyüterek operatörleri yanıltabilir, yanlış bakım veya yanlış izolasyon kararlarını tetikleyebilir. NIST'e göre modelin görev içindeki rolü, insanın onay düzeyi, veri sınırları ve durdurma mekanizmaları net değilse risk katlanır. Bu nedenle kritik altyapılarda BDM tabanlı sistemler genel amaçlı ofis asistanı gibi değil, kontrollü yüksek riskli dijital bileşen olarak yönetilmelidir.

Aşırı yetki, BDM'lere karar alma süreçleri üzerinde, özellikle kritik uygulamalarda, çok fazla kontrol verilmesi anlamına gelmektedir. Bir modelin uygun kontroller olmadan yüksek riskli kararlar aldığı finansal işlemlerin otomatikleştirilmesi buna örnek verilebilir. Modelin karar alma yeteneklerini sınırlamak ve insan denetimini kritik süreçlere dâhil etmek bu riski azaltmak için önemlidir. Örneğin, bir kuruluş yasal belge taslağı için bir BDM'ye aşırı güvenebilir ancak model hata yapabilir veya kritik bilgileri atlayabilir. **Geri dönüş mekanizmaları uygulamak ve BDM'leri birincil karar vericiler yerine yardımcı araçlar olarak kullanmak, bu açığı azaltmaya yardımcı olabilir.** Yönetişim açısından bunun riski, yetki devrinin nerede başlayıp nerede durduğunun belirsiz olmasıdır. Böyle bir durumda hata veya kötüye kullanım yalnızca teknik bir arıza olmaktan çıkıp denetim zincirinin kopması anlamına da gelir. Bu nedenle aşırı yetki riski; kurum içinde rol tabanlı yetki, insan onayı, acil durdurma mekanizması ve işlem günlüğü zorunluluğuyla yönetilmelidir.

Aşırı güven, model çıktısının doğrulanmadan iş süreçlerine aktarılmasıdır. Kamuda bu durum; yanlış idari işlem, savunma tedarikinde yanlış değerlendirme, kritik altyapıda yanlış operasyon önerisi anlamına gelmektedir. Bu nedenle BDM'lere ilişkin riskler bütüncül bir tehdit mimarisi içinde ele alınmalıdır. İnfografik 7, bu mimarinin genel görünümünü ve tehditleri göstermektedir. Tablo 2 ise İnfografik 7'de gösterilen başlıca tehditleri ve bunlara karşı öngörülen temel önlemleri özetlemektedir.

İnfografik 7: Detaylı Tehdit Modeli



Tablo 2: Büyük Dil Modeli Tehditleri

Tehdit No.	Tehdit Adı	Tehdit Açıklaması	Önlemler
T1	Bellek Zehirleme	Bellek zehirleme, bir YZ ajanının kısa ve uzun süreli bellek sistemlerini istismar ederek zararlı veya yanlış veri enjekte etmeyi ve ajanının bağlamını sömürmeyi ifade eder. Bu durum, karar alma süreçlerinin değişmesine ve yetkisiz işlemlere yol açabilir.	- Bellek içeriği doğrulaması, oturum izolasyonu, bellek erişimi için güçlü kimlik doğrulama, anomali tespit sistemleri ve düzenli bellek temizleme rutinleri uygulanmalıdır. - Anomali tespit edildiğinde adli inceleme ve geri alma için YZ tarafından üretilen bellek anlık görüntüleri tutulmalıdır.
T2	Araçların Kötüye Kullanımı	Saldırganlar, aldatıcı istemler veya komutlarla YZ ajanlarını sahip oldukları yetkiler içinde entegre araçlarını kötüye kullanmaya yönlendirir. Buna, ajanın hasmane biçimde manipüle edilmiş veriyi alıp istenmeyen eylemler gerçekleştirmesi ve kötü niyetli araç çağrılarını tetiklemesi de dâhildir.	- Sıkı araç erişim doğrulaması veya çalıştırma öncesi doğrulama uygulanmalıdır. - Araç kullanımına oran sınırlaması getirilmeli, kullanım örüntüleri izlenmeli, ajan talimatları doğrulanmalı ve kötüye kullanımı önlemek için net operasyon sınırları tanımlanmalıdır. - Araç çağrılarını izleyen çalıştırma günlükleri tutulmalıdır.
T3	Yetki İhlali/ Ayrıcalık Ele Geçirme	Saldırganlar izin yönetimindeki zayıflıkları kullanarak yetkisiz işlemler gerçekleştirir. Bu durum, çoğu zaman dinamik rol mirası veya yanlış yapılandırmalardan kaynaklanır.	- Granüler yetki kontrolleri, dinamik erişim doğrulaması, rol değişikliklerinin güçlü izlenmesi ve yükseltilmiş ayrıcalık işlemlerinin ayrıntılı denetimi sağlanmalıdır. - Önceden tanımlanmış iş akışları dışında ajanlar arası yetki devrine izin verilmemelidir.
T4	Aşırı Kaynak Yüklemesi	Bu tehdit; YZ sistemlerinin işlem, bellek ve hizmet kapasitesini hedef alarak performansı düşürmeyi veya sistemi çalışamaz hâle getirmeyi amaçlar. YZ sistemlerinin yoğun kaynak yapısı bu saldırıyı kolaylaştırabilir.	- Kaynak yönetim kontrolleri, uyarlanabilir ölçekleme, kota mekanizmaları ve gerçek zamanlı yük izleme uygulanmalıdır. - Ajan oturumu başına yüksek frekanslı görev taleplerini sınırlayan YZ oran sınırlama politikaları uygulanmalıdır.

Tehdit No.	Tehdit Adı	Tehdit Açıklaması	Önlemler
T5	Zincirleme Halüsinasyon Saldırıları	Bu saldırılar, YZ'nin bağlamsal olarak makul ancak yanlış bilgi üretme eğiliminden yararlanır. Üretilen yanlış bilgi, sistem boyunca yayılıp karar süreçlerini bozabilir ve araç çağrılarını da yıkıcı biçimde etkileyebilir.	- Güçlü çıktı doğrulama mekanizmaları, davranışsal kısıtlar, çok kaynaklı doğrulama ve geri bildirim döngüleriyle sürekli düzeltme sağlanmalıdır. - Kritik karar süreçlerinde kullanılmadan önce YZ tarafından üretilen bilginin ikinci kez doğrulanması zorunlu olmalıdır.
T6	Niyet Bozma ve Hedef Manipülasyonu	Bu tehdit, bir YZ ajanının planlama ve hedef belirleme yeteneklerindeki zayıflıkları istismar ederek amaçlarının veya akıl yürütmesinin saldırgan tarafından değiştirilmesini sağlar. Yaygın bir yöntem, araçların kötüye kullanımında da belirtilen ajan ele geçirmedir.	- Plan doğrulama çerçeveleri, yansıma süreçleri için sınır yönetimi ve hedef hizalamasını koruyan dinamik koruma mekanizmaları uygulanmalıdır. - Başka bir modelin ajanı denetleyip önemli hedef sapmalarını işaretlediği davranış denetimi kullanılmalıdır.
T7	Uyumsuz ve Aldatıcı Davranışlar	Otonom ajanlar, doğrudan kötü niyetli girdi olmasa bile hedeflerini gerçekleştirmek için zararlı ya da yasaklı eylemler yapabilir. Bu durum, hizasız stratejiler geliştirdiklerinde beklenmeyen veya felaket sonuçlara yol açabilir.	- Modeller zararlı görevleri tanıyıp reddedecek şekilde eğitilmeli, politika kısıtları uygulanmalı, yüksek riskli eylemler için insan onayı zorunlu olmalı, kayıt ve izleme mekanizmaları kurulmalıdır. - Davranış tutarlılığı analizi ve doğruluk doğrulama modelleri gibi aldatma tespiti yöntemleri kullanılmalıdır.
T8	İnkâr Edilebilirlik	YZ ajanlarının yaptığı işlemler, yetersiz kayıt tutma veya karar süreçlerindeki şeffaflık eksikliği nedeniyle geriye dönük izlenemez veya hesap verilebilir olmaz.	- Kapsamlı sistem kaydı tutma, kriptografik doğrulama, zenginleştirilmiş üst veri ve gerçek zamanlı izleme uygulanmalıdır. - Düzenleyici uyum için YZ tarafından üretilen sistem kayıtları kriptografik olarak imzalanmalı ve değiştirilemez olmalıdır.

Tehdit No.	Tehdit Adı	Tehdit Açıklaması	Önlemler
T9	Kimlik Sahteciliği ve Taklit/Ajan Kimliği Ele Geçirme	Saldırganlar, YZ ajanlarını veya kullanıcıları taklit etmek için kimlik doğrulama mekanizmalarını istismar eder. Buna, kalıcı ve resmî bir ajan kimliğinin çalınması veya kötüye kullanılması da dâhildir; bu da ajanın konuşma arayüzünü ve güvenlik bariyerlerini aşan ayrıcalıklı, uzun süreli uygulama programlama arayüzü erişimi sağlayabilir.	- Kapsamlı kimlik doğrulama çerçeveleri geliştirilmeli, güven sınırları tanımlanmalı, en az ayrıcalık ilkesi uygulanmalı ve taklit girişimlerini tespit etmek için sürekli izleme yapılmalıdır. - İkinci bir model kullanılarak davranış profillemesi ile ajan aktivitesindeki sapmalar izlenmelidir.
T10	İnsan Döngüsünü Aşırı Yükleme	İnsan gözetimi ve karar doğrulaması içeren sistemlerde, saldırganlar insanın bilişsel sınırlarını veya etkileşim çerçevesini sömürmeyi hedefler.	- Gelişmiş insan-YZ etkileşim çerçeveleri ve uyarlanabilir güven mekanizmaları geliştirilmelidir. - Düşük riskli kararlar otomatikleştirilirken yüksek riskli anomalilerde insan müdahalesine öncelik veren hiyerarşik iş birliği modeli uygulanmalıdır.
T11	Beklenmeyen Uzaktan Kod Çalıştırma Saldırıları	Saldırganlar; YZ tarafından üretilen çalıştırma ortamlarını kullanarak zararlı kod enjekte eder, istenmeyen sistem davranışlarını tetikler veya yetkisiz betikler çalıştırır.	- YZ'nin kod üretme izinleri sınırlandırılmalı, kodlar yalıtılmış ve denetimli bir çalışma ortamında çalıştırılmalı ve YZ tarafından üretilen betikler izlenmelidir. - Yükseltilmiş ayrıcalık içeren YZ kaynaklı kodlar manuel incelemeye yönlendirilmelidir.
T12	Ajanlar Arası İletişim Zehirleme	Saldırganlar; YZ ajanları arasındaki iletişim kanallarını manipüle ederek yanlış bilgi yayar, iş akışlarını bozar veya karar süreçlerini etkiler.	- Kriptografik mesaj doğrulama, iletişim doğrulama politikaları ve ajanlar arası etkileşimlerde anomali izleme uygulanmalıdır. - Kritik karar süreçlerinde çoklu ajan uzlaşma doğrulaması zorunlu tutulmalıdır.

Tehdit No.	Tehdit Adı	Tehdit Açıklaması	Önlemler
T13	Çok Ajanlı Sistemlerde Kötü Niyetli Ajanlar	Kötü niyetli veya ele geçirilmiş YZ ajanları, normal izleme sınırlarının dışında hareket ederek yetkisiz işlemler yapabilir veya veri sızdırabilir. Buna, ele geçirilen bir ajanın kötü niyetli mantığı diğer ajanlara yaydığı bulaşıcı arka kapılar da dâhildir.	- Politika düzenlemeleri, kısıtları ve sürekli davranış izleme ile ajan özerkliği sınırlandırılmalıdır. - BDM'ler için tam kriptografik doğrulama mekanizmaları henüz bulunmasa da kontrollü barındırma ortamları, düzenli kırmızı takım ve giriş/çıkış sapma izleme ile bütünlük korunabilir.
T14	Çok Ajanlı Sistemlere Yönelik İnsan Saldırıları	Saldırganlar, ajanlar arası görev devri, güven ilişkileri ve iş akışı bağımlılıklarını sömürerek ayrıcalık yükseltmeye veya YZ destekli operasyonları manipüle etmeye çalışır.	- Ajan delegasyon mekanizmaları sınırlandırılmalı, ajanlar arası kimlik doğrulama zorunlu olmalı ve manipülasyon girişimlerini saptamak için davranış izleme yapılmalıdır. - Ayrıcalık yükseltmeyi önlemek için görev segmentasyonu uygulanmalıdır.
T15	İnsan Manipülasyonu	YZ ajanlarının insanlarla doğrudan etkileşim kurduğu durumlarda, güven ilişkisi kullanıcı şüpheciliğini azaltır ve ajanın yanıtlarına aşırı güven doğurur. Saldırganlar; bu durumu kullanarak ajanı kullanıcıyı manipüle etmeye, yanlış bilgi yaymaya veya gizli eylemler yapmaya zorlayabilir.	- Ajan davranışının tanımlı rol ve beklenen eylemlerle uyumlu olup olmadığı izlenmelidir. - Araç erişimi sınırlandırılmalı, bağlantı üretme yeteneği kısıtlanmalı ve koruma katmanları, moderasyon uygulama programlama arayüzleri veya ikinci model kullanılarak manipüle edilmiş yanıtları tespit edecek doğrulama mekanizmaları kurulmalıdır.
T16	Güvensiz Ajanlar Arası Protokol İstismarı	Model Bağlam Protokolü veya Ajanlar Arası İletişim Protokolü gibi protokollerdeki zayıflıklar, örneğin onay atlatma veya bağlam ele geçirme, ajanların yetkisiz eylemler yapmasına yol açabilir.	- Ajanlar arasında güçlü kimlik doğrulama uygulanmalıdır. - Bağlam yükleri ve araç üst verileri dâhil tüm protokol verileri temizlenmeli ve doğrulanmalıdır. - Ajanlar arası delegasyon sıkı kapsamlı işlevlerle sınırlandırılmalı, tüm iletişim ve araç çağrılarının kaydı tutulmalı, iletişimler şifrelenmelidir.

Tehdit No.	Tehdit Adı	Tehdit Açıklaması	Önlemler
T17	Tedarik Zinciri Ele Geçirme	Tehlikeye girmiş bir tedarik zinciri; ajanın içine savunmasız, zararlı, güncel olmayan veya başka şekilde tehlikeli bileşenlerin girmesine neden olabilir. Bu durum; model, kütüphane, araç, zehirlenmiş derleme ortamı veya diğer sistem bileşenleri üzerinden ajanın davranışını manipüle etmeye, veri almaya veya keyfî kod çalıştırmaya yol açabilir.	- YZ ekosistemi; dijital olarak imzalanmış yapıtlar, doğrulanabilir yazılım bileşen listeleri ve YZ bileşen listeleri, sürüm kontrolü ve akran incelemesi yoluyla güvence altına alınmalıdır. - Tedarik zinciri boyunca güçlü kimlik doğrulama uygulanmalı, güvenilmeyen araç kurulumları sınırlandırılmalı, ajanlar yalıtılmış ve denetimli bir çalışma ortamında çalıştırılmalıdır. - Model davranışındaki sapmalar ve kötü niyetli faaliyetler sürekli izlenmeli, simüle edilmiş tedarik zinciri saldırıları üzerinden kırmızı takım testleri uygulanmalıdır.

Türkiye açısından incelendiğinde bu tehditler, yalnızca yeni siber saldırı türlerinin ortaya çıkması anlamına gelmemektedir. Asıl mesele; kamu hizmetleri, kritik altyapılar ve kurumsal karar süreçleri YZ tabanlı sistemlere daha fazla bağlandıkça, güvenlik açıklarının doğrudan operasyonel ve stratejik sonuçlar üretme riskinin artmasıdır. Bu nedenle politika önceliği; YZ kullanan sistemlerin hangi veriyle, hangi yetki sınırları içinde ve hangi dış bağımlılıklarla çalıştığını açık biçimde belirlemek ve buna uygun güvenlik, denetim ve insan onayı mekanizmalarını kurmaktır. Türkiye'nin bu alandaki başarısı, YZ'yi ne kadar hızlı kullandığından çok onu ne kadar güvenli, denetlenebilir ve hesap verebilir bir çerçevede yönettiğine bağlı olacaktır.

BÖLÜM 4

TÜRKİYE ODAKLI STRATEJİK ETKİ DEĞERLENDİRMESİ

Türkiye açısından stratejik etkiler, tüm sektörlerde aynı ağırlıkta ortaya çıkmamaktadır. Kamu dijitalleşmesi ve e-Devlet yüzeyi, enerji ve telekomünikasyon gibi yüksek dijital bağlılık içeren kritik altyapılar, finansal sistemler, savunma tedarik zinciri ve bilgi ekosistemine duyarlı alanlar öncelikli risk taşımaktadır. Bu alanlarda yapay zekâ (YZ) destekli tehditlerin etkisi; veri ihlali veya hizmet kesintisi, karar kalitesinin bozulması, kurumsal güvenin aşınması, dış teknoloji bağımlılığının derinleşmesi ve kriz anında operasyonel sürekliliğin zayıflaması şeklinde ortaya çıkabilir. **Bu nedenle stratejik etki değerlendirmesi; teknik zafiyet mantığının ötesinde devlet kapasitesi, kurumsal dayanıklılık ve dijital egemenlik mantığıyla yapılmalıdır.**

Kamu kurumları açısından YZ; tehdit tespiti, dolandırıcılık analizi, olay müdahalesi, karar destek ve hizmet sunumu gibi alanlarda hız, ölçek ve öngörü kabiliyeti sağlamaktadır. YZ'nin; kamu yönetiminde verimlilik, hesap verebilirlik ve tepki verme kapasitesini artırmakta, özellikle kamu hizmetlerinin tasarımı ve sunumunda analitik ve karar destek işlevleri öne çıkmaktadır. Ancak devlet kapasitesindeki bu artış, otomatik olarak stratejik özerklik anlamına gelmemektedir. YZ sistemlerinin etkili kullanımı; algoritmik yetenekler dışında, veriye erişim, güvenli entegrasyon, model davranışının denetlenebilirliği, bulut altyapısının sürekliliği ve hesaplama gücüne erişim gibi ön koşullara bağlıdır. NIST, üretken YZ için geliştirdiği risk yönetimi profilinde bu teknolojilerin yönetim, ölçüm ve kontrol süreçleri kurulmadan devreye alınmasının; gizlilik, güvenlik, yanlış çıktı üretimi, üçüncü taraf bağımlılığı ve operasyonel kırılganlık gibi riskleri artırdığını vurgulamaktadır. **Bu sebeple YZ çağında devlet kapasitesi; kullanılan dijital zekâ altyapısının güvenilirliği, denetlenebilir olması ve dayanıklı biçimde yönetilebilmesi bağlamında tekrar düşünülmelidir.**

Bu dönüşüm, büyük teknoloji şirketleri ile kamu arasındaki güç ilişkisini de yeniden şekillendirmektedir. **Özellikle temel modeller, bulut altyapısı, model eğitimi, dağıtım kanalları ve veri işleme kapasitesi gibi katmanlarda az sayıda uluslararası aktörün öne çıkması; kamu kurumlarını sıradan bir yazılım satın alan kullanıcıdan çok kritik altyapısını dış sağlayıcıların kuralları içinde işleten bağımlı aktörlere dönüştürebilmektedir.** Nitekim temel model eğitimi; ince ayar ve dağıtım katmanlarında yoğunlaşmanın artması, pazar gücünün az sayıda şirketin elinde toplanması ve bu riskin yalnızca ekonomik değil yönetişim odağında da sonuçlar doğurması anlamına gelmektedir. Bu çerçevede kamu ile büyük teknoloji şirketleri arasındaki ilişki; klasik tedarikçi-müşteri ilişkisini aşarak veri yerleşimi, sistem kaydı erişimi, güvenlik denetimi, fiyatlandırma, lisans bağımlılığı ve model güncellemeleri üzerinde kontrol asimetrileri üreten, çerçeve sözleşmeyle yönetilmesi gereken yapısal bir güç ilişkisine dönüşmektedir.[39] **Bu nedenle yerli teknoloji ekosistemi ve tedarik zinciri bağımlılığı, doğrudan ulusal güvenlik ve siber dayanıklılık bağlamında ele alınmalıdır.**

Türkiye'nin 2024-2028 Ulusal Siber Güvenlik Stratejisi,[40] yerli ve millî siber güvenlik teknolojilerinin geliştirilmesini açık bir hedef olarak ortaya koymakta ve siber tehditlerle mücadelede ulusal kapasitenin güçlendirilmesini stratejik öncelik olarak tanımlamaktadır (bk. İnfografik 8). Bu yaklaşım, kritik dijital kabiliyetlerde dışa bağımlılığın; kriz anlarında operasyonel süreklilik, hızlı müdahale, güvenlik güncellemesi ve tedarik sürdürülebilirliği açısından ciddi kırılganlıklar doğurabileceğini

kabul etmektedir. Özellikle bulut, model servisleri, grafik işlemci temelli işlem gücü ve güvenlik yazılımları gibi alanlarda yabancı teknolojiye aşırı bağımlılık; jeopolitik baskılar, ihracat kısıtları, lisans değişiklikleri veya hizmet koşullarındaki tek taraflı dönüşümler nedeniyle güvenlik riskine dönüşebilir.

İnfografik 8: Türkiye'nin 2024-2028 Ulusal Siber Güvenlik Stratejisi'ne Göre Hedefler

Kaynak: T.C. Ulaştırma ve Altyapı Bakanlığı.

Açık kaynak modeller ile kapalı modeller arasındaki fark tam bu noktada önem kazanmaktadır. Bu durum; yalnızca teknik mimari meselesinden ibaret olmayıp denetlenebilirlik, veri egemenliği, operasyonel kontrol ve stratejik özerklik bakımından farklı güvenlik profilleri üretmektedir. Açık kaynak modeller; kurumlara modeli kendi ortamlarında çalıştırma, veriyi kurum sınırları içinde tutma, güvenlik katmanlarını özelleştirme ve davranış analizi yapma imkânı sağlayarak egemenlik avantajı sunabilir. Buna karşılık yeterli kurumsal yetkinlik, makine öğrenmesi (ML) yaşam döngüsü yönetimi olgunluğu ve güvenli model yaşam döngüsü yönetimi yoksa açık modeller; yanlış yapılandırma, güvenlik açığı, kötüye kullanım ve bakım yükü nedeniyle ek riskler de doğurabilir. Kapalı modeller ise daha yüksek ölçek, yönetilen servis kolaylığı ve hızlı devreye alma avantajı sunmakla birlikte model davranışının sınırlı görünürlüğü, veri akışının denetlenememesi ve üçüncü taraf güvenlik kontrollerine bağımlılık gibi sorunlar yaratabilir. **Dolayısıyla açık-kapalı model ayrımı, maliyet ve performans tercihi dışında egemenlik, denetim ve güvenlik mimarisi tercihidir.**[41]

Bu bağlamda Türkiye açısından stratejik önem taşıyan ve odaklanılması gereken başlıklar ulusal güvenlik ve kritik altyapı; NATO, AB ve uluslararası alanda süren veri egemenliği ve tedarik zinciri tartışmaları; kamu dijitalleşmesi ve e-Devlet yüzeyi ile son olarak toplumsal güven, derin sahte ve bilgi ekosisteminin etkileşimidir.

Ulusal Güvenlik ve Kritik Altyapı

OECD, kamu yönetiminde YZ kullanımının; karar desteği, dolandırıcılık tespiti ve hizmet optimizasyonu gibi alanlarda hızla yayıldığını belirtmektedir. NATO ise YZ'yi savunma ve dijital dönüşümün temel bileşenlerinden biri olarak gördüğünü ortaya koymaktadır.[42] YZ destekli sistemler; istihbarat analizi, tehdit tespiti, sınır güvenliği, siber savunma ve karar destek süreçlerinde devlete önemli kapasite artışı sağlayabilir. Bununla birlikte bu kapasite artışı, yeni stratejik bağımlılıklar da üretmektedir. Devletin kullandığı YZ sistemleri dış tedarikçilere, yabancı bulut altyapılarına, kapalı modellere veya dış kaynaklı veri akışlarına bağımlı hâle geldikçe ulusal güvenlik; yalnızca saldırılara karşı korunma meselesi olmaktan çıkarak teknoloji egemenliği, kriz anında süreklilik ve stratejik özerklik meselesine dönüşmektedir. **Bu nedenle YZ çağında ulusal güvenlik, yalnızca daha güçlü savunma araçlarına sahip olmayı kapsamamakta; aynı zamanda bu araçların denetimini elde tutmak anlamına da gelmektedir.**[43]

Kritik altyapılarda yabancı YZ çözümlerine bağımlılık ise daha yüksek düzeyde stratejik risk üretmektedir. Kritik altyapılar bakımından YZ iki yönlü etki üretmektedir. Bir taraftan erken uyarı, anomali tespiti, kestirimci bakım ve olay müdahalesi gibi avantajlar sunarken diğer taraftan görünürlüğü düşük, dış bağımlılığı yüksek ve yanlış kararların etkisi büyük sistemler yaratabilmektedir. AB AI Act Tasarısı,[44] kritik altyapılarda kullanılan belirli YZ sistemlerini yüksek riskli kategoriye yerleştirmiştir. Bu tasarı; enerji, ulaşım, temel hizmetler ve diğer kritik sektörlerde YZ'nin yalnızca sıradan bir dijitalleşme başlığı olmadığını; aynı zamanda güvenlik ile yönetişim konusu olduğunu da açıkça göstermektedir. Bu tür sistemlerde yabancı çözümlere aşırı bağımlılık; görünürlük kaybı, karar süreçlerinin dışarıya taşınması, kriz anında müdahale yetkisinin sınırlanması, tedarik zinciri üzerinden dolaylı saldırı riski ve operasyonel verinin yabancı hukuk alanlarına açılması gibi sorunlar doğurabilir.

Özellikle enerji, telekomünikasyon, finans, ulaşım ve kamu hizmetleri gibi sektörlerde yabancı YZ çözümlerine aşırı bağımlılık; tedarik zinciri kırılganlığı, operasyonel veri akışının dış ortamlara taşınması, kriz anında müdahale zorluğu ve güvenlik denetimlerinde şeffaflık eksikliği gibi riskler üretmektedir. Kritik altyapıda kullanılan bir modelin nasıl karar verdiğinin tam olarak bilinmemesi veya sistemin dış bir bulut servisinde çalışması, teknik bir tercih olmanın ötesinde egemenlik ve kamu otoritesi sorunu yaratabilir. Bu nedenle kritik altyapılarda YZ kullanımı; kontrol, denetlenebilirlik ve süreklilik açısından da değerlendirilmelidir.

Sektörler arasında enerji, telekomünikasyon ve savunma en yüksek stratejik etki grubunda yer almaktadır. Tablo 3, YZ destekli siber tehditlerin hangi sektörlerde daha yüksek stratejik riskler yarattığını ortaya koymakta; bu risklerin yalnızca teknik boyutla sınırlı kalmayıp aynı zamanda yönetişim yapıları ve kurumsal kapasiteyle yakından ilişkili olduğunu da vurgulamaktadır. **Çünkü burada saldırı yalnızca ekonomik zarar doğurmamakta; kamu düzeni, caydırıcılık, haberleşme sürekliliği ve ulusal güvenlik üzerinde doğrudan etki üretebilmektedir.** Finans sektörü; yaygın dijital kullanım ve yüksek işlem hacmi nedeniyle saldırgan otomasyonu için en uygun alanlardan biridir. Ulaştırma sektörü ise bağlantılı sistemler ve akıllı altyapılar nedeniyle önümüzdeki dönemde daha görünür bir risk alanı olacaktır.

Tablo 3: Öncelikli Sektörlerde Yapay Zekâ Destekli Riskler ve Etkileri

Sektör	Başlıca YZ-Siber Risk	Olasılık	Etki	Mevcut Kapasite Açığı	Öncelikli Politikalar
Savunma Sanayisi Tedarik Zinciri	Tedarik zinciri sızması, model/ algoritma hırsızlığı, iletişim ve görev verilerinin manipülasyonu	Orta	Çok Yüksek	Millîleşme yönelimi güçlü ancak dış bileşen, yazılım ve tedarik zinciri güvenliği stratejik risk olmaya devam edebilir.	- YZ bileşen envanteri, tedarik zinciri güvenlik denetimi - Yerli/denetlenebilir çözüm önceliği - Hassas veriler için kapalı ortam kullanımı - Tedarik süreçlerinde kayıt ve doğrulama yükümlülüğü
Enerji	OT/SCADA saldırıları, YZ destekli hizmet kesintisi, kestirimci bakım ve veri manipülasyonu	Yüksek	Çok Yüksek	Kritik hizmet sürekliliği nedeniyle yüksek öncelik, YZ'nin OT'ye entegrasyonu ek güvenlik katmanı gerektirir.	- Kritik altyapılar için YZ güvenlik standardı - BT-OT entegre risk değerlendirmesi - Yedekli çalışma düzeni - Kırmızı takım testleri - Tedarikçi doğrulama ve manuel devralma prosedürleri
Finans	Oltalama, sentetik kimlik, dolandırıcılık otomasyonu, veri sızıntısı	Yüksek	Yüksek	Regülasyon ve güvenlik olgunluğu görece yüksek olsa da saldırganların otomasyon avantajı büyümektedir.	- Çok katmanlı doğrulama - İkinci kanal teyidi - Yüksek riskli işlemlerde manuel onay - Model risk yönetimi çerçevesi - Sentetik medya tespit ve raporlama kapasitesi
Telekomü-nikasyon	DDoS, ağ yönetim sistemlerine sızma, yabancı ekipman ve tedarik bağımlılığı	Yüksek	Çok Yüksek	Hizmet sürekliliği ve ulusal iletişim omurgası niteliği nedeniyle kesinti etkisi çarpanlıdır.	- Ağ otomasyonunda yetki sınırları, anomali tespiti ve insan onayı dengesi - Sektörel YZ güvenlik rehberi - Olay raporlama ve tedarik zinciri denetimi

Sektör	Başlıca YZ-Siber Risk	Olasılık	Etki	Mevcut Kapasite Açığı	Öncelikli Politikalar
Ulaştırma	Akıllı ulaşım sistemleri, otonom araç zinciri, lojistik platform manipülasyonu	Orta-Yüksek	Yüksek	Dijitalleşme arttıkça saldırı yüzeyi büyür; AB'nin otonom araç tedarik zinciri risk değerlendirmeleri, bu alanın yükselen risk olduğunu göstermektedir.	- Akıllı ulaşım sistemleri için YZ güvenlik standardı - Tedarik zinciri denetimi - Araç ve altyapı sistemlerinde güvenli entegrasyon - Yüksek riskli işlemlerde insan onayı ve manuel devralma prosedürleri - Zorunlu olay raporlama ve sektörel tatbikat mekanizmaları

Kritik altyapı işletmecileri YZ'yi; anomali tespiti, karar destek, otomatik müdahale ve kestirimci bakım için kullanmaya başladıkça saldırı yüzeyi yalnızca ağlar ve uç sistemlerle sınırlı kalmaz. Veri bütünlüğü, model güvenliği, bulut bağımlılığı ve tedarik zinciri güvenliği de kritik hâle gelir. YZ çağında bu kırılganlıklar yeni bir katman daha kazanır. CISA,[45] YZ'nin OT ortamlarına güvenli entegrasyonunun, doğrudan operasyonel risk ve güvenlik riski yarattığını vurgulamaktadır. Bu çerçevede kritik altyapı riskleri beş maddede toplanabilir:

- Eski ve heterojen sistemlerin modern YZ bileşenleriyle birlikte çalışması.
- Üçüncü taraf ve yabancı tedarikçi bağımlılığı.
- Sektörel görünürlük ve olay paylaşımında parçalanma riski.
- OT ile kurumsal BT ortamlarının yakınsaması.
- Kriz anında hızlı ve yerli müdahale kapasitesinin her sektörde aynı olgunlukta olmaması.

Türkiye'de kritik altyapı yaklaşımı, siber güvenlik organizasyonu ile uzun süredir sektörel bir mantıkla ele alınmaktadır.[46] Resmî rehberlerde kritik altyapı sektörleri; ulaştırma, enerji, haberleşme, finans, su yönetimi ve kritik kamu hizmetleri olarak çerçevelenmiştir. Ayrıca Ulusal Siber Olaylara Müdahale Merkezi (USOM), sektörel SOME[47] ve kurumsal SOME[48] yapıları bu alanlarda siber olay koordinasyonu için tanımlanmıştır. 2024-2028 Ulusal Siber Güvenlik Stratejisi de kritik altyapıların korunmasını ve yerli/millî siber güvenlik teknolojilerinin geliştirilmesini öncelikler arasında saymaktadır. Türkiye'nin kritik sektör çerçevesi AB/AB Ağ ve Bilgi Sistemleri Direktifi 2 (NIS2) ve güncel tedarik zinciri güvenliği yaklaşımıyla uyumludur.[49]

NATO, AB ve Stratejik Teknoloji Bağımlılıkları

NATO açısından YZ ve siber güvenlik tartışması; savunma kapasitesi, birlikte çalışabilirlik, risk yönetimi ve hasmane YZ kullanımına karşı korunma meselesidir. NATO,[50] YZ'nin ittifak içinde güvenli ve sorumlu biçimde kullanılmasını hızlandırmayı, YZ teknolojilerini korumayı ve hasmane YZ kullanımına karşı önlem almayı açık hedefler arasında saymaktadır. Bu durum, YZ'nin savunma alanında doğrudan güvenlik politikası konusu olduğunu göstermektedir.

NATO'nun 360 derece güvenlik ve hibrit tehdit yaklaşımı da benzer biçimde siber saldırı, dezenformasyon, ekonomik baskı, düzensiz aktör kullanımı ve stratejik bağımlılıkların tek bir güvenlik resmi içinde değerlendirilmesi gerektiğini savunmaktadır. Buna göre hibrit tehditlerin; hızı, ölçeği ve yoğunluğu son yıllarda artmıştır. **Bu perspektif, teknoloji bağımlılığını artık sadece ekonomik verimlilik sorunu olmaktan çıkarıp güvenlik ve caydırıcılık başlığına taşımaktadır.**

AB tarafında ise tartışma güvenilir YZ ve güvenli/egemen dijital altyapı olmak üzere iki eksende ilerlemektedir. AI Act Tasarısı, dünyadaki ilk kapsamlı YZ çerçevesi olarak risk temelli yaklaşımı benimseyip özellikle yüksek riskli kullanımlarda geliştirici ve uygulayıcılara özel yükümlülükler getirmektedir. NIS2 ise 18 kritik sektörde ortak siber güvenlik seviyesini yükseltmeyi ve üye devletler arasında daha sıkı koordinasyon kurmayı hedeflemektedir. Bu iki düzenleme birlikte okunduğunda AB'nin, YZ ve siber güvenliği yenilik, güven ve düzenleme üçgeninde kurguladığı görülmektedir. 2025-2026 döneminde AB'nin veri egemenliği ve tedarik zinciri güvenliği vurgusu daha da belirginleşmiştir. Avrupa Komisyonunun Cloud Sovereignty Framework (Bağımsız Bulut Çerçevesi) girişimi,[51] bulut egemenliğini stratejik, hukuki, operasyonel, güvenlik, tedarik zinciri şeffaflığı ve teknolojik açıklık gibi hedefler üzerinden tanımlamaktadır. 2026'da duyurulan AB ICT Supply Chain Security Toolbox (Bilgi-İletişim Teknolojileri - BİT Tedarik Zinciri Güvenliği Araç Seti)[52] ise kritik tedarikçilerin değerlendirilmesi, çok tedarikçili stratejiler ve yüksek riskli sağlayıcılara bağımlılığın azaltılması gibi tedbirleri öne çıkarmaktadır. **Bu durum, veri egemenliği tartışmasının artık yalnızca verinin nerede tutulduğu meselesi olmaktan çıktığını; sağlayıcı bağımlılığı, yabancı müdahale riski, tedarik zinciri görünürlüğü ve kriz anında kontrol yeteneği meselesi olduğunu göstermektedir.**

Bu bağlamda Türkiye açısından iki husus ön plana çıkmaktadır. Birincisi, NATO bağlamında birlikte çalışabilirlik ve ortak tehdit resmi önemlidir. İkincisi, AB'de gelişen egemenlik ve tedarik zinciri güvenliği anlayışı, Türkiye'de de kritik altyapılar ve kamu dijitalleşmesi için veri, model, bulut ve donanım bağımlılıklarının yeniden düşünülmesini gerekli kılar. **Dolayısıyla Türkiye'nin politika seçeneği YZ kullanımını aşarak hangi katmanlarda yerli/denetlenebilir/çoklu tedarik yapısı kurulması gerektiğine yoğunlaşmaktadır.**

Kamu Dijitalleşmesi ve e-Devlet Yüzeyi

Türkiye açısından bakıldığında YZ, dijitalleşme ve siber güvenlik tartışması, bazı konularda daha da önem kazanmaktadır. Nitekim e-Devlet Kapısı istatistikleri, kamu dijitalleşmesinin artık çok geniş bir kullanıcı tabanına ve hizmet ölçeğine ulaştığını göstermektedir. Zira Türkiye'de kamu dijitalleşmesi

artık sınırlı sayıda çevrim içi hizmetten ibaret olmaktan çıkmış; geniş ölçekli ve yoğun kullanılan bir dijital kamu yüzeyi hâline gelmiştir. e-Devlet Kapısı'nın 2024 verilerine göre kullanıcı sayısı 66,7 milyon, yıllık giriş sayısı 4,2 milyar, sunulan hizmet sayısı 8.309 ve hizmet sunan kurum sayısı 1.080'dir.[53] Bu veriler, kamu hizmetlerinde yüksek yoğunluklu bir dijital temas yüzeyi oluştuğunu göstermektedir.

Bu ölçekteki dijitalleşme, devlet kapasitesini artırmakta ancak aynı zamanda saldırı yüzeyini de büyütmektedir. Kullanıcı yoğunluğu, kurumsal çeşitlilik ve hizmet sayısındaki artış; kimlik, erişim, veri bütünlüğü, hizmet sürekliliği ve tedarik zinciri güvenliği başlıklarını daha kritik hâle getirmektedir. Özellikle tekil zafiyetlerin çok sayıda kullanıcı ve kuruma etkimesi, e-Devlet mimarisini yalnızca bir dijital hizmet platformu olmaktan çıkarıp ulusal ölçekte bir güvenlik varlığına dönüştürmektedir.

YZ, bu yüzeyi çift yönlü biçimde etkileyebilir. Savunma tarafında; dolandırıcılık tespiti, anomali analizi, olay korelasyonu ve kullanıcı davranışı temelli güvenlik kontrolleri için yeni imkânlar üretebilir. Saldırı tarafında ise kimlik avını kişiselleştirme, sentetik içerikle kurumsal güveni zayıflatma, sosyal mühendisliği ölçeklendirme ve kurumsal karar süreçlerine yanlış veri enjekte etme kapasitesini artırabilir. Bu nedenle kamu dijitalleşmesi ile YZ birlikteliği, verimlilik kadar yönetişim ve dayanıklılık perspektifinden de değerlendirilmelidir.

Kamu dijitalleşmesinin bir diğer sonucu da teknolojik görünmez bağımlılıktır. Kamu kurumu, kendi hizmetini sunuyor görünse de arka planda bulut, kimlik, sistem kaydı, analitik, model servisleri veya güvenlik ürünleri bakımından dış sağlayıcılara bağımlı olabilir. Bu durum, özellikle üretken YZ ve bulut tabanlı hizmetlerin kamu süreçlerine girmesiyle daha kritik hâle gelmiştir. Avrupa Komisyonunun son dönemde bulut egemenliği ve tedarik zinciri güvenliği üzerine attığı adımlar, kamu dijitalleşmesinin artık yalnızca çevrim içi hizmet kalitesiyle sınırlı olmadığını; aynı zamanda egemenlik ve denetlenebilirlik konusu olarak da görüldüğünü ortaya koymaktadır.

Toplumsal Güven, Derin Sahte ve Bilgi Ekosistemi

YZ'nin stratejik etkilerinden biri de toplumsal güven üzerinde ortaya çıkmaktadır. Derin sahte içerikler, YZ destekli dezenformasyon, sentetik medya ve ikna odaklı içerik üretim araçları; kamusal tartışma alanını, seçim güvenliğini, medya güvenilirliğini ve kurumlara duyulan güveni doğrudan etkileyebilmektedir.

Buradaki risk, yalnızca tek tek sahte içeriklerin yayılması değildir. Asıl sorun, bilgi ekosisteminde genel bir güvensizlik ortamı oluşmasıdır. Bir içerik gerçek olsa bile derin sahte şüphesi, kamusal hakikat zeminini aşındırabilir. Bu durum; özellikle kriz zamanlarında, seçim süreçlerinde, toplumsal olaylarda veya devlet kurumlarının kamuoyu ile iletişiminde daha yıkıcı hâle gelebilir. Dolayısıyla derin sahte ve sentetik medya tehdidi, yalnızca siber suç veya bireysel dolandırıcılık başlığı altında değerlendirilemez. Bu konu; toplumsal güvenin, demokratik süreçlerin ve kurumsal meşruiyetin aşınması bağlamında ele alınmalıdır.

Bölgesel güvenlik ortamında siber tehditler artık nadiren tek başına ortaya çıkmaktadır. Daha çok dezenformasyon, ekonomik baskı, vekil aktör kullanımı, sınır ötesi dijital operasyonlar ve kritik altyapıya yönelik baskılarla birleşen hibrit tehdit biçiminde görülmektedir. Bu ortamda dezenformasyon ve daha geniş anlamda hasmane bilgi manipülasyonu, siber alanın yan ürünü değil onun stratejik uzantısıdır. Nitekim hasım kaynaklı bilgi manipülasyonu ve müdahale operasyonlarının artık daha sistematik biçimde haritalandığı ve tehdit altyapılarının açık, örtülü, devlet bağlantılı ve devlet uyumlu kanallar üzerinden çalıştığı bilinmektedir. Bu durum, derin sahte ve sentetik medya kullanımının; bilgi ekosistemini bozma, kurumsal güveni aşındırma ve kriz anlarında algı üstünlüğü sağlama aracı olarak değerlendirildiğini göstermektedir.

Bölgesel ortamda vekil aktörler ve devlet bağlantılı yapılar arasındaki sınırın bulanıklaşması ayrıca önemlidir. Çeşitli uluslararası kurumların ilgili tehdit değerlendirmeleri de devlet bağlantılı gruplar, siber aktivist gruplar ve propaganda ağları arasındaki örtüşmenin arttığını, kamu yönetimi ve kritik hizmetlerin yüksek hedef değerine sahip olduğunu göstermektedir. Özellikle kamu yönetimi sektörü, öne çıkan hedef alanlardan biridir. Bu tablo; diplomatik gerilim, seçim süreçleri, askerî krizler veya sınır ötesi çatışma dönemlerinde siber faaliyet ile bilgi manipülasyonunun birlikte kullanılması riskini artırmaktadır.

Türkiye açısından bölgesel tehdit ortamı; yakın coğrafyadaki çatışmalar, sınır ötesi askerî ve diplomatik gerilimler, göç ve lojistik hatları, savunma sanayisi tedarik ağları ve yoğun kamu dijitalleşmesi nedeniyle çok katmanlı bir risk üretmektedir. Bu nedenle bölgesel tehdit okuması yalnızca siber saldırıya indirgenmeyerek dezenformasyon, siber baskı, vekil aktör ve kritik tedarik zinciri zorlama kombinasyonu üzerinden okunmalıdır.

Bölgesel dinamikler ve tehdit ortamı, Türkiye'nin siber güvenlik yaklaşımında iki öncelik yaratmaktadır. Birincisi, teknik savunma ve stratejik iletişim/dezenformasyonla mücadele kapasitesinin birlikte ele alınmasıdır. İkincisi ise sınır ötesi ve dolaylı tehditlerin yalnızca askerî veya siber başlık altında değil, hibrit güvenlik perspektifiyle değerlendirilmesidir. Bu nedenle YZ çağında bölgesel tehdit yönetimi; güvenlik operasyon merkezi ve siber olaylara müdahale ekibi kapasitesinin ötesinde bilgi ekosistemi dayanıklılığı, tedarik zinciri farkındalığı ve kamu güvenini koruyan kurumsal koordinasyon gerektirmektedir.

BÖLÜM 5

TÜRKİYE'NİN STRATEJİK ÖNCELİKLERİ

Yapay zekâ (YZ) destekli siber tehditler karşısında Türkiye'nin öncelikli yönetişim ihtiyaçları stratejik bir çerçevede ele alınmalıdır. Temel mesele, yalnızca yeni riskleri tanımlamak değildir. Asıl ihtiyaç; bu risklere kurumsal kapasite, düzenleme, denetim, veri yönetişimi, kritik altyapı güvenliği ve toplumsal farkındalık boyutlarıyla birlikte yanıt verebilmektir. Bu çerçevede Siber Güvenlik Başkanlığının (SGB)[54] kurulması; teknik savunma kapasitesinin ötesinde kritik altyapıların korunması, kurumlar arası koordinasyonun güçlendirilmesi, standartların geliştirilmesi, SOME yapılanmasının olgunlaştırılması, kamuda YZ kullanımının yönetişimi ve ulusal güvenlik ekosisteminin desteklenmesi bakımından yeni bir uygulama zemini sunmaktadır.

Merkezî Koordinasyon ve Kurumsal Mimari

Bu raporda politika açığı, teknik risk ile kurumsal yanıt kapasitesi arasındaki boşluk olarak tanımlanmaktadır. Yani kurumların YZ destekli sistemleri kullanma hızı ile bu sistemleri düzenleme, denetleme, kayıt altına alma, sınırlandırma ve kriz anında yönetme kapasitesi arasındaki fark büyüdükçe stratejik kırılganlık derinleşmektedir. Türkiye açısından ilk öncelik, bu boşluğu azaltacak merkezî bir koordinasyon ve kurumsal mimari kurmaktır. Bu kurumsal mimari; On İkinci Kalkınma Planı,[55] Ulusal Yapay Zekâ Stratejisi[56] ve Cumhurbaşkanlığı yıllık programlarında ortaya konan dijital dönüşüm, veri yönetişimi ve güvenli YZ hedeflerinin uygulama zeminini de güçlendirir. Böylece YZ'ye ilişkin siber güvenlik öncelikleri, daha geniş ulusal teknoloji ve kamu modernizasyonu gündemiyle uyumlu hâle gelir.

Koordinasyon alanındaki başlıca açık; YZ ve siber güvenliğin birden fazla kurumun yetki alanına girmesine rağmen bu aktörler arasında karar alma, olay paylaşımı, ortak standart üretimi ve uygulama gözetimi için yeterince bütünleşik mekanizmaların her zaman kurulamamış olmasıdır. YZ destekli sistemler, klasik olay müdahalesinden daha geniş bir koordinasyon ihtiyacı doğurmaktadır. Çünkü mesele yalnızca zararlı trafiğin engellenmesi değildir. Modelin nasıl eğitildiği, hangi verilerle beslendiği, bulut ortamının nerede olduğu, tedarikçinin kim olduğu, karar destek sisteminin hangi kamu hizmetinde kullanıldığı ve ortaya çıkan zarardan kimin sorumlu olduğu gibi çok katmanlı sorular da bu başlığın parçasıdır.

Türkiye açısından öncelik, YZ'ye ilişkin kararların dağınık bir uygulama alanı olarak kalmamasıdır. Ulusal düzeyde; ortak ilke setleri, ortak risk dili, ortak olay raporlama mantığı ve ortak denetim beklentileri tanımlanmalıdır. Kurum içi ölçekte ise hukuk, uyum, risk yönetimi, bilgi güvenliği, veri yönetişimi ve iç denetim birimlerinin aynı çerçeve içinde çalışması sağlanmalıdır. SGB'nin merkezî koordinasyon rolü, bu ortak mimarinin kurulmasında temel kaldıraç olabilir.

Regülasyon, Standartlar ve Denetim

Regülasyon alanındaki temel açık, YZ'ye ilişkin kuralların çoğu yerde ya çok genel kalması ya da siber güvenlik, veri koruma, kamu tedariki ve kritik altyapı yönetimiyle yeterince entegre olmamasıdır. YZ'ye özgü risk kategorileri, kamu kurumlarında üretken YZ kullanımı, model tedarik zinciri, veri yerleşimi, sentetik medya, BDM tabanlı karar destek sistemleri ve ajan tabanlı YZ uygulamaları için daha ayrıntılı ikincil düzenleme ve sektörel rehber ihtiyacı artmaktadır.

Bu alandaki açık üç boyutta tanımlanabilir. Birincisi, tanım ve kapsam açığıdır. Hangi YZ sistemlerinin yüksek riskli sayılacağı ve hangi kullanım alanlarının özel kontrole tabi olacağı netleştirilmelidir. İkincisi, uygulama açığıdır. Risk değerlendirmesi, kayıt tutma, test, denetim, insan gözetimi ve olay bildirimi gibi mekanizmaların kurumsal seviyede nasıl işletileceği belirlenmelidir. Üçüncüsü ise uyumlaştırma açığıdır. YZ kuralları; siber güvenlik, kişisel veriler, kamu alımları ve kritik altyapı mevzuatıyla birlikte düşünülmelidir. Buna ek olarak üretken YZ ile üretilen ve özellikle internet ortamında dolaşıma giren içeriklerden doğan sorumluluk meselesi de daha görünür hâle gelmektedir. TBMM Yapay Zekâ Araştırma Komisyonu Raporu'nda da[57] vurgulandığı üzere bu alanda mevcut özel hukuk ve ceza hukuku hükümlerinin uygulanabilirliği kadar 5651 sayılı Kanun[58] bağlamındaki sorumluluk rejiminin de yüksek riskli sentetik içerikler bakımından yeniden değerlendirilmesi önem taşımaktadır.

SGB; standart geliştirme, teknik ölçüt belirleme, denetim kapasitesini yönlendirme ve yüksek riskli alanlarda asgari güvenlik beklentilerini somutlaştırma bakımından merkezî bir rol üstlenebilir. Özellikle kamu kurumlarının kullanacağı sistemlerde; güvenlik tasarımı, işlem günlüğü, veri sınıflandırması, tedarikçi şeffaflığı, denetlenebilirlik ve insan onayı gibi koşulların ortak teknik çerçevelerle desteklenmesi gerekir.

Açıklanabilirlik ve denetlenebilirlik de bu başlığın ayrılmaz parçalarıdır. YZ destekli sistemlerin kurumsal süreçlerde yaygınlaşması, yalnızca doğruluk ve performans değil, açıklanabilirlik ve hesap verebilirlik gereksinimini de öne çıkarmaktadır. Özellikle siber güvenlik, finans, sağlık ve kamu karar destek sistemlerinde açıklanabilirlik; yanlış pozitif ve yanlış negatif kararların incelenmesini, iç denetimin güçlenmesini ve kurumsal güvenin korunmasını sağlar. Bu nedenle açıklanabilir YZ, teknik bir tercih olmanın ötesinde bir denetim ve yönetişim koşulu olarak ele alınmalıdır.

Bu alandaki uygulama maliyeti genel olarak orta düzeydedir. Maliyet daha çok mevzuat hazırlığı, etki analizi, paydaş danışmaları, sektörel rehberlerin geliştirilmesi, test ve denetim mekanizmalarının kurulması ile uygulama kapasitesinin güçlendirilmesi boyutunda ortaya çıkmaktadır. Buna karşılık beklenen etki çok yüksektir. Güçlü bir düzenleme ve standart çerçevesi; sorumluluk alanlarını netleştirir, yüksek riskli YZ kullanımını sınırlar ve kamu ile özel sektör için daha öngörülebilir bir uygulama zemini oluşturur.

Kritik Altyapılar ve Sektörel Dayanıklılık

Türkiye açısından enerji, finans, telekomünikasyon, ulaşım, savunma sanayisi ve kamu hizmetleri gibi alanlar, YZ destekli siber tehditlerin en yüksek etki üretebileceği sektörlerdir. Bu alanlarda risk, yalnızca bilgi işlem sistemlerinin ihlali ile sınırlı değildir. Operasyonel süreklilik; emniyet, tedarik güvenliği, kamu düzeni ve toplumsal güven üzerinde doğrudan sonuç doğurabilir. Bu nedenle stratejik öncelik, kritik altyapıların yalnızca klasik BT güvenliği mantığıyla korunması değildir. Veri bütünlüğü, model güvenilirliği, karar destek süreçlerinin doğruluğu, tedarik zinciri şeffaflığı ve dış teknoloji bağımlılıklarının yönetimi birlikte ele alınmalıdır. Özellikle bakım önerisi veren yardımcı YZ asistanları, olay özeti üreten modeller, arıza sınıflandırması yapan sistemler ve ajan tabanlı iş akışları; yanlış veri, yanlış bağlam veya manipüle edilmiş model davranışı nedeniyle doğrudan operasyonel riske dönüşebilir.

SGB'nin kritik altyapılar için belirleyeceği ilke, standart ve koordinasyon çerçevesi bu nedenle ağ savunmasını olduğu kadar YZ ile bütünleşik dijital bileşenlerin güvenli kullanımını da kapsamalıdır. Kritik sistemlerin envanterinin çıkarılması, hangi hizmetin hangi dış modele veya hangi bulut katmanına bağımlı olduğunun görünür hâle getirilmesi ve güvenlik yükümlülüklerinin kritiklik düzeyine göre farklılaştırılması temel ihtiyaçlardır.

Sıfır güven modeline geçiş de bu başlık altında stratejik önem taşımaktadır. YZ destekli tehditlerin arttığı ortamda, geleneksel varsayılan güven yaklaşımı giderek yetersiz hâle gelmektedir. Çok faktörlü kimlik doğrulama, minimum ayrıcalık ilkesi, sürekli davranış analizi, merkezî sistem kaydı, veri erişimlerinin izlenmesi, hassas veriler için ek koruma önlemleri ve gerektiğinde otomatik müdahale mekanizmaları kritik altyapılarda kademeli olarak yaygınlaştırılmalıdır. Kısa vadede temel kimlik ve erişim kontrolleri güçlendirilmelidir. Orta vadede dinamik risk değerlendirmesi ve yarı otomatik müdahale yetenekleri kurulmalıdır. Uzun vadede ise kimlik, ağ, veri, cihaz ve uygulama katmanlarında bütünleşik sıfır güven mimarisi oluşturulmalıdır.

Sıfır güven modeli için benimsenmesi gereken YZ güvenlik politikaları aşağıdaki gibi gruplanabilir.

Kısa Vade (0-12 Ay)

- Bu aşamada amaç, düşük-orta karmaşıklıkta ancak etkisi yüksek olan temel kontrolleri hızla devreye almaktır.
- Kimlik doğrulama her seviyede devam etmeli ve çok faktörlü kimlik doğrulama yaygınlaştırılmalıdır.
- Ağ erişimi minimum ayrıcalık prensibi ile sınırlandırılmalıdır.
- Kullanıcı ve sistem davranışları sürekli analiz edilmelidir.
- Anormal aktiviteler tespit edildiğinde anında uyarılar oluşturulmalıdır.
- Kötü amaçlı IP adresleri, anormal kullanıcı davranışları ve tehdit trendleri sürekli takip edilmelidir.
- Veri erişimleri analiz edilmeli ve hassas veriler ek güvenlik önlemleriyle korunmalıdır.
- YZ destekli veri sızıntısı önleme sistemleri uygulanmalıdır.
- Derin sahte tespit sistemleri siber güvenlik politikalarına entegre edilmelidir.
- Sahte kimlik kullanımına karşı otomatik uyarı mekanizmaları oluşturulmalıdır.
- Her erişim talebi için risk değerlendirmesi mantığı başlatılmalı ve bu öncelikle kritik sistem ile kullanıcı gruplarında uygulanmalıdır.

Orta Vade (1-3 Yıl)

- Bu aşamada amaç, temel kontrolleri olgunlaştırmak ve YZ destekli analiz ile yarı otomatik müdahale yeteneklerini kurmaktır.
- Her erişim talebi YZ ile analiz edilerek dinamik risk değerlendirmesi yapılmalıdır.
- Tehdit verileri gerçek zamanlı olarak analiz edilmeli ve tahmin edici savunma sistemleri oluşturulmalıdır.

- ML ile sistemler sürekli güncellenmeli ve yeni saldırı modellerine adapte edilmelidir.
- Otomatik tehdit tespit ve yanıt sistemleri kurulmalıdır.
- Şüpheli işlemler YZ tarafından analiz edilerek otomatik aksiyonlar alınmalıdır.
- Kimlik doğrulama süreçlerinde YZ destekli yüz ve ses analizi kullanılmalıdır.
- Saldırı sonrası iyileşme süreçleri YZ ile hızlandırılmalıdır.

Uzun Vade (3-5 Yıl)

- Bu aşamada amaç, yüksek olgunluk gerektiren, stratejik ve ileri seviye güvenlik mimarilerini kurmaktır.
- Bir saldırı tespit edildiğinde, YZ otomatik olarak ilgili sunucuları izole edebilmelidir.
- Kurum genelinde; yüksek doğruluklu, güvenilir ve denetlenebilir otonom/yarı otonom müdahale mekanizmaları kurulmalıdır.
- Post-kuantum kriptografi kullanılarak YZ destekli şifre kırma saldırılarına karşı koruma sağlanmalıdır.
- Sıfır güven mimarisi; kimlik, ağ, veri, cihaz ve uygulama katmanlarında bütünleşik ve sürekli çalışan bir yapıya dönüştürülmelidir.

Bu dönüşümün uygulama maliyeti orta ile yüksek düzey arasında değişebilir. Kimlik altyapısının yenilenmesi, mikro segmentasyon, cihaz görünürlüğü, log bütünlüğü ve güvenlik orkestrasyonu bu maliyeti artırır. Buna karşılık beklenen etki çok yüksektir. Yetkisiz erişimlerin azaltılması, iç tehditlerin sınırlandırılması, yanal hareketlerin zorlaştırılması ve hizmet sürekliliğinin güçlendirilmesi bu yatırımı stratejik hâle getirmektedir.

Olay Müdahalesi ve Tehdit İstihbaratı

Türkiye'de USOM'un ulusal ve uluslararası koordinasyonu yürüten yapısı ile SOME ağının kurumlar ve sektörler arasında siber olay yönetimi için temel çerçeveyi oluşturması önemli bir dayanak sağlamaktadır. Bununla birlikte YZ çağında olay müdahalesi, klasik zararlı yazılım ve ağ trafiği takibinin ötesine geçmektedir. Sentetik medya, kimlik manipülasyonu, model bütünlüğüne yönelik saldırılar, veri zehirleme, tedarik zinciri kaynaklı davranış sapmaları ve ajan tabanlı sistemlerin kötüye kullanımı gibi tehditler; olay müdahale perspektifinin genişletilmesini gerektirmektedir.

Bu bağlamda SOME yapılanmasının olgunlaştırılması, güvenlik operasyon merkezî kapasitesi ile tehdit istihbaratı süreçlerinin YZ boyutunu da içerecek şekilde güncellenmesi stratejik bir önceliktir. Sorun yaşayan kurumlara yalnızca teknik müdahale desteği verilmesi yeterli değildir. Olayın; veri katmanı, model katmanı, tedarik zinciri bağlantısı, karar destek etkisi ve kamu güveni üzerindeki sonuçları da aynı anda değerlendirilmelidir.

Başarı ölçütü, olaylara yalnızca daha hızlı müdahale edilmesi değildir. Asıl ölçüt; kurumlar arasında rol karmaşasının azaltılması, tehdit bilgisinin daha erken paylaşılması, YZ kaynaklı risklerin olay

yönetimi süreçlerine entegre edilmesi ve kriz anlarında tek merkezli ancak çok paydaşlı bir yönetişim refleksinin güçlendirilmesidir.

Kamuda Yapay Zekâ ve Veri Yönetişimi

YZ kullanımının kamuda yaygınlaşması, veri ve model yönetişimini Türkiye'nin stratejik öncelikleri arasına taşımaktadır. Sorun yalnızca hangi modelin kullanıldığı değildir. Hangi verinin modele gireceği, hangi verinin dış servislere çıkamayacağı, çıktının hangi aşamada insan denetimine tabi olacağı, modelin nasıl izleneceği ve yanlış ya da manipüle edilmiş bir çıktının sorumluluğunun kimde olacağı netleştirilmelidir.

Veri ve model yönetişimi bakımından temel ihtiyaçlar açıktır. Veri kaynağı doğrulaması yapılmalıdır. Model yaşam döngüsü kayıt altına alınmalıdır. Giriş ve çıkış filtreleme mekanizmaları kurulmalıdır. Üçüncü taraf model, eklenti ve ajan bileşenleri denetlenmelidir. BDM tabanlı sistemlerde istem enjeksiyonu, hassas bilgi ifşası, tedarik zinciri zafiyetleri, aşırı yetki ve aşırı güven riskleri; kurumsal karar kalitesi açısından doğrudan yönetişim sorunu üretmektedir.

Kamuda YZ uygulamalarının çoğalmasıyla birlikte karar destek ile karar verme arasındaki sınır daha kritik hâle gelmektedir. Aşırı yetki verilmiş bir sistem yanlış bağlamla işlem başlatabilir. Aşırı güvenilen bir model çıktısı, denetlenmeden kurumsal akışa girebilir. Bu nedenle insan denetimi, işlem günlüğü, rol tabanlı yetki, acil durdurma mekanizması ve sorumluluk zinciri; kamusal kullanım için vazgeçilmez unsurlar hâline gelmektedir.

Kamuda kullanılan yüksek etkili YZ sistemlerinde açıklanabilir olmak; denetlenebilirlik ve hesap verebilirliğin temel koşullarından biridir. Bir modelin hangi veri, kural veya örüntüye dayanarak çıktı ürettiğinin makul ölçüde anlaşılabilmesi; yanlış kararların incelenmesini, insan denetiminin işletilmesini ve kurumsal sorumluluğun belirlenmesini kolaylaştırır. Bu nedenle kamu kurumlarında açıklanabilirlik; model dokümantasyonu, kayıt tutma, test ve doğrulama süreçleriyle birlikte ele alınması gereken bir yönetişim unsuru olarak değerlendirilmelidir.

SGB'nin kamuda YZ, dijital devlet ve veri yönetişimi alanında üstlenebileceği rol, bu başlığı daha da önemli kılmaktadır. Ortak veri alanı yaklaşımı, veri kalite kriterleri, kamu bilişim projelerinde ilke ve standartların belirlenmesi ve YZ uygulamalarında ortak güvenlik kurallarının oluşturulması; kamunun dağınık ve düşük güvenilirlikli uygulamalara sürüklenmesini önleyebilir. Bu nedenle Başkanlığın rolü yalnızca siber savunma değil, güvenli dijital devlet mimarisi kurma kapasitesi olarak da değerlendirilmelidir. TBMM Yapay Zekâ Araştırma Komisyonu Raporu'nun da işaret ettiği üzere veri yönetişimi alanında merkezî bir otorite modeli ihtiyacı daha görünür hâle gelmektedir. Bu ihtiyaç, yeni bir Türkiye Veri Kurumu kurulması ya da mevcut kurumsal yapının dönüştürülmesi şeklinde tartışılabilir. Ancak hangi model benimsenirse benimsensin; ortak veri alanı, veri kalite standartları ve güvenli veri erişimi bakımından merkezî eş güdüm kapasitesinin güçlendirilmesi gerekmektedir.

Kamuda verimlilik artışı önemli bir fırsattır. Ancak bu fırsat; veri mahremiyeti, model güvenliği, dışa bağımlılık ve denetlenebilirlik koşulları sağlanmadan kalıcı bir kurumsal kazanıma dönüşmez. Türkiye

açısından stratejik öncelik, YZ'yi kamu süreçlerine yaymak kadar bu yayılmayı; güvenli, kayıtlı, denetlenebilir ve hesap verebilir bir çerçeveye bağlayabilmektir.

Ekosistem Geliştirme ve Toplumsal Farkındalık

Yetenek açığı, YZ destekli siber güvenlikte en kritik yapısal sorunlardan biridir. Sorun yalnızca veri bilimci veya ML uzmanı eksikliği değildir. Kamu ve kritik sektörlerde; YZ okuryazarlığı, siber güvenlik bilgisi, risk yönetişimi, model denetimi, veri yönetimi ve kamu politikası anlayışını birleştiren hibrit insan kaynağı açığı da bulunmaktadır. Bu nedenle stratejik öncelik; teknik uzman yetiştirmek kadar karar vericiler, hukukçular, denetçiler, satın alma birimleri, üst yönetim ve saha personeli için farklılaşmış kapasite programları oluşturmaktır.

Kamu sektörü açısından sorun daha da belirgindir. YZ kullanan sistemleri satın alan, işleten, denetleyen ve bunların sonuçlarından sorumlu olan insan kaynağının niteliği, sistemin kendisi kadar önemlidir. Kurum içi ölçekte; bilgi güvenliği, veri yönetişimi, insan kaynakları, iç denetim, hukuk ve eğitim birimlerinin birlikte çalışması gerekir. Ulusal ölçekte ise üniversiteler, meslek yüksekokulları, araştırma merkezleri, düzenleyici kurumlar, sektör birlikleri ve özel sektör arasında daha güçlü iş birliği mekanizmalarına ihtiyaç vardır.

Toplumsal farkındalık da bu başlığın ayrılmaz parçasıdır. YZ destekli oltalama, derin sahte içerikler, sentetik kimlikler ve kurumsal taklit girişimleri; yalnızca teknik güvenlik açığı üretmemektedir. Ayrıca toplumsal güveni, kamu kurumlarının meşruiyetini ve bilgi ekosisteminin dayanıklılığını da etkilemektedir. Bu nedenle farkındalık çalışmaları yalnızca bireysel kullanıcı eğitimine indirgenmemelidir. Kamu iletişimi doğrulama mekanizmaları, medya okuryazarlığı, sentetik medya farkındalığı, karar vericiler için kavramsal çerçeve çalışmaları ve sektörler arası ortak tatbikatlar birlikte ele alınmalıdır.

SGB'nin; ekosistem geliştirme, bilinçlendirme, eğitim ve yerli kapasiteyi destekleme rolü bu alanda önemli bir kaldıraç sağlayabilir. Başkanlık; kamu-özel sektör-üniversite iş birliğiyle ortak eğitim programları, teknik rehberler, sektörel farkındalık kampanyaları ve yerli güvenlik ürünlerinin kullanımını destekleyen mekanizmalar geliştirebilir. Böylece güvenlik ekosistemi yalnızca tehditlere tepki veren bir yapı olmaktan çıkıp bilgi üreten, standart geliştiren ve toplumsal direnç oluşturan bir kapasiteye dönüşebilir.

SONUÇ VE TÜRKİYE'NİN HEDEFLERİ

SONUÇ VE TÜRKİYE'NİN HEDEFLERİ

Yapay zekâ (YZ) çağında siber güvenliğin en kritik sorunları; yönetişim, denetim, koordinasyon ve nitelikli insan kaynağı eksikliğidir. YZ destekli tehditler; saldırı maliyetini düşürmekte, saldırıları kişiselleştirmekte, kurumsal karar süreçlerine sızmakta ve kritik altyapılar üzerindeki riskleri daha karmaşık hâle getirmektedir. Buna karşılık savunma tarafında asıl ihtiyaç, daha fazla otomasyon kadar bu otomasyonu; güvenli, izlenebilir ve hesap verebilir biçimde yönetebilmektir.

Mevcut bulgular, tamamen YZ tabanlı bir siber güvenlik mimarisinin tek başına yeterli olmadığını göstermektedir. **YZ sistemleri büyük veri kümeleri üzerinden saldırı örüntülerini, anomali sinyallerini ve olağan dışı davranışları daha hızlı tespit edebilse de insan uzmanların; bağlamı yorumlama, yanlış pozitifleri ayıklama, kritik kararları doğrulama ve kurumsal etkileri değerlendirme kapasitesi hâlen vazgeçilmezdir. Bu nedenle en gerçekçi ve sürdürülebilir yaklaşım, insan uzmanlığını dışlamayan aksine YZ'nin hız ve ölçek avantajını insan denetimiyle birleştiren hibrit savunma modelidir.** Kurumsal kapasite açısından temel mesele; otomasyonun güvenli, denetlenebilir ve sorumluluğu açık biçimde tanımlanmış hâle getirilmesidir.

Türkiye açısından ise asıl mesele; YZ'nin kamu hizmetlerine, kritik altyapılara ve kurumsal süreçlere nasıl bir veri rejimi, denetim yapısı, insan onayı ve tedarik güvenliği modeliyle entegre edileceğidir. Kamu hizmetlerinin geniş ölçüde dijitalleşmiş olması, e-Devlet temelli kullanımın yaygınlığı, kritik sektörlerin yüksek bağlılık düzeyi ve savunma sanayisi tedarik zincirlerinin hassasiyeti dikkate alındığında, YZ destekli siber tehditler yalnızca teknik açıklar üretmez. Aynı zamanda kamu hizmetlerinde aksama, kurumsal karar kalitesinde bozulma, bilgi ekosisteminde manipülasyon, toplumsal güvenin aşınması ve dış teknoloji sağlayıcılarına bağımlılığın derinleşmesi gibi daha geniş sonuçlar doğurur.

Türkiye için öncelik; YZ'yi hızla yaygınlaştırmaktan ziyade yüksek riskli alanlarda kontrollü benimseme, açık görev dağılımı, kayıt tutma yükümlülüğü, insan denetimi, tedarik zinciri görünürlüğü ve kriz anında süreklilik kapasitesi oluşturmaktır. Etkili politika çerçevesi; siber güvenlik, veri yönetişimi, kamu yönetimi, savunma planlaması ve kritik altyapı dayanıklılığını aynı stratejik çerçevede birleştirmek zorundadır. Başka bir ifadeyle YZ, ulusal hazırlık ve stratejik dayanıklılık meselesi olarak ele alınmalıdır.

Türkiye için politika yanıtı; kısa, orta ve uzun vadeli hedeflere dayanan, çok aktörlü ve güvenlik ekosistemiyle bütünleşik bir yol haritası şeklinde kurgulanmalıdır. Bu yol haritası; kamu kurumları, düzenleyici otoriteler, kritik altyapı işletmecileri, özel sektör, savunma sanayisi şirketleri, üniversiteler, meslek ve sivil toplum kuruluşları arasında görev paylaşımı üretmelidir. Aynı zamanda toplumsal farkındalığı artıracak kavramsal çalışmalar, rehberler ve eğitim programlarıyla desteklenmelidir.

Kısa Vadeli Hedefler

- Merkezî koordinasyonun güçlendirilmesi ve YZ destekli siber riskler için ortak bir kurumsal çerçevenin oluşturulması.
- Kamu kurumları, kritik altyapı işletmecileri ve düzenlemeye tabi sektörlerde kullanılan YZ sistemleri için zorunlu envanter çıkarılması.
- YZ sistemlerinin işlediği veri türü, etki ettiği karar süreçleri, sahip olduğu yetki düzeyi ve bağlı olduğu dış servis sağlayıcıların görünür hâle getirilmesi.

- BDM ve ajan tabanlı sistemler için veri sınıflandırması, işlem günlüğü, çıktı doğrulama ve insan onayı gibi asgari güvenlik kurallarının belirlenmesi.
- Yüksek riskli işlemlerde çok katmanlı doğrulama süreçlerinin güncellenmesi.
- SGB koordinasyonunda kamu genelinde ortak uygulama esaslarının belirlenmesi.

Orta Vadeli Hedefler

- Regülasyon, standart, denetim ve sektörel dayanıklılık mekanizmalarının kurumsallaştırılması.
- Kritik altyapılar ve kamu hizmetlerinde kullanılan YZ sistemleri için sektörel teknik standartların geliştirilmesi.
- Kamu alımlarında güvenlik, denetlenebilirlik, kayıt tutma, olay raporlama, tedarik zinciri görünürlüğü ve insan denetimi şartlarının açık biçimde tanımlanması.
- SOME yapılanmasının olgunluğunun artırılması ve tehdit istihbaratı paylaşım süreçlerinin YZ kaynaklı riskleri kapsayacak şekilde güçlendirilmesi.
- Olay müdahale süreçlerinin, YZ destekli tehdit senaryolarını içerecek biçimde güncellenmesi.
- Kamuda YZ kullanımına ilişkin veri yönetişimi, yetki sınırları ve sorumluluk zincirinin daha açık hâle getirilmesi.
- Güvenlik ekosisteminin yalnızca olaylara tepki veren bir yapıdan çıkarılarak önleyici, denetleyici ve öğrenen bir yapıya dönüştürülmesi.

Uzun Vadeli Hedefler

- Dış teknoloji bağımlılığının güvenlik sonuçlarını yönetebilen güçlü bir ulusal kapasitenin oluşturulması.
- Test, doğrulama, sertifikasyon ve denetim kapasitesinin geliştirilmesi.
- Uzman insan kaynağını güçlendiren ve kamu, özel sektör ile akademi arasında sürdürülebilir iş birliği sağlayan mekanizmaların kurulması.
- Yerli siber güvenlik ve YZ ekosisteminin desteklenmesi.
- Kritik alanlarda stratejik bağımlılık yaratabilecek dış bileşenlerin daha yakından izlenmesi ve yönetilmesi.
- Kimlik manipülasyonu, derin sahte, sentetik medya ve bilgi güvenliği risklerine karşı toplumsal farkındalığın artırılması.
- YZ'nin; güvenli, denetlenebilir, hesap verebilir ve dayanıklı bir yönetişim çerçevesi içinde yönetilmesini sağlayan kalıcı bir ulusal yapı kurulması.

Sonuç olarak YZ çağında siber güvenlik; sistemleri korumanın ötesinde devlet kapasitesini, kurumsal karar kalitesini, toplumsal güveni ve stratejik özerkliği birlikte yönetme meselesidir. Türkiye açısından başarı ölçütü; YZ'nin güvenli, denetlenebilir, hesap verebilir ve dayanıklı bir ulusal çerçeve içinde yönetilebilmesidir.

KAYNAKÇA

RA -
POR

KAYNAKÇA

1 A. J. Gonçalves de Azambuja, C. Pleske, K. Schützer, R. Anderl, B. Schleich ve V. R. Almeida, "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0-A Survey," Electronics 2023, cilt 12, no. 8, ss. 1-18, 2023.

2 M. Malatji ve A. Tolah, "Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI," AI and Ethics, 2024.

3 Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang ve K.-K. R. Choo, "Artificial intelligence in cyber security: research advances, challenges, and opportunities," Artificial Intelligence Review, cilt 55, ss. 1029-1053, 2022.

4 ENISA, "Enisa Sectorial Threat Landscape," Erişim Adresi: https://www.enisa.europa.eu/sites/default/files/2025-12/ENISA%20Public%20Administration%20TL%202024%20-%20v1.1.pdf [Erişim Tarihi: 14.03.2026].

5 ENISA, "Cybersecurity of Critical Sectors," Erişim Adresi: https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors [Erişim Tarihi: 14.03.2026].

6 NIST, "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations," Erişim Adresi: https://csrc.nist.gov/csrc/media/Presentations/2025/adversarial-machine-learning/images-media/WedPM1.1-ApostolVassilev_presentation.pdf [Erişim Tarihi: 14.03.2026].

7 MITRE ATLAS, "SAFE-AI A Framework for Securing AI-Enabled Systems," Erişim Adresi: https://atlas.mitre.org/pdf-files/SAFEAI_Full_Report.pdf [Erişim Tarihi: 14.03.2026].

8 K. Singh, R. Saxena ve B. Kumar, "AI Security Cyber Threats and Threat-Informed Defense," 8th Cyber Security in Networking Conference (CSNet), ss. 305-312, 2024.

9 Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang ve K.-K. R. Choo, "Artificial intelligence in cyber security: research advances, challenges, and opportunities," Artificial Intelligence Review, cilt 55, ss. 1029-1053, 2022.

10 R. Kaur, D. Gabrijelčič ve T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," Information Fusion, cilt 97, s. 101804, 2023.

11 M. Hasan, M. S. Rahman, J. Helge ve I. H. Sarker, "Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis," Blockchain: Research and Applications, cilt 5, no. 3, s. 100207, 2024.

12 OpenAI, "Disrupting malicious uses of AI: June 2025", Erişim Adresi: https://cdn.openai.com/threat-intelligence-reports/5f73af09-a3a3-4a55-992e-069237681620/disrupting-malicious-uses-of-ai-june-2025.pdf [Erişim Tarihi: 27.03.2026].

13 FBI, "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud", Erişim Adresi: https://www.ic3.gov/PSA/2024/PSA241203 [Erişim Tarihi: 27.03.2026].

14 ENISA, "Cybersecurity of Critical Sectors," Erişim Adresi: https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors [Erişim Tarihi: 14.03.2026].

15 M. Büyükavcılar ve A. Çetin, "Derin Öğrenme ile Resim ve Videolar Üzerinde Derin Sahte Tespiti," Gazi Üniversitesi, Ankara, 2023.

[16] A. Biswas ve W. Talukdar, "Guardrails for trust, safety, and ethical development and deployment of Large Language Models (LLM)," Journal of Science & Technology, cilt 4, no. 6, ss. 55-82, 2023.

[17] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang ve K.-K. R. Choo, "Artificial intelligence in cyber security: research advances, challenges, and opportunities," Artificial Intelligence Review, cilt 55, ss. 1029-1053, 2022.

[18] CISA, "CISA Roadmap for Artificial Intelligence," Erişim Adresi: https://www.cisa.gov/sites/default/files/2025-04/ARCHIVE_20232024CISARoadmapAI508.pdf [Erişim Tarihi: 14.03.2026].

[19] OpenAI, "Disrupting malicious uses of AI: June 2025", Erişim Adresi: https://cdn.openai.com/threat-intelligence-reports/5f73af09-a3a3-4a55-992e-069237681620/disrupting-malicious-uses-of-ai-june-2025.pdf [Erişim Tarihi: 27.03.2026].

[20] OWASP, "Top 10 for Large Language Model Applications 2025," Erişim Adresi: https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-v2025.pdf [Erişim Tarihi: 07.03.2026].

[21] O. F. Al-Dulalimi, "Deep Fake Image Detection Based On Deep Learning Using A Hybrid CNN-LSTM Machine Learning Architectures As Classifiers," Altinbas University, İstanbul, 2024.

[22] NIST, "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations," Erişim Adresi: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2025.pdf [Erişim Tarihi: 14.03.2026].

[23] M. ATLAS, "SAFE-AI A Framework for Securing AI-Enabled Systems," Erişim Adresi: https://atlas.mitre.org/pdf-files/SAFEAI_Full_Report.pdf [Erişim Tarihi: 14.03.2026].

[24] R. M. Rajendran ve B. Vyas, "Cyber Security Threat And Its Prevention Through Artificial Intelligence Technology," International Journal for Multidisciplinary Research (IJFMR), cilt 5, no. 6, 2023.

[25] CISA, "CISA Roadmap for Artificial Intelligence," Erişim Adresi: https://www.cisa.gov/sites/default/files/2025-04/ARCHIVE_20232024CISARoadmapAI508.pdf [Erişim Tarihi: 14.03.2026].

[26] K. Dhanushkodi ve S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," IEEE Access, cilt 12, ss. 173127-173136, 2024.

[27] K. Singh, R. Saxena ve B. Kumar, "AI Security Cyber Threats and Threat-Informed Defense," 8th Cyber Security in Networking Conference (CSNet), ss. 305-312, 2024.

[28] UNICRI, "Malicious Uses and Abuses of Artificial Intelligence," Erişim Adresi: https://unicri.org/sites/default/files/2020-11/AI%20MLC.pdf [Erişim Tarihi: 27.03.2026].

[29] A. Biswas ve W. Talukdar, "Guardrails for trust, safety, and ethical development and deployment of Large Language Models (LLM)," Journal of Science & Technology, cilt 4, no. 6, ss. 55-82, 2023.

[30] OWASP, "Top 10 for Large Language Model Applications 2025," Erişim Adresi: https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-v2025.pdf [Erişim Tarihi: 07.03.2026].

[31] E. A. I. Act, "Annex III: High-Risk AI Systems Referred to in Article," Erişim Adresi: https://artificialintelligenceact.eu/annex/3 [Erişim Tarihi: 14.03.2026].

[32] R. Kaur, D. Gabrijelčič ve T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," Information Fusion, cilt 97, s. 101804, 2023.

[33] OECD, "Artificial Intelligence, Data And Competition," Erişim Adresi: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/artificial-intelligence-data-and-competition_9d0ac766/e7e88884-en.pdf [Erişim Tarihi: 14.03.2026].

[34] E. A. I. Act, "Annex III: High-Risk AI Systems Referred to in Article," Erişim Adresi: https://artificialintelligenceact.eu/annex/3 [Erişim Tarihi: 14.03.2026].

[35] J. K. Nguyen, "Human bias in AI models? Anchoring effects and mitigation strategies in large language models," Journal of Behavioral and Experimental Finance, cilt 43, 2024.

[36] K. Dhanushkodi ve S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," IEEE Access, cilt 12, ss. 173127-173136, 2024.

[37] OECD, "Going Digital Guide to Data Governance Policy Making," Erişim Adresi: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/going-digital-guide-to-data-governance-policy-making_28519d90/40d53904-en.pdf [Erişim Tarihi: 14.03.2026].

[38] E. A. I. Act, "Annex III: High-Risk AI Systems Referred to in Article," Erişim Adresi: https://artificialintelligenceact.eu/annex/3 [Erişim Tarihi: 14.03.2026].

[39] OECD, "Artificial Intelligence, Data And Competition," Erişim Adresi: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/artificial-intelligence-data-and-competition_9d0ac766/e7e88884-en.pdf [Erişim Tarihi: 14.03.2026].

[40] T. C. Ulaştırma ve Altyapı Bakanlığı, "Ulusal Siber Güvenlik Stratejisi 2024-2028," 2024. Erişim Adresi: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2024-2028.pdf [Erişim Tarihi: 07.03.2026].

[41] CISA, "Principles for the Secure Integration of Artificial Intelligence in Operational Technology," America's Cyber Defense Agency, Erişim Adresi: https://www.cisa.gov/resources-tools/resources/principles-secure-integration-artificial-intelligence-operational-technology [Erişim Tarihi: 14.03.2026].

[42] I. G. A. Cruz, "Security against Cyber Threats Using Artificial Intelligence," Library Progress International, cilt 44, no. 3, ss. 3253-3259, 2024.

[43] OECD, "AI, data governance and privacy," Erişim Adresi: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/ai-data-governance-and-privacy_2ac13a42/2476b1a4-en.pdf [Erişim Tarihi: 07.03.2026].

[44] E. Commission, "AI Act," Erişim Adresi: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai [Erişim Tarihi: 14.03.2026].

[45] CISA, "Principles for the Secure Integration of Artificial Intelligence in Operational Technology," America's Cyber Defense Agency, Erişim Adresi: https://www.cisa.gov/resources-tools/resources/principles-secure-integration-artificial-intelligence-operational-technology [Erişim Tarihi: 14.03.2026].

[46] USOM, "Ulusal Siber Olaylara Müdahale Merkezi," Erişim Adresi: https://www.usom.gov.tr [Erişim Tarihi: 07.03.2026].

[47] USOM, "Sektörel SOME Kurulum ve Yönetim Rehberi," Erişim Adresi: https://dsy.usom.gov.tr/usom/19/02/190211090404_Sektorel%20SOME%20Rehberi.pdf [Erişim Tarihi: 14.03.2026].

[48] USOM, "Kurumsal SOME Kurulum ve Yönetim Rehberi," Erişim Adresi: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/kurumsal-some-reh-v1.pdf [Erişim Tarihi: 14.03.2026].

[49] E. A. I. Act, "Annex III: High-Risk AI Systems Referred to in Article," Erişim Adresi: https://artificialintelligenceact.eu/annex/3 [Erişim Tarihi: 14.03.2026].

[50] NATO, "Summary of NATO's revised Artificial Intelligence (AI) strategy," Erişim Adresi: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy [Erişim Tarihi: 14.03.2026].

[51] E. Commission, "The Commission moves forward on cloud sovereignty with a EUR 180 million tender," Erişim Adresi: https://commission.europa.eu/news-and-media/news/commission-moves-forward-cloud-sovereignty-eur-180-million-tender-2025-10-10_en [Erişim Tarihi: 14.03.2026].

[52] E. Commission, "Toolbox to improve ICT supply chain security," Erişim Adresi: https://ec.europa.eu/newsroom/dae/redirection/document/124123 [Erişim Tarihi: 14.03.2026].

[53] e-Devlet, "e-Devlet Kapısı İstatistikleri, 2024," Erişim Adresi: https://www.turkiye.gov.tr/resmi-istatistik-programi?y=2024 [Erişim Tarihi: 14.03.2026].

[54] T.C. Resmî Gazete, "Siber Güvenlik Kanunu," Erişim Adresi: https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm [Erişim Tarihi: 14.04.2026].

[55] T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, "On İkinci Kalkınma Planı (2024-2028)," Erişim Adresi: https://www.sbb.gov.tr/wp-content/uploads/2023/12/On-Ikinci-Kalkinma-Plani_2024-2028_11122023.pdf [Erişim Tarihi: 14.04.2026].

[56] T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, "Ulusal Yapay Zeka Stratejisi (2021-2025)," Erişim Adresi: https://bilgem.tubitak.gov.tr/wp-content/uploads/sites/8/TR-UlusalYZStratejisi2021-2025.pdf [Erişim Tarihi: 14.04.2026].

[57] Türkiye Büyük Millet Meclisi, "Yapay Zekânın Kazanımlarına Yönelik Atılacak Adımların Belirlenmesi, Bu Alanda Hukuki Altyapının Oluşturulması ve Yapay Zekâ Kullanımının Barındırdığı Risklerin Önlenmesine İlişkin Tedbirlerin Belirlenmesi Amacıyla Kurulan Meclis Araştırması Komisyonu Raporu" Erişim Adresi: https://cdn.tbmm.gov.tr/KKBSPublicFile/D28/Y1/T10/DosyaKomisyonRaporunuVerdi/9f0e7abf-41f6-4133-ab3d-4879113f7f9f.pdf [Erişim Tarihi: 14.04.2026].

[58] T.C. Resmî Gazete, "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun," Erişim Adresi: https://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm [Erişim Tarihi: 14.04.2026].

NOTLAR

RA-
POR

YAPAY ZEKÂ ÇAĞINDA SİBER GÜVENLİK VE TÜRKİYE'NİN STRATEJİK ÖNCELİKLERİ

NİSAN 2026