# Siber Tehdit İstihbaratı İçin Üretici Yapay Zeka Modelleri

Yadigar İmamverdiyev
Azerbaycan Teknik Üniversitesi

## Giriş

Günümüzde siber saldırılar sadece teknik sistemleri değil, ulusal güvenliği de tehdit ediyor. Bu tehditlere karşı önleyici tedbirlerin alınması ve siber tehdit istihbaratı (STİ) yapılması hayati önem taşımaktadır. Ancak tehditlerin ölçeği ve karmaşıklığı arttıkça, insan temelli yaklaşımlar yeterli olmuyor. Burada yapay zeka (YZ) yeni bir aşamanın temellerini atıyor. Üretken Yapay Zeka'nın bu alanda çok çeşitli potansiyel uygulama alanları bulunmaktadır. Bu raporun amacı, siber tehdit istihbaratı alanında üretken yapay zekâ modellerinin potansiyel yeteneklerini analiz etmek ve gelecek vaat eden araştırma konularını belirlemektir.

**Siber tehdit istihbaratı.** STİ yaşam döngüsü planlama, toplama, işleme, analiz, paylaşım ve geri bildirim süreçlerini içerir. Planlama aşaması, tehdit bilgilerinin nasıl toplanacağını, analiz edileceğini, uygulanacağını ve paylaşılacağını belirler. Toplama sürecinde siber tehdit istihbaratına yönelik veriler çeşitli kaynaklardan toplanır. İşleme aşamasında toplanan veriler yapılandırılır ve analize hazır hale getirilir. Analiz sürecinde istihbarat bilgileri değerlendirilir, anomaliler ve tehdit göstergeleri belirlenir.

STİ kaynakları arasında açık kaynaklar (OSINT), kapalı kaynaklar, tehdit istihbarat platformları, karanlık web izleme ve teknik kaynaklar yer almaktadır.

STİ, stratejik, taktik, operasyonel ve teknik düzeylerde uygulanmakta olup, her düzey farklı amaçlara hizmet etmekte, içeriği ve hedef kitlesi farklılık göstermektedir.

**Üretken YZ modelleri.** Üretken modellerin tarihi, HMM (Gizli Markov Modeli) ve GMM (Gauss Karışım Modeli) modellerinin oluşturulduğu 1950'lere kadar uzanmaktadır. Bu üretken modellerin geliştirilmesinde önemli bir atılım ancak derin öğrenmenin ortaya çıkmasıyla sağlandı. Üretken Çatışmacı Ağların (GAN) tanıtılmasıyla bu modellerin üretken gücü önemli ölçüde artırılmıştır. ChatGPT şu anda üretken yapay zekanın gücünü kamuoyuna gösteriyor. Birçok üretken teknolojinin temelinde BERT ve GPT gibi büyük dil modelleri (LLM) için uygulanan dönüştürücü mimari yer alır.

**STİ'de üretken YZ modellerinin potansiyel uygulamaları.** Transformatörlerin metin analizi ve üretimindeki potansiyeli göz önüne alındığında, siber tehdit istihbaratında kullanımları aşağıdaki yönlerde analiz edilebilir:

- STİ verilerinin otomatik işlenmesi – derin öğrenme modelleri, raporlar oluşturmak için açık kaynaklı verileri işleyebilir (T5 ve BART) ve güvenlik raporları ile siber saldırıların otomatik özetleri derlenebilir (T5 ve GPT).

- Anormallik tespiti – zaman serisi dönüştürücüler, ağ trafiğini, günlük dosyalarını ve SIEM verilerini analiz ederek DDoS saldırılarını, SQL enjeksiyonlarını ve diğer anormal faaliyetleri tespit edebilir.

- Kötü amaçlı e-posta tespiti – dönüştürücüler, kimlik avı saldırılarını (BERT ve GPT) tespit etmek ve sahte e-postalardaki anormallikleri belirlemek için e-postaların içeriğini analiz edebilir.

- Kötü amaçlı yazılım analizi – CodeBERT gibi Transformatör tabanlı kod analizi modelleri, kötü amaçlı kodları tespit etmek ve analiz etmek için kullanılır.

• Dark Web izleme – dönüştürücüler (CLIP) Dark Web forumlarında görsel ve metinsel analizler gerçekleştirerek yeni tehdit vektörlerini tespit edebilir.

## Sonuç

Yapay zeka ve özellikle üretken modeller, siber tehditlerin erken tespiti ve öngörülmesinde bir dönüm noktasıdır. Bu yaklaşımlar güvenlik politikasının sadece teknik düzeyde değil stratejik düzeyde de oluşmasını etkilemektedir. Ancak insan denetimi ve etik çerçeveler olmadan bu sistemler risk taşıyabilir.