ETAMER NEXUS: STRATEJİK ANALİZ SERİSİ
Sayı: 2026/01 | WEF Özel Dosyası

Siber Saldırıların Psikolojik Anatomisi: AI Destekli Manipülasyona Karşı Bilişsel Savunma ve Algoritmik Güven Yönetimi

The Psychological Anatomy of Cyber Attacks: Cognitive Defense and Algorithmic Trust Management Against AI-Driven Manipulation

Dr. Alper KÜÇÜK[1]

ETAMER (Eğitim ve Teknoloji Araştırma Merkezi)
E-mail: alperkucuk@etamer.org
ORCID: **https://orcid.org/0000-0002-8084-5032**

Öz

Dünya Ekonomik Forumu (WEF) *Global Cybersecurity Outlook 2026* raporu, siber tehdit aktörlerinin teknik istismar (exploit) yöntemlerinden ziyade, doğrudan insan bilişini hedef alan semantik ve psikolojik operasyonlara yöneldiğini belgelemektedir. Üretken Yapay Zeka (GenAI), siber suçların "ölçeklenebilirliğini" artırırken, insan karar alma mekanizmalarındaki heuristik (sezgisel) açıkları sömüren hiper-gerçekçi manipülasyon araçları sunmaktadır. Bu çalışma, yapay zeka destekli sosyal mühendislik saldırılarının nöro-bilişsel temellerini; **"Amigdala Gaspı" (Amygdala Hijack)**ve **"Limbik Sistemin Ele Geçirilmesi"** kavramları üzerinden analiz etmektedir. Otorite taklidi, semantik ikna ve duygusal tetikleme mekanizmalarını kuramsal bir çerçeveye oturtan makale, teknik savunma katmanlarını tamamlayıcı bir unsur olarak **"Bilişsel Savunma" (Cognitive Defense)** mimarisi önermekte ve Türkiye'nin siber güvenlik doktrininde **"Bilişsel Bağışıklık" (Cognitive Immunity)** inşasının stratejik gerekliliğini tartışmaktadır.

Anahtar Kelimeler: Siber Psikoloji, Bilişsel Savunma, Üretken Yapay Zeka (GenAI), Sosyal Mühendislik, Bilişsel Bağışıklık, Nöro-Siber Güvenlik, Algoritmik Manipülasyon.

Abstract

The World Economic Forum (WEF) *Global Cybersecurity Outlook 2026* report documents a pivotal shift among cyber threat actors from technical exploits toward semantic and psychological operations targeting human cognition. Generative Artificial Intelligence (GenAI) enhances the "scalability" of cybercrime while providing hyper-realistic manipulation tools that exploit heuristic vulnerabilities in human decision-making processes. This paper analyzes the neuro-cognitive foundations of AI-powered social engineering attacks through the lenses of **"Amygdala Hijack"** and **"Limbic System Overriding."** By framing authority impersonation, semantic persuasion, and emotional triggering within a theoretical context, the study proposes a **"Cognitive Defense"** architecture as a critical supplement to technical security layers. Furthermore, it discusses the strategic importance of building **"Cognitive Immunity"** within Türkiye's national cybersecurity doctrine.

Keywords: Cyber Psychology, Cognitive Defense, Generative AI (GenAI), Social Engineering, Cognitive Immunity, Neuro-Cybersecurity, Algorithmic Manipulation.

GİRİŞ

Dijital Ontolojide Güvenin Erozyonu

Siber güvenlik paradigması, geleneksel olarak ağ topolojisi ve veri bütünlüğü üzerine odaklanmıştır. Ancak 2026 projeksiyonları, asıl kırılganlığın "insan-bilgisayar etkileşimi" (HCI) ara yüzündeki bilişsel süreçlerde olduğunu göstermektedir. WEF raporuna göre, yapay zeka sadece saldırı hızını artırmakla kalmamış, aynı zamanda "güvenin dijital temsili"ni manipüle ederek bireylerin gerçeği ayırt etme yetisini (reality testing) hedef almıştır. Bu durum, siber güvenliği salt bir mühendislik probleminden çıkarıp, disiplinler arası bir "algı yönetimi" mücadelesine dönüştürmüştür.

Yapay Zeka Destekli Sosyal Mühendislikte Nöro-Psikolojik Mekanizmalar

GenAI tabanlı saldırılar, insan beyninin kısıtlı işlem kapasitesini ve evrimsel kısa yollarını (cognitive biases) sistematik olarak istismar eder:

- **Limbik Sistemin Hijack/Gasp Edilmesi ve Amigdala Tetiklemesi:** Deepfake ses ve video teknolojileri, kurban üzerinde yüksek düzeyde stres ve aciliyet hissi yaratır. Bu durum, rasyonel kararların verildiği prefrontal korteksin aktivitesini baskılayarak, limbik sistem üzerinden tepkisel ve hatalı kararlar alınmasına (örneğin; yetkisiz fon transferi) yol açar.

- **Sosyal Mühendislikte Semantik Yakınsama:** Büyük Dil Modelleri (LLM), kurbanın dijital ayak izini (Open Source Intelligence - OSINT) tarayarak, kişinin değer yargılarına, mesleki jargonuna ve iletişim tonuna "semantik olarak uyumlu" içerikler üretir. Bu durum, "Benzerlik-Çekim Etkisi" (Similarity-Attraction Effect) üzerinden savunma mekanizmalarını devre dışı bırakır.

"Endüstriyel Ölçekte" İkna: Botlardan Otonom Manipülasyon Ajanlarına

WEF 2026 raporu, siber suçun evriminde "otonom ajanların" rolünü vurgulamaktadır (Bölüm 3.3).

- **Dinamik Sosyal Mühendislik:** Sabit senaryolu oltalama (phishing) saldırılarının yerini, kurbanın tepkilerine göre gerçek zamanlı olarak argüman geliştiren AI ajanları almıştır. Bu ajanlar, Robert Cialdini'nin "İkna İlkeleri"ni (Otorite, Azlık, Karşılıklılık vb.) algoritmik bir hassasiyetle uygular.
- **Bilişsel Yükleme (Cognitive Loading):** Çok kanallı saldırı vektörleri (aynı anda gelen sahte görüntülü arama, SMS ve e-posta), bireyin bilgi işleme kapasitesini aşırı yükleyerek "karar yorgunluğu" (decision fatigue) yaratır ve güvenlik protokollerinin ihmal edilmesine neden olur.

Bilişsel Savunma (Cognitive Defense) Mimarisi ve Stratejik Adaptasyon

Teknik güvenlik katmanları (Firewall, EDR, MFA), insan iradesinin manipüle edildiği senaryolarda yetersiz kalmaktadır. Türkiye için önerilen "Bilişsel Savunma" modeli üç temel analitik katmandan oluşur:

1. **Algoritmik Doğrulama Katmanı (Sentetik Medya Tespiti):** İletişimin insan veya yapay zeka kaynaklı olup olmadığını belirleyen, yerli üretim "Multimodal Deepfake Dedektörleri"nin kurumsal altyapılara entegrasyonu.
2. **Davranışsal Güvenlik Protokolleri (Sıfır Güven İletişimi):** "Güven ama doğrula" prensibinin "Doğrulamadan asla güvenme" (Zero Trust Communication) şekline evrilmesi. Özellikle kritik veri ve finans transferlerinde AI tarafından taklit edilemeyecek "ikincil fiziksel doğrulama" zorunlulukları.
3. **Bilişsel Aşılama (Cognitive Inoculation):** ETAMER bünyesinde geliştirilecek siber-psikolojik simülasyonlar ile bireylerin saldırı tekniklerini önceden deneyimlemesi sağlanarak, gerçek bir saldırı anında "bilişsel bağışıklık" yanıtı geliştirmesi amaçlanmaktadır.

Türkiye İçin Siber-Psikolojik İstihbarat ve Müdahale Ağı

WEF raporu, siber dayanıklılığın "kolektif" olması gerektiğini belirtmektedir. Türkiye'nin siber güvenlik stratejisi, sadece "paket analizi" yapan mühendisleri değil, aynı zamanda "anlatı (narrative) analizi" yapan dil bilimcileri ve davranış bilimcileri de içermelidir.

- **Stratejik Odak:** ETAMER rehberliğinde, kamu ve özel sektör çalışanları için "Yapay Zekâ Manipülasyonu Farkındalık Endeksi" oluşturulmalı ve bu endeks üzerinden periyodik siber psikolojik dayanıklılık ölçümleri yapılmalıdır.

SONUÇ

Algoritmik Çağda İnsan Egemenliğini Korumak

Bu bağlamda araştırma sunduğu panoramada siber güvenlik, artık bir "yazılım güncellemesi" değil, bir "zihin güncellemesi"dir. Yapay zekanın ikna ve manipülasyon kabiliyeti arttıkça, en güçlü savunma hattımız rasyonel şüpheciliğimiz ve eleştirel düşünme yetimiz olacaktır. Türkiye, "Bilişsel Savunma" doktrinini ulusal güvenlik stratejisinin bir parçası haline getirerek, yapay zekanın yarattığı psikolojik asimetriyi dengeleyebilir ve dijital dünyada insan iradesinin egemenliğini koruyabilir.

---

* [1] *Bu çalışma, WEF Global Cybersecurity Outlook 2026 raporunun verileri ve ETAMER'in stratejik eğitim vizyonu doğrultusunda yürütülen teknoloji politikaları araştırmaları kapsamında Nexus Bülteni için hazırlanmıştır. İçerik, yazarın uzmanlık görüşlerini ve kurumun stratejik vizyonunu yansıtmaktadır.*