STRATEJİK ANALİZ SERİSİ

SAYI: 2026/01 | WEF ÖZEL DOSYASI

ETAMER NEXUS

2026 Eşiğinde – Belirsizliği Yönetmek, Geleceği Tasarlamak

EDİTÖRDEN

Değerli Nexus Okurları

> Dünya, teknolojik bir ivmelenmenin ötesinde, dijital varoluşun kurallarının yeniden yazıldığı bir dönemeçte.

Dünya Ekonomik Forumu'nun (WEF) son raporu olan **Global Cybersecurity Outlook 2026**, bizlere sadece bir risk analizi sunmuyor; aynı zamanda siber güvenliğin artık kurumların bodrum katlarından çıkıp, ulusal beka stratejilerinin en tepesine yerleştiğini ilan ediyor.

Bugün, yapay zekanın asimetrik bir silah olarak kullanıldığı, jeopolitik gerilimlerin siber saldırılarla hibritleştiği ve siber eşitsizliğin toplumsal bir yara haline geldiği bir manzarayla karşı karşıyayız. Ancak ETAMER olarak inanıyoruz ki; **siber dayanıklılık sadece bir savunma refleksi değil, bir kültürel uyanıştır.**

Elinizdeki bu özel sayı, WEF'in küresel verilerini Türkiye'nin yerel dinamikleriyle harmanlayarak bir yol haritası sunuyor. Bu sayfalar boyunca, "Yapay Zeka Paradoksu"ndan "Dijital Egemenliğe", "Kuantum Tehditleri"nden "Siber Psikoloji"ye kadar 2026'yı şekillendirecek ana hatları bulacaksınız.

Amacımız sadece korkutmak değil, **"farkındalıkla donatmak."** Çünkü siber uzayda en büyük zırhımız, kullandığımız algoritmalar kadar, o algoritmaları yöneten zihinlerin yetkinliğidir.

Dijital sınırlarda daha güvenli bir gelecek için…

Editör Kurulu, ETAMER Nexus

BÖLÜM 1

Yapay Zeka Paradoksu – Siber Savunma ve Saldırı Arasında Yeni Bir Cephe

Dünya Ekonomik Forumu (WEF) tarafından yayımlanan **Global Cybersecurity Outlook 2026** raporu, siber güvenlik dünyasının tarihinde daha önce görülmemiş bir kırılma noktasına işaret ediyor: **Yapay Zeka (AI) Paradoksu.** Rapor, üretken yapay zekanın (GenAI) siber uzayı hem bir kaos alanına hem de yüksek disiplinli bir savunma kalesine dönüştürdüğünü vurguluyor. Türkiye gibi dijital dönüşüm hızı yüksek ve jeopolitik olarak sıcak bir bölgede bulunan bir aktör için bu paradoks, sadece teknik bir tercih değil, ulusal bir beka meselesidir.

%94

Yapay Zeka Riski

Katılımcıların yapay zekanın siber riskleri temelden değiştirdiğini belirtme oranı

%64

Otonom Savunma

AI tabanlı güvenlik araçlarıyla tehdit algılama sürelerini düşüren kuruluş oranı

%60+

AI Optimizasyonu

Türkiye odaklı sosyal mühendislik saldırılarının yapay zeka tarafından optimize edilme oranı (2026)

1.1. Saldırı Sofistikasyonunda "Hızdan Hassasiyete" Geçiş

WEF 2026 raporuna göre, siber saldırganlar artık kaba kuvvet (brute force) yöntemlerinden ziyade, AI kullanarak **"hiper-kişiselleştirilmiş"** saldırılara yönelmektedir. En büyük korku "yapay zekanın saldırganlara sağladığı asimetrik avantajdır."

Türkiye Analizi ve Dil Bariyerinin Çöküşü: Geçmiş yıllarda Türkiye, Türkçe dil yapısının karmaşıklığı sayesinde küresel oltalama (phishing) saldırılarına karşı doğal bir "dil kalkanına" sahipti. Ancak Büyük Dil Modelleri (LLM), bu bariyeri tamamen ortadan kaldırdı. Bugün, bir saldırgan hiç Türkçe bilmeden, AI yardımıyla kusursuz bir gramer ve kültürel bağlamla saldırı gerçekleştirebilmektedir.

1.2. Otonom Savunma: "Milisaniyeler Savaşı"

Artık insan gözünün ve manuel analizlerin yetişemeyeceği kadar hızlı gelişen saldırılara karşı tek çözüm, **Otonom Güvenlik Operasyon Merkezleri (ASOC)** haline gelmiştir.

Yerli Savunma Ekosistemi: Türkiye, özellikle İHA/SİHA teknolojilerinde elde ettiği otonom yazılım tecrübesini siber güvenliğe tahvil etmeye başlamıştır. ASELSAN ve HAVELSAN gibi kuruluşların yanı sıra, siber güvenlik kümelerindeki yerli girişimler, "Kendi Kendini Onaran Ağlar" (Self-Healing Networks) üzerinde çalışmaktadır.

1.3. "Gölge AI" (Shadow AI) ve Veri Sızıntısı Riski

Çalışanların hassas verileri, kod bloklarını veya stratejik planları analiz ettirmek için halka açık AI araçlarına yüklemesi, 2026'nın en büyük veri sızıntısı kaynağı olarak tanımlanmaktadır. **Türkiye'deki kurumlarda "AI Okuryazarlığı" bir yan yetkinlik değil, temel bir siber güvenlik gerekliliğidir.**

1.4. Algoritmik Manipülasyon ve Dezenformasyon

Raporda siber suçların evrimi başlığı altında ele alınan en tehlikeli unsurlardan biri, AI tarafından üretilen dezenformasyondur. Sadece sistemlere sızmak değil, kamuoyunun algısını manipüle ederek ekonomik ve sosyal istikrarsızlık yaratmak, 2026'nın hibrit tehditleri arasındadır.

Stratejik Öngörü: Türkiye'nin siber güvenlik stratejisi, sadece veriyi korumakla sınırlı kalmamalı; "Bilgi Güvenliği"ni (Information Security), "Gerçeklik Güvenliği" (Truth Security) boyutuna taşımalıdır. Deepfake ve sentetik medya saldırıları, finansal piyasaları manipüle etmekten toplumsal kutuplaşmayı tetiklemeye kadar geniş bir yelpazedeulusal güvenliği tehdit etmektedir.

> **Sonuç:** WEF 2026 raporu bize siber güvenliğin artık bir "itfaiyecilik" (olay müdahalesi) değil, bir "mimari zeka" yarışı olduğunu kanıtlıyor. Türkiye, bu paradoksun içinde yapay zekayı sadece bir araç olarak tüketen değil, onun etik sınırlarını belirleyen, denetleyen ve yerli algoritmalarla kendi dijital sınırlarını koruyan bir aktör olmak zorundadır.

BÖLÜM 2

Dijital Egemenlik ve Jeopolitik Fay Hatları – Türkiye'nin Kritik Altyapı Güvenliği

WEF 2026 raporu, siber güvenliğin artık sadece teknik bir disiplin olmadığını, **jeopolitiğin en tanımlayıcı özelliği haline geldiğini** ilan ediyor. Rapor, küresel liderlerin **%64'ünün** siber stratejilerini doğrudan jeopolitik gerilimlere göre şekillendirdiğini vurgularken, Türkiye gibi enerji koridorlarının, veri hatlarının ve kıtaların kesişme noktasında bulunan ülkeler için **"Dijital Egemenlik"** kavramı yeni bir anlam kazanıyor.

2.1. Siber Uzayda "Gri Bölge" Çatışmaları

Devlet destekli siber aktörler artık sadece casusluk yapmıyor; barış ile savaş arasındaki **"gri bölgede"** kalıcı istikrarsızlık yaratmayı hedefliyor. Türkiye'nin savunma sanayiindeki atılımları ve bölgesel bir güç merkezi olma hedefi, ülkeyi devlet destekli APT (Gelişmiş Sürekli Tehdit) gruplarının birincil hedefi haline getirmektedir.

2.2. Kritik Altyapılar: Enerji, Su ve Deniz Altı Kabloları

WEF 2026 raporu, özellikle deniz altı internet kablolarına ve enerji şebekelerine yönelik artan risklere dikkat çekiyor. Türkiye, **Trans Anadolu Doğalgaz Boru Hattı (TANAP)** gibi devasa enerji projelerinin ve Akdeniz'deki fiber optik hatların güvenliğini sağlamak durumundadır. Enerji şebekelerimizin OT sistemleri, yapay zeka destekli otonom sızma girişimlerine karşı sürekli denetlenmelidir.

2.3. Tedarik Zinciri ve "Güvenilir Tedarikçi" Kavramı

Kuruluşların **%45'inin** tedarik zincirlerindeki siber riskler konusunda hala yeterli şeffaflığa sahip olmaması, 2026'nın en çarpıcı bulgularından biridir. Türkiye, Avrupa ve Asya arasındaki tedarik zincirinde kritik bir halkadır. Yerli üreticilerimizin küresel standartlara uyumu, sadece bir güvenlik meselesi değil, aynı zamanda ihracat kapasitemizi belirleyen bir ekonomik parametredir.

2.4. Dijital Egemenlik ve Veri Milliyetçiliği

WEF, verinin depolandığı coğrafyanın ve üzerinde çalışan yasaların bir **"güç unsuru"** haline geldiğini belirtmektedir. Türkiye'nin "Yerli Bulut" (National Cloud) stratejisi, WEF raporunun işaret ettiği jeopolitik risklere karşı en güçlü savunma mekanizmasıdır. Vatandaş verisinin ve kritik kamu verisinin Türkiye sınırları içerisinde, milli şifreleme algoritmalarıyla korunması, dijital egemenliğin temel taşıdır.

Sonuç: 2026 yılında siber güvenlik, artık sadece bir IT departmanının sorumluluğu değil, Milli Güvenlik Kurulu'nun temel bir maddesidir. Türkiye, coğrafi kaderini dijital bir avantaja dönüştürmek için, kritik altyapılarını yapay zeka ve kuantum sonrası şifreleme teknolojileriyle zırhlandırmalıdır.

BÖLÜM 3

Siber Eşitsizlik ve İnsan Faktörü – Dijital Savunma Kültürünün İnşası

WEF 2026 raporu, siber güvenlik dünyasında giderek derinleşen bir uçuruma dikkat çekiyor: **Siber Eşitsizlik (Cyber Inequity).** Rapora göre, büyük ölçekli kuruluşlar ile KOBİ'ler ve gelişmekte olan ülkeler arasındaki dayanıklılık farkı son iki yılda alarm verici düzeyde artmıştır. Bu bölüm, bu eşitsizliği gidermenin yolunun sadece teknoloji transferinden değil, köklü bir **"insan odaklı dönüşüm"** ve eğitim seferberliğinden geçtiğini analiz etmektedir.

3.1. Yetenek Krizinden "Yetenek Dönüşümüne"

Rapor, dünya genelinde siber güvenlik uzmanı açığının kritik seviyelerde olduğunu, ancak asıl sorunun sayısal eksiklikten ziyade **"beceri uyumsuzluğu"** olduğunu vurguluyor. 2026 yılında bir siber güvenlik uzmanının sadece kod yazması veya ağ izlemesi yetmiyor; aynı zamanda yapay zeka etiği, veri hukuku ve psikolojik operasyonlar konusunda da yetkin olması bekleniyor.

ETAMER'in "Hibrit Uzman" Modeli: ETAMER olarak önerdiğimiz müfredat; teknik bilginin yanına siber psikoloji, kriz yönetimi ve etik liderliği koyarak, Türkiye'nin küresel siber iş gücü pazarındaki rekabetçiliğini artırmayı hedeflemektedir.

3.2. Siber Eşitsizlik: Küçük İşletmeler ve Yerel Yönetimler

WEF raporu, saldırganların artık **"en zayıf halkayı"** hedef aldığını; bunun da genellikle büyük tedarik zincirlerinin bir parçası olan ancak bütçesi kısıtlı KOBİ'ler olduğunu belirtiyor. Türkiye ekonomisinin bel kemiği olan küçük işletmeler, 2026'da "ekosistem güvenliğinin" en kırılgan noktasını oluşturmaktadır.

Toplumsal Dayanıklılık Stratejisi: Siber dayanıklılık sadece elit bir grubun korunduğu bir kale değil, bir **"kamu sağlığı"** meselesi gibi ele alınmalıdır. Belediyelerin, yerel ticaret odalarının ve eğitim kurumlarının siber hijyen standartlarının yükseltilmesi, ulusal siber kalkanımızın bütünlüğünü korumak için elzemdir.

3.3. Siber Psikoloji ve Davranışsal Bariyerler

Yapay zeka destekli dolandırıcılık ve manipülasyon, teknik bir açıktan ziyade **"insan zaafiyetini"** sömürmektedir. 2026 yılında karşılaşılan en büyük tehditler; deepfake seslerle yapılan CEO dolandırıcılıkları ve hiper-kişiselleştirilmiş sosyal mühendislik saldırılarıdır.

Eğitimde Paradigma Değişimi: Artık "şifreni kimseyle paylaşma" düzeyindeki temel eğitimler hükmünü yitirmiştir. ETAMER'in üzerinde çalıştığı **"Bilişsel Bağışıklık"** projeleri, bireyleri gelen dijital bilginin doğruluğunu sorgulayan, manipülasyon tekniklerini tanıyan ve kriz anında panik yerine protokollere uyan "bilinçli dijital vatandaşlar" haline getirmeyi amaçlamaktadır.

3.4. Kuantum Sonrası Çağa İnsan Kaynağını Hazırlamak

WEF raporu, kuantum bilgisayarların mevcut şifreleme sistemlerini kırma potansiyeline atıfta bulunarak, kurumların şimdiden **"kuantum dayanıklı" (quantum-ready)** bir iş gücü yetiştirmesi gerektiğini belirtiyor.

Gelecek Vizyonu: Türkiye'nin matematik ve kriptoloji alanındaki birikimi, kuantum sonrası döneme geçişte en büyük sermayesidir. Genç araştırmacıların post-kuantum algoritmalar üzerinde uzmanlaşması için ETAMER bünyesinde kurulacak burs ve araştırma programlarının önemi bu bölümde vurgulanmaktadır.

> **Sonuç:** 2026 yılında en güçlü siber savunma duvarı, en gelişmiş firewall değil, en yüksek farkındalığa sahip kullanıcıdır. Siber eşitsizliği yenmek, Türkiye'nin dijital refahını korumak için bir tercih değil, bir zorunluluktur. ETAMER, bu eşitsizliği eğitimde fırsat eşitliği ve stratejik yetenek yönetimi ile kapatma misyonunu üstlenmektedir.

BÖLÜM 4

Sessizce Yükselen Tehditler ve ETAMER 2026 Stratejik Yol Haritası

WEF 2026 raporunun en dikkat çekici kısımlarından biri, bugün henüz ana akım gündemde olmayan ancak 2026 ve sonrasında siber güvenliğin temelini sarsacak olan **"sessiz tehditler"** başlığıdır. Bu son bölüm, kuantum bilişimden uzay tabanlı varlıklara kadar uzanan bu yeni sınırları analiz ederken, ETAMER'in bu değişim karşısındaki kurumsal duruşunu ve eylem planını özetlemektedir.

4.1. Kuantum Sonrası Dünya: "Şimdi Topla, Sonra Çöz" Tehdidi

WEF raporu, **"Harvest Now, Decrypt Later" (Şimdi Topla, Sonra Çöz)** stratejisinin siber aktörler tarafından aktif olarak kullanıldığını belirtiyor. Saldırganlar, bugün kıramadıkları şifreli verileri, gelecekteki kuantum bilgisayarlarla çözmek üzere depolamaktadır.

ETAMER'in Kuantum Hazırlığı: Türkiye'nin kritik verilerinin (nüfus, sağlık, finansal kayıtlar) 2030'lu yıllarda savunmasız kalmaması için **PQC (Kuantum Sonrası Kriptografi)** geçiş süreci bugünden başlatılmalıdır. ETAMER, akademik dünyayı ve yerli teknoloji geliştiricileri bir araya getirerek, kuantum-dirençli algoritmaların yerli sistemlere entegrasyonu için bir "Kuantum Siber Güvenlik Çalışma Grubu" kuracaktır.

4.2. Uzay ve Uydu Sistemlerinin Güvenliği

Rapor, küresel internet trafiğinin giderek daha fazla alçak yörünge (LEO) uydularına bağımlı hale geldiğine dikkat çekiyor. Uzay tabanlı varlıklara yönelik bir siber saldırı, sadece iletişimi kesmekle kalmayıp küresel navigasyon ve lojistik sistemlerini felç edebilir.

Stratejik Öngörü: Türkiye'nin uzay programı ve TÜRKSAT uyduları, 2026 siber savunma doktrinimizin bir parçasıdır. ETAMER Nexus, uzay siber güvenliğini (Space Cybersecurity) Türkiye'deki akademik literatüre kazandıracak ilk kapsamlı çalışmaları bu bültenle başlatmaktadır.

4.3. ETAMER 2026 Stratejik Eylem Planı

WEF raporunun sunduğu bu küresel kılavuz ışığında, ETAMER olarak Türkiye'nin siber dayanıklılığını artırmak için şu **3 ana sütun** üzerinde hareket edeceğiz:

1. Algoritmik Savunma

Yapay zekayı sadece bir araç değil, otonom bir savunma sistemi olarak yerelleştirmek.

2. Toplumsal Bilişsel Bağışıklık

Siber güvenliği teknik bir konu olmaktan çıkarıp, ilkokul seviyesinden itibaren bir **"dijital vatandaşlık kültürü"** haline getirmek.

3. Ekosistem Güvenliği

KOBİ'lerden savunma sanayiine kadar uzanan tedarik zincirinde **"hiçbir halkayı geride bırakmayan"** bir denetim ve destek mekanizması kurgulamak.

> **Sonuç:** WEF Global Cybersecurity Outlook 2026 raporu bize tek bir gerçeği fısıldıyor: Siber dayanıklılık bir varış noktası değil, sürekli bir devinim halidir. ETAMER olarak bu bültenle sunduğumuz vizyon, Türkiye'nin siber uzayda sadece savunma yapan bir kale değil; akıl, teknoloji ve etik değerlerle donatılmış, proaktif bir aktör olmasını hedeflemektedir. 2026'nın siber dünyası karmaşık olabilir; ancak doğru strateji, nitelikli insan kaynağı ve milli teknoloji birikimiyle bu karmaşayı bir fırsata dönüştürmek bizim elimizdedir.

ETAMER Nexus Özel Sayısı Sonu. Bu çalışma, Dünya Ekonomik Forumu 2026 raporundaki veriler ışığında ETAMER Araştırma Ekibi tarafından hazırlanmıştır.

SONUÇ

Yeni Bir Siber Toplum Sözleşmesine Doğru

ETAMER Nexus'un bu özel sayısında, 2026'nın siber ufkunu dört temel başlıkta analiz ettik. Ancak bu analizlerin ötesinde, raporun satır aralarından süzülen en net gerçek şudur: **Yalnızca teknoloji ile korunan bir dünya, artık güvenli bir dünya değildir.**

🧠 Zeka, Zeka ile Denetlenmelidir

Yapay zeka saldırılarına karşı yine yapay zeka ile tahkim edilmiş yerli savunma kalkanları şarttır.

🌐 Egemenlik Veride Başlar

Dijital sınırlarımız, en az fiziksel sınırlarımız kadar kutsaldır.

⚖️ Eşitsizlik En Büyük Açıktır

En güçlü kurumumuz ile en küçük KOBİ'miz arasındaki güvenlik farkı, ulusal direncimizin gerçek ölçüsüdür.

Geleceğe Çağrı

Siber güvenlik artık teknik bir departmanın "ticketing" sistemi değil; bir **liderlik sınavı**, bir **eğitim seferberliği** ve topyekûn bir **dayanıklılık mücadelesidir.** ETAMER olarak biz, bu mücadelede akademik derinliği, stratejik akılla birleştirerek Türkiye'nin dijital geleceğine rehberlik etmeye devam edeceğiz.

Unutmayın: 2026'da siber güvenliği sağlayan şey kurulan duvarlar değil, kurulan bağlar olacaktır. Kamu, akademi ve özel sektör arasındaki bu "Kolektif Savunma" bağı, bizi geleceğin sessizce yükselen tehditlerine karşı ayakta tutacak tek kuvvettir.

> **Gelecek, onu bugünden inşa edenlerindir.**
> *Güvenli Yarınlar Dileğiyle.*

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.