AVİM Yorum • No: 2026 / 31 • Mart 2026

NATO'NUN DİJİTAL AÇIKLARI: GÜNEY KAFKASYA'DA ERMENİSTAN'IN ABD DESTEKLİ YAPAY ZEKA MEGA PROJESİ

Teoman Ertuğrul TULUN

Analist

Bu yazı AVİM tarafından ilk olarak 3 Mart 2026'da yayınlanmış İngilizce bir makalenin betimleyici Türkçe çevirisidir.

Giriş

Ermenistan merkezli yapay zeka mega projesi , önemli dış finansal ve siyasi katkıyla desteklenen, hızla genişleyen bir yüksek teknoloji girişimi olarak tanıtılmış ve gelecekteki bölgesel bir "yapay zeka merkezi" olarak sunulmuştur.[1] Kamuoyunda, bu proje büyük ölçüde inovasyon, yatırım ve dijital modernizasyonunun amiral gemisi olarak nitelendirilmiş ve dönüştürücü ekonomik potansiyeli vurgulanmıştır.

Ancak bu yorumız, sözkonusu projeyi tarafsız bir teknoloji parkı olarak değil, öncelikle bir güvenlik ve kritik dijital altyapı meselesi olarak ele almaktadır. Bu çerçevede, NATO üyelerinin önemli yapay zeka ve bulut kapasitelerinin, çözülmemiş çatışmaların ve değişen ittifakların bölgesel düzenin ve işbirliğine dayalı güvenliğin tutarlılığını zorladığı, NATO üyesi olmayan, jeopolitik açıdan kırılgan ortamlara yerleştirmelerinin ne ölçüde isabetli olduğu sorusunu sormaktadır.[2]

Bölgesel güvenlik ve bulut kesintileri

Bu bağlamda, Türkiye, Azerbaycan, Gürcistan ve İran arasında, Rusya'nın genişletilmiş güvenlik çemberi içinde yer alan Güney Kafkasya'da bulunan Ermenistan, NATO üyesi değildir ve savaş sonrası anlaşmazlıklar ile çözülmemiş sınır ve statü sorunları ile uğraşmaya devam etmektedir. Ermenistan'ın güvenlik duruşu, İttifak'ınkine benzer kolektif savunma garantilerine dahil olmaksızın, Rusya'ya olan özgün bağımlılıktan kademeli olarak uzaklaşmasıyla şekillenmiştir. [3]

Aynı zamanda, ABD-İsrail-İran çatışmasının yoğunlaştığı bir dönemde Körfez'deki büyük bulut veri merkezlerinin "nesneler" tarafından vurulması sonucu elektrik ve internet bağlantısının kesilmesi, görünüşte tarafsız olan dijital altyapının hızla kinetik, diğer bir

deyişe hareketli nitelikte fiziksel risklere maruz kalabileceğini göstermiştir. Bu gelişmeler bir arada değerlendirildiğinde, ihtilaflı bölgelerdeki büyük yapay zeka ve bulut tesislerinin, tamamen ticari veya teknolojik bir bakış açısıyla değil, bölgesel güvenliğin daha geniş bir hukuk-tarih-politika çerçevesi içinde analiz edilmesi gereği ortaya çıkmaktadır . [4]

Kritik altyapı, işbirliğine dayalı güvenlik, stratejik bağımlılık

Yukarıda özetlenen bölgesel tablo, büyük yapay zeka ve bulut sistemlerini, öncelikle yatırım büyüklüğü veya yenilik getirme söylemiyle değerlendirilen sıradan "teknoloji parkları" olarak değil, mevcut güvenlik mimarilerine gömülü kritik dijital altyapı olarak kavramsallaştırmasını gerekli kılmaktadır. İttifak ve ortaklık ortamlarında, işbirliğine dayalı güvenlik kavramı, bu tür altyapıyı paylaşan devletlerin temel tehdit algılarını, antlaşma yükümlülüklerini ve kriz yönetimi normlarını da paylaştığını varsayar; bu ortak temel eksik olduğunda ise, karşılıklı bağımlılık ek bir kırılganlık kanalı haline gelebilir.

NATO müşterek savunma mantığı, hayati yeteneklerin İttifak içinde veya İttifak'ın koruması altında güvenilir bir şekilde mevcut olacağı varsayımına dayanır. Sözkonusu NATO bağlamında, önemli dijital varlıkların müttefik olmayan bölgelere taşınması, resmi garantiler ile fiili operasyonel dayanıklılık arasında boşluklar oluşması riskini beraberinde getirir. Bu bağlamda, stratejik bağımlılık kavramı merkezi bir önem kazanır. Vazgeçilmez veri işleme, depolama ve yapay zeka yetenekleri, çözülmemiş güvenlik ikilemleri olan müttefik olmayan bölgelere dış kaynak olarak verilirse, ittifak üyeleri, bu yeteneklere en çok ihtiyaç duyulablilecek dönemlerde siyasi baskıya, kinetik bozulmaya veya erişim engellemesine asimetrik bir şekilde maruz kalma riskini almış olurlar.

İttifak güvenliği perspektifinden Ermenistan'ın yapay zeka merkezi

Bu kavramsal çerçevede, Ermenistan merkezli yapay zeka merkezi, yenilik, yatırım ve yetenek çekme söylemi olarak kamuoyuna sunulmakta ve kendisini dijital dönüşüm ve bölgesel modernizasyonun motoru olarak tanıtmaktadır. Ancak bu anlatı, arka planı ve kavramsal bölümlerde vurgulanan unsurlar itibariylei tam olarak parantez içine alınması gereken bir nitelik taşımaktadır. Zira, yukarıda belirtildiği üere, Ermenistan'ın çözülmemiş çatışmaları, NATO ile karşılaştırılabilir herhangi bir müşterek savunma sistemi dışında kalması ve diğer çatışma bölgelerindeki büyük bulut altyapılarının kanıtlanmış kırılganlıkları mevcuttur.

Mevzuata uygunluk ve ihracat kontrol izinlerine yapılan vurgu, sağlamlık imajı yaratmaktadır. Ancak bu tür yasal-bürokratik filtreler, kritik tesisler üzerinde tırmanma, hedef alma veya zorlayıcı etki gibi fiziksel ve jeopolitik riskleri kendi başlarına ele almamaktadır. NATO üyeleri veya müttefik kurumlar, böyle bir ortamda hassas yapay zeka iş yüklerine maruz kalır, verilere ihtiyaç duyarsa, ticari dış kaynak kullanımı ile güvenlikle ilgili temel işlevlerin fiilen devri arasındaki ayrım giderek bulanıklaşacaktır.

Diğer taraftan, siber savunmayı, denizcilik ve konvansiyonel alanları giderek daha fazla

bütünsel bir biçimde ele alan Türkiye'nin geniş bölgesel güvenlik perspektifinden bakıldığında ise, toprak/ülke savunma ilkeleri ile kritik dijital altyapıların dışsallaştırılması arasında ortaya çıkabilecek bu tür tutarsızlıklar, stratejik istikrarın zaten kırılgan olduğu Güney Kafkasya-Karadeniz kemeri boyunca zaafiyetler yaratma riski taşımakta ve bu nedenle Türkiye açısından özellikle sorunlu görünmektedir.[5]

Normatif değerlendirme ve politika açısı

Ermenistan'ın istikrarsız güvenlik ortamı ve diğer çatışma bölgelerindeki büyük bulut altyapılarının kanıtlanmış kırılganlığı göz önüne alındığında, görev açısından kritik AI ve veri kapasitelerinin NATO dışı bölgelere taşınması, İttifak için hem normatif hem de stratejik açıdan sorunlu görünmektedir. İşbirliğine dayalı güvenlik perspektifinden bakıldığında, savunma, kriz yönetimi veya stratejik iletişimin temelini oluşturan önemli dijital kapasitelerin, müşterek savunma garantilerinin dışında ve çözülmemiş bölgesel anlaşmazlıklara maruz kalan yerlerde barındırılmasına ilişkin bir düzenlemeyi haklı çıkarmak zordur. [6]

Karadeniz'den Güney Kafkasya'ya uzanan tek bir bölgesel güvenlik kompleksinin birbiriyle bağlantılı boyutları olarak siber, dijital ve deniz alanlarını giderek daha fazla kavramsallaştıran Türkiye için, bu dışsallaştırma, yukarıda esasen önemle vurgulandığı üzere, zaten kırılgan olan istikrar yayına yeni kırılganlıklar getirme riski taşımaktadır. Bu nedenle, ihtiyatlı bir yaklaşım, NATO üyeleri ve bölgesel ortakların, vazgeçilmez dijital altyapıyı ittifak sınırları içinde tutmaya öncelik vermelerini veya en azından ittifak dışı barındırma işlemlerini, erişim, koruma ve kriz zamanlarında karar almayı açıkça düzenleyen, anlaşma benzeri sağlam çok taraflı güvencelere tabi tutmalarını elzem kılmaktadır.

Sonuç

Güney Kafkasya'daki bölgesel güvenlik ortamı, yakın çatışma bölgelerindeki bulut altyapılarının kanıtlanmış kırılganlığı ve NATO'nun kendine özgü ittifak-güvenlik mantığı, hep birlikte aynı sonuca işaret etmektedir: AI ve bulut sistemlerinin coğrafyasının, müşterek savunma ve yasal sorumluluk coğrafyasını aşmasına izin verilmemelidir. Ermenistan merkezli yapay zeka merkezi, ihtilaflı bölgelerdeki yüksek teknoloji projelerinin, caydırıcılık, kriz yönetimi ve savunma planlaması için giderek daha merkezi hale gelen yeteneklere ev sahipliği yaptıklarında nasıl yeni stratejik bağımlılık biçimleri yaratabileceğini göstermektedir. Türkiye ve diğer NATO üyeleri için bu, yatırım veya yenilik dar bir odaklanma yerine, hem bölgesel anlaşmazlıkları hem de ittifak taahhütlerini ciddiye alan bir hukuk-tarih-siyaset merceğinden benzer girişimlerin sürekli izlenmesini gerektirmektedir. Kavramsal tutarlılık, kritik dijital altyapıların, yerleşik müşterek güvenlik çerçevelerinin ötesinde güvenli bir şekilde dışsallaştırılabilecek bağımsız teknik girişimler olarak değil, işbirliğine dayalı güvenlik ve bölgesel düzenin ayrılmaz bileşenleri olarak anlaşılmasını ve düzenlenmesini gerektirmektedir.

Resim: DPIndia

[1] HPC Wire Editörlüğü, Firebird ve ABD Hükümeti Ermenistan AI Megaprojesini 4 Milyar Dolarlık İkinci Aşamaya Taşıyor, HPC Wire, 10 Şubat 2026, erişim tarihi 02 Mart 2026 , https://www.hpcwire.com/off-the-wire/firebird-and-us-government-move-armenia-ai-megaproject-into-4b-phase-two/

[2] Labarre, F. ve Niculescu, G. (ed.), Güney Kafkasya için Yeni Güvenlik Düzenlemeleri? Güney Kafkasya Çalışma Grubu (RSSC SG), 26. Çalıştay raporu, Avusturya Ulusal Savunma Akademisi, 2024; Teoman Ertuğrul Tulun, NATOnun Siber Güvenlik ve Denizcilik Stratejisinin Entegrasyonu: Montrö Sözleşmesinin Korunması, AVİM Analizi No: 2024/12 (ve PDF versiyonu Analiz No: 2024/12, 6 Ağustos 2024) https://avim.org.tr/en/Analiz/INTEGRATING-NATO-S-CYBERSECURITY-AND-MARITIME-STRATEGY-UPHOLDING-THE-MONTREUX-CONVENTION

[3] Tutku Dilaver, Güney Kafkasyada Güvenlik Dengesi, AVİM Analizi No: 2023/02 (19 Ocak 2023) https://avim.org.tr/en/Analiz/SECURITY-BALANCE-IN-SOUTH-CAUCASUS ; Emil Avdaliani, NATO ve Güney Kafkasya: Vizyon Eksikliği mi, Stratejik Geri Çekilme mi?, Caucasus Watch, [yayın tarihi], erişim tarihi 02 Mart 2026, https://caucasuswatch.de/en/insights/nato-and-the-south-caucasus-lack-of-vision-or-strategic-withdrawal.html; Kuzey Atlantik Antlaşması Örgütü (NATO), Ermenistan ile İlişkiler, son güncelleme 29 Mayıs 2024, erişim tarihi 02 Mart 2026, https://www.nato.int/en/what-we-do/partnerships-and-cooperation/relations-with-armenia

[4] India Time Editorial, İran-İsrail Savaşı: Amazon Cloud Unit, İran Saldırıları Sırasında Bahreyn ve BAE Veri Merkezlerinde Sorunlara Dikkat Çekiyor, The Economic Times 2 Mart 2026, erişim tarihi 2 Mart 2026, https://economictimes.indiatimes.com/tech/technology/iran-israel-war-amazon-cloud-unit-flags-issues-at-bahrain-uae-data-centers-amid-iran-strikes/articleshow/128939726.cms

[5] Dr. Frédéric Labarre ve Dr. George Niculescu, eds., Güney Kafkasya için Yeni Güvenlik Düzenlemeleri: Güney Kafkasyada Bölgesel İstikrar Çalışma Grubunun 26. Çalıştayı Politika Önerileri (Viyana: Bundesministerium Landesverteidigung Aralık 2023, 1-4, https://www.bmlv.gv.at/wissen-forschung/publikationen/publikation.php?id=1186

[6] Kuzey Atlantik Antlaşması Örgütü. Siber Savunma Taahhüdü. Varşova Zirvesi, 9 Temmuz 2016. Erişim tarihi: 02 Mart 2026. https://www.nato.int/cps/en/natohq/official_texts_133177.htm

Yazar Hakkında :

Teoman Ertuğrul Tulun , Avrasya İncelemeleri Merkezi'nde (Ankara) analisttir. Dr. Teoman Ertuğrul Tulun, Siyaset Bilimi ve Kamu Yönetimi doktorasını Ankara İhsan Doğramacı Bilkent Üniversitesi'nde tamamladı. Avrupa Birliği Çalışmaları, Küreselleşme, Yabancı Düşmanlığı, Nefret Söylemi Çalışmaları ve Uluslararası İlişkiler *alanlarında çalışmalar yapmaktadır.*

Atıfta bulunmak için: TULUN, Teoman Ertuğrul. 2026. "NATO'NUN DİJİTAL AÇIKLARI: GÜNEY KAFKASYA'DA ERMENİSTAN'IN ABD DESTEKLİ YAPAY ZEKA MEGA PROJESİ." Avrasya İncelemeleri Merkezi (AVİM), Yorum No.2026 / 31. Mart 12. Erişim Temmuz 03, 2026. https://mail.avim.org.tr/tr/Yorum/NATO-NUN-DIJITAL-ACIKLARI-GUNEY-KAFKASYA-DA-ERMENISTAN-IN-ABD-DESTEKLI-YAPAY-ZEKA-MEGA-PROJESI

Süleyman Nazif Sok. No: 12/B Daire 3-4 06550 Çankaya-ANKARA / TÜRKİYE
Tel: +90 (312) 438 50 23-24 • **Fax**: +90 (312) 438 50 26
@avimorgtr
https://www.facebook.com/avrasyaincelemelerimerkezi
E-Posta: info@avim.org.tr
http://avim.org.tr