resaid.bilgi.org.tr

CREATING SOCIETAL
COGNITIVE RESILIENCE
AGAINST INFORMATION
DISORDERS

resaid

JEAN MONNET
CENTRE OF EXCELLENCE

YAPAY ZEKÂ ÇAĞINDA BİLİŞSEL GÜVENLİK: SENTETİK ETKİYE KARŞI ULUSAL ESNEK-DAYANIKLILIK OLUŞTURMAK

Politika Belgesi No 4 | 2025

Avrupa Birliği tarafından
ortak finanse edilmektedir

İstanbul
Bilgi Üniversitesi

CREATING SOCIETAL
COGNITIVE RESILIENCE
AGAINST INFORMATION
DISORDERS

resaid

JEAN MONNET
CENTRE OF EXCELLENCE

YAPAY ZEKÂ ÇAĞINDA BİLİŞSEL GÜVENLİK: SENTETİK ETKİYE KARŞI ULUSAL ESNEK-DAYANIKLILIK OLUŞTURMAK

Salih Bıçakcı

Politika Belgesi No 4 | 2025

Avrupa Birliği tarafından finanse edilmektedir. Ancak ifade edilen görüş ve düşünceler sadece yazar(lar)a aittir ve Avrupa Birliği veya Avrupa Eğitim ve Kültür Yürütme Ajansı'nın (EACEA) görüşlerini yansıtmak zorunda değildir. Avrupa Birliği ve EACEA bunlardan sorumlu tutulamaz.

Avrupa Birliği tarafından
ortak finanse edilmektedir

İstanbul
Bilgi Üniversitesi

Yapay Zekâ Çağında Bilişsel Güvenlik: Sentetik Etkiye Karşı Ulusal Esnek-Dayanıklılık Oluşturmak

Salih Bıçakçı

Giriş

21. yüzyılda güç, kullanım biçimi, ona karşı verilen mücadelede ve onu savunma yolları açısından köklü bir dönüşüm geçirmiştir. Geçmiş dönemlerde topraklar, sınırlar, kaynaklar ve askeri güç gibi unsurları kapsayan fiziksel güvenlik öncelikliyken, modern dönemdeki güvenliğin odağı yeni, soyut ama aynı derecede önemli bir alanla karakterize edilmektedir: insan zihni. Dikkat, güven, hafıza ve karar verme süreçleri; düşman devletler, siyasi hareketler ve kâr odaklı platformlar tarafından yönetilen etki operasyonlarının başlıca hedefleri haline gelmiştir. Bu yeni araştırma alanı, akademisyenler ve uygulayıcılar arasında genellikle "bilişsel güvenlik" olarak bilinmektedir.

Bilişsel güvenliğin bir kavram olarak yükselişi, Dördüncü Sanayi Devrimi ile yakından ilişkili, daha geniş dönüşümlerle ayrılmaz bir şekilde bağlantılıdır. Yapay zekâ, makine öğrenmesi, her yerde bulunan bağlanmışlık ve algoritmik bilgi arabuluculuğu (algorithmic information mediation), bilgi ortamını yeniden şekillendirerek benzeri görülmemiş bir içerik yoğunluğu ve hızı yaratmıştır. Bu ortam, bilginin aktığı tarafsız bir platformdan ibaret değildir; bireylerin gerçekliği nasıl algıladıklarını, doğruyu yanlıştan nasıl ayırt ettiklerini ve kolektif kararları nasıl aldıklarını aktif olarak şekillendirmektedir. Bu anlamda, bilişsel süreçler, enerji şebekeleri veya finansal sistemler kadar ulusal güvenlik ve demokratik direnç için hayati öneme sahip yeni bir tür kritik altyapı haline gelmiştir.

Ancak sorun şu ki, bilgi güvenliğine yönelik geleneksel yaklaşımlar, bu teknoloji odaklı yeni dönemin zorluklarını ele almak için yeterli donanıma sahip değildir. Son yirmi yılın hâkim çerçeveleri, siber güvenlik ve dezenformasyona odaklanarak, teknik altyapıyı korumaya veya bilgi içeriğinin doğruluğunu sağlamaya yoğunlaşmıştır. Siber güvenlik, güvenilirlik veya tutarlılıktan ziyade, öncelikle veri bütünlüğüne odaklanmıştır. Siber güvenlik, ağları, verileri ve dijital sistemleri kötü niyetli saldırılara karşı korumak için geliştirilmiştir. Dezenformasyona karşı çabalar ise esas olarak gerçeklerin doğrulanması, içerik denetimi ve yanlış iddiaların kontrolü etrafında şekillenmiştir. Her iki yaklaşım da gereklidir, ancak hiçbiri yapay zekâ destekli manipülasyon karşısında yeterli değildir.

Bu yetersizlik, modern tehditlerin geleneksel savunma mekanizmalarını aşmasından kaynaklanmaktadır. Üretken yapay zekâ (Generative AI), "görmek inanmaktır" epistemik temelini aşındıracak kadar gerçekçi sentetik görüntüler, sesler, metinler ve veriler üretebilir. Siyasi liderlerin deep fake'leri, gerçekliği ortaya çıkarılmadan önce geniş çapta yayılabilir. Aynı zamanda, yapay zekâ destekli (ro)botlar ve sohbet aracıları, mesajlarını kişisel hassasiyetlere göre uyarlayarak bireyleri büyük ölçekte ikna edici etkileşimlere dahil edebilir. Aynı zamanda, sosyal medya platformları tarafından yapılan algoritmik küratörlük (algorithmic curation), doğruluğa değil duygusal rezonans (emotional resonance) dayalı içeriği güçlendirerek genellikle kutuplaşmayı ve güvensizliği yoğunlaştırır. Bu dinamikler, doğruluk kontrolü yapanları bir iddiayı çürütmüş olsa bile, kamu güvenine verilen zararın zaten gerçekleşmiş olduğu anlamına gelir.

Bu nedenle, okumakta olduğunuz araştırma odak noktası olarak bilginin içeriğini korumaktan ziyade bilişsel sürecin savunma alanı olarak tanımlanması gerektiğini savunmaktadır. Bilişsel güvenlik, gerçeği denetlemek veya ifade özgürlüğünü bastırmakla ilgili değildir; daha çok, insanların manipülasyon ve aldatma karşısında özerklik, muhakeme ve esnek-dirençliliklerini (resilience) kullanabilmelerini sağlamakla ilgilidir. Yapay zekâ çağında demokratik toplumları güvence altına almak için, bilişsel güvenlik ulusal esnek-dirençliliğin temel direği haline gelmelidir.

Bu argümanın etkileri çok derindir. Belirsizlik altında karar verme, demokrasi, savunma ve kriz yönetiminin temel bir işleviyse, bilişsel zayıflıkları istismar etmek, egemenliği ve istikrarı doğrudan tehdit eder. Vatandaşların gerçek ve sentetik mesajları ayırt edemediği veya kurumlara olan güvenin çöktüğü bir toplum, kendisini etkili bir şekilde yönetemeyen bir toplumdur. Bilişsel güvenliğin aşınması, bu nedenle demokratik meşruiyet ve stratejik esnek-dirençlilik krizine dönüşür.

Bu makalenin kapsamı içinde hem kavramsal hem de politika odaklı konular incelenmektedir. Makale, bilişsel güvenliği tanımlayarak ve onu güvenlik çalışmalarının daha geniş bir alanı içinde konumlandırarak başlamakta ve bilişsel güvenliğin siber güvenlik ve bilgi güvenliğinin ötesine geçerek insan bilişinin kendisinin zayıflıklarını ele aldığını vurgulamaktadır. Ardından, bilgi ortamını dönüştüren bir faktör olarak yapay zekânın rolünü inceleyerek sentetik medya ile algoritmik ikna yöntemlerinin manipülasyon risklerini nasıl artırdığını göstermektedir.

Üçüncü bölümde, NATO, Avrupa Birliği ve Türkiye'deki politika araçlarının eksiklikleri incelenerek, demokrasileri tehditlere karşı savunmasız bırakan temel boşluklar tespit edilmektedir. Dördüncü bölümde, teknik, eğitsel, kurumsal ve toplumsal önlemleri entegre eden bir bilişsel direnç çerçevesi geliştirilmektedir. Son olarak, sonuç bölümünde bu paradigma değişiminin daha geniş kapsamlı etkileri üzerinde durulmakta ve demokrasilerin siber savunmaya yaptıkları kadar acil bir şekilde bilişsel güvenliğe de yatırım yapmaları çağrısında bulunulmaktadır.

Kavramsal analiz ile politika önerilerini birleştiren bu makale, bilişsel güvenliğin hem akademik bir alan hem de stratejik bir zorunluluk olarak anlaşılmasını hedeflemektedir. Makale, psikoloji, güvenlik çalışmaları ve teknoloji politikası alanlarında ortaya çıkan yeni literatürden yararlanırken, argümanını NATO, Avrupa Birliği ve Türkiye bağlamında karşılaştırmalı bir yaklaşımla küresel seviyede ele almaktadır. Nihai hedef, problemi teşhis etmekle kalmayıp bir yol önermektir.

1. Stratejik Bir Alan Olarak Bilişsel Güvenliğin Ortaya Çıkışı

Bilişsel güvenliğin ayrı bir araştırma ve uygulama alanı olarak ortaya çıkışı, devletlerin, kuruluşların ve akademisyenlerin yirmi birinci yüzyılda riski algılama biçimlerinde bir paradigma değişimini ifade etmektedir. Tarihsel olarak, güvenlik çerçeveleri kara, deniz ve hava gibi fiziksel alanlara odaklanmıştı ve daha sonra uzay ve siber uzay ile genişletilmişti. Dijital ortamın ortaya çıkışı ve ağ bağlantılı altyapıların yaygınlaşması, siber güvenliği birincil bir endişe konusu haline getirdi. Artan önemi dolayısıyla siber güvenlik, kendi sınırlılıklarını giderek genişletmiştir. Siber güvenlik, dijital sistemlerin teknik her türlü altyapısını ve bu altyapı içinde iletilen verinin bütünlüğünü, gizliliğini ve ulaşılabilirliğini korur, fakat iletilen bilginin insan bilişi tarafından nasıl işlendiği, yorumlandığı ve üzerinde nasıl hareket edildiği konusunu ele almaz.

Bilişsel güvenlik, siber güvenlik paradigmalarını kısmen temel alır, ancak onlardan da ayrılır. İnsan bilişinin, yani yargılama, güven, hafıza ve karar verme kapasitemizin, başlı başına stratejik bir hedef haline geldiğini kabul eder. James Bone (2017) "bilişsel hackleme" (cognitive hacking) üzerine yaptığı öncü çalışmasında, düşmanların teknik zayıflıkları ve insan psikolojisinin öngörülebilir önyargılarını ve sezgilerini istismar ettiğini savunmuştur. Benzer şekilde, Huang ve Zhu (2023) bilişsel güvenliği sistem bilimsel bir zorluk olarak çerçevelendirerek, insan zihninin toplumları istikrarsızlaştırmak için manipüle edilebilen bilgi, teknoloji ve sosyal etkileşim ağlarına gömülü olduğunu vurgulamaktadır.

Dördüncü Sanayi Devrimi bu dönüşümü hızlandırmıştır. Yapay zekâ, makine öğrenimi, büyük veri analitiği ve her yerde bağlantı olanaklarının hızla yaygınlaşması, bilişsel güvenlik açıklarının büyüdüğü bir bilgi ortamı yaratmıştır. Verimlilik ve kişiselleştirmeyi mümkün kılan özellikler, yani algoritmik küratörlük (algorithmic curation), tahmine dayalı analitik ve gerçek zamanlı iletişim, aynı zamanda istismar için fırsatlar da yaratmaktadır. Bone ve Lee (2023) bilişsel risk üzerine yaptıkları son çalışmada vurguladıkları gibi, kuruluşlar ve hükümetler bu yeni tehditleri hesaba katmak için risk anlayışlarını yeniden kavramlaştırmalıdır.

Bilişsel güvenliğin ortaya çıkışını anlamak için bilgi ve güvenlik paradigmalarının tarihsel gelişimini analiz etmek faydalıdır. Soğuk Savaş döneminde bilgi, öncelikle propaganda ve ideolojik rekabet bağlamında bir çekişme alanı olarak kabul ediliyordu. Odak noktası mesajların içeriğiydi: kim daha ikna edici anlatılar sunabilirdi? 1990'larda İnternet'in ortaya çıkmasıyla dikkatler, ağları, verileri ve dijital altyapıyı yetkisiz erişim ve sabotaja karşı korumayı içeren siber güvenliğe kaydı. 2000'li ve 2010'lu yıllarda, sosyal medyanın yaygınlaşması ve devlet ve devlet dışı aktörler tarafından bilgi akışının silah olarak kullanılması, "bilgi savaşı" ve "dezenformasyon kampanyaları" konusunda endişeleri artırdı.

Her paradigma, değişen ortamın temel bir yönünü yakalamış olsa da bunlar kapsam bakımından sınırlı kalmıştır. Propaganda analizleri, açık mesajlara odaklanmış, ancak bilişsel önyargıların rolünü hafife almıştır. Siber güvenlik, teknik savunmalara odaklanmış, fakat insan yorumunun kırılganlıklarını göz ardı etmiştir. Dezenformasyon çerçeveleri ise içeriğe yoğunlaşmış, yanlışlığın doğruluk kontrolü ve içerik denetimiyle giderilebileceği varsayımına dayanmıştır. Ancak bu paradigmalar, bilginin inanç ve eyleme dönüştüğü zihinsel süreçlerin (bilişin) doğrudan hedef alınabileceği gerçeğini gözden kaçırmıştır.

Bu nedenle, bilişsel güvenlik, psikoloji, nörobilim ve davranışsal ekonomi alanlarından elde edilen bilgileri güvenlik çalışmaları alanına entegre etme girişimini temsil etmektedir. Kahneman ve Tversky'nin (1974) sezgisel yöntemler üzerine yaptıkları çalışmalardan günümüzün motive edilmiş akıl yürütme (motivated reasoning) üzerine yapılan çalışmalara kadar, bilişsel önyargılar üzerine yapılan araştırmalar, insanların rasyonel bilgi işleyiciler olmadığını göstermiştir. Bizi manipülasyona açık hale getiren zihinsel kısayollara (mental shortcuts) güveniriz. Düşmanlar, önceden var olan inançlarla uyumlu içeriği abartarak doğrulama yanlılığı (confirmation bias) veya canlı ama temsil edici olmayan olayları vurgulayarak kullanılabilirlik önyargısını istismar ederler. Bu savunmasızlık sadece bilginin içeriğinde değil, bilişin kendisinin yapısında da yatmaktadır.

Bu farkındalık, derin stratejik sonuçlar doğurur. Düşmanların artık geleneksel anlamda toprakları kontrol etmeye, altyapıyı yok etmeye veya hatta ikna edici anlatılar üretmeye ihtiyaçları olmadığını gösterir. Bunun yerine, şüphe, kafa karışıklığı ve güvensizlik tohumları ekerek toplumları istikrarsızlaştırabilirler. Pomerantsev'in (2019) gözlemlediği gibi, modern bilgi savaşının amacı genellikle insanları belirli bir yalanla ikna etmek değil, gerçeğin olasılığına olan güvenlerini sarsmaktır. Bu ortamda, bilişsel alan çatışmanın belirleyici sahası haline gelmektedir.

NATO bu gerçeği kabul etmeye başlamıştır. NATO'nun "NATO 2030" gündemi, dezenformasyon ve hibrit tehditlerin ele alınmasının önemini vurgulamaktadır ve bilişin kara, deniz, hava, siber ve uzay ile savaşın yeni bir "alanı" olarak kavramsallaştırılması gerekip gerekmediği konusunda tartışmalar artmaktadır. Avrupa Birliği de Avrupa European External Action Service'in East StratCom Task Force gibi girişimler aracılığıyla dezenformasyonu izleme ve dezenformasyonla mücadeleye yatırım yapmıştır. Ancak hem NATO hem de AB, reaktif önlemlerin ötesine geçmekte zorlanmaktadır. Doğruluk kontrolü, karşı anlatılar ve platform düzenlemesi çok önemlidir, ancak bunlar bilişsel süreçten çok bilgi içeriğine odaklanmaktadır.

Türkiye bu konuda özellikle öğretici bir örnek teşkil etmektedir. Avrupa, Orta Doğu ve Avrasya'nın kesişme noktasında bulunan Türkiye, birçok etki ekosistemine maruz kalmaktadır: Rus dezenformasyon kampanyaları, Batı anlatıları, bölgesel mezhepçi propaganda ve iç kutuplaşma. Bu nedenle Türkiye'de bilişsel güvenliğin zorlukları hem dışsal hem de içseldir. Dışsal olarak, düşmanca aktörler dini, etnik ve jeopolitik bölünmeleri kullanarak uyumu zayıflatmaktadır. İçsel olarak ise siyasi kutuplaşma, manipülatif anlatıların kök salması için verimli bir zemin oluşturmaktadır. Türkiye'nin deneyimi, bilişsel güvenliğin ikili doğasını göstermektedir: bu hem dış savunma meselesi hem de iç direnç meselesidir.

Bilişsel güvenliğin bilimsel olarak incelemesi hâlâ erken aşamalarındadır, ancak hızla gelişmektedir. Huang ve Zhu (2023), bilişi daha geniş bir sosyo-teknik sistemin parçası olarak ele alan sistem-bilimsel bir yaklaşım önermektedir. Onlara göre, bilişsel güvenlik; nörobilim, psikoloji, bilgisayar bilimi ve siyaset bilimi alanlarından elde edilen içgörülerin bütünleştirildiği disiplinler arası bir iş birliği gerektirir. Risk yönetimi perspektifinden bakıldığında ise Bone ve Lee (2023), bilişsel kırılganlıkların sistematik olarak tanımlanması, değerlendirilmesi ve azaltılması gereken kurumsal riskler olarak ele alınması gerektiğini vurgulamaktadır. Her iki yaklaşım da bilişin korunması gereken stratejik bir varlık olduğunu kabul etme noktasında birleşmektedir.

Bu bölüm, stratejik bir alan olarak bilişsel güvenliğin ortaya çıkışını haritalandırmayı amaçlamıştır. Mevcut bilgi güvenliği ve siber güvenlik paradigmalarının gerekli olduğu, ancak yapay zekâ destekli manipülasyon bağlamında yetersiz olduğu savunulmuştur. Bilişsel güvenlik, insan bilişinin kendisinin zayıflıklarına odaklanarak bu alanı genişletir. Psikoloji ve davranış bilimlerinden elde edilen içgörülere dayanır ve Dördüncü Sanayi Devrimi'nin dönüşümlerini yansıtır. NATO, AB ve Türkiye örnekleri, bu paradigmanın küresel önemini vurgulamaktadır.

İlerledikçe, bu kavramsal içgörüleri etkili politika çerçevelerine ve pratik stratejilere dönüştürmek bir zorluk oluşturacaktır. Bilişsel güvenlik, siber güvenlik ve fiziksel savunma ile karşılaştırılabilir şekilde, ulusal direncin bir ayağı olarak kurumsallaştırılmalıdır. Ancak, demokratik ilkelere ve insan özerkliğine saygı gösteren şekillerde de uygulanmalıdır. Bu nedenle, bu makalenin sonraki bölümlerinde yapay zekanın bilişsel güvenliği nasıl bozduğu, mevcut politikaların nerede yetersiz kaldığı ve bu zorlukları ele almak için bir direnç çerçevesinin nasıl geliştirilebileceği incelenmektedir.

2. Post-Truth Çağında Bilgi Düzensizliği ve Bilişsel Zafiyetin (Cognitive Vulnerability) Dinamikleri

Günümüzün bilgi ortamında, düzensizlik giderek daha fazla, gerçek ile yanlış, olgu ile görüş, bilgi ile inanç arasındaki sınırların bulanıklaştığı bir durum olarak tanımlanmaktadır. Bu bağlamda, “hakikat sonrası (post-truth) çağı” sadece yanlış bilgilendirilmiş bireyleri ifade etmekle kalmaz, bilgi, biliş ve siyaset arasındaki ilişkide köklü bir dönüşümü de işaret etmektedir. Hakikat sonrası’nın belirleyici özelliği, hakikatin yokluğu değil, onun meşruiyetinin ortadan kalkmasıdır: hakikat, ayrıcalıklı otoritesinden yoksun, birçok anlatıdan sadece biri haline gelir. Bu bağlamda, güvenlik çalışmalarının temel sorusu, yanlış bilgileri düzeltmekten öteye, toplumların gerçeklik hakkında ortak bir anlayış oluşturdukları bilişsel süreçleri korumaya kaymaktadır. Karar verme sürecinde sunulan bilgilerdeki en ufak değişiklikler bile, herhangi bir müdahale olmaksızın alınan kararları önemli ölçüde etkileyebilir.

Yanlış bilginin devamlılığı, geleneksel doğruluk kontrolünün yetersizliğini ortaya koymaktadır. Nyhan ve Reifler (2010), yanlış iddiaların düzeltilmesinin bazen yanlış algıları ortadan kaldırmak yerine pekiştirdiği “geri tepme etkisi’ni (backfire effect) ortaya koymuştur. Benzer şekilde, Vosoughi, Roy ve Aral (2018) yanlış haberlerin, güvenilir haberlere göre sosyal medyada daha hızlı ve daha geniş bir şekilde yayıldığını, bunun da temel nedeninin yanlış haberlerin daha yeni ve duygusal olarak daha ilgi çekici olmasından

kaynaklandığını göstermiştir. Bu bulgular, temel bir bilişsel asimetriyi ortaya koymaktadır: sezgisellik (heuristics) ve duygu odaklı dikkat (emotion-driven attention) gibi insan bilişini verimli kılan mekanizmalar, aynı zamanda onu manipülasyona da açık hale getirmektedir.

> Bilişsel asimetri (cognitive asymmetry), iki aktörün algılama, yorumlama ve karar verme kapasiteleri arasındaki kasıtlı eşitsizliği ifade etmektedir. Bu durum, bir tarafın kendi belirsizliğini ve karar verme gecikmesini sistematik olarak azaltırken, aynı zamanda diğer tarafın kafa karışıklığını, doğrulama maliyetlerini ve karar verme süresini artırarak, zorlama yoluna başvurmadan bir avantaj elde ettiğinde ortaya çıkmaktadır.

Hakikat sonrası koşullarında, düşmanlar artık izleyicileri tutarlı bir yalanla ikna etmek zorunda değillerdir. Bunun yerine, çelişkili iddialarla ortamı boğarak kurumlara olan güveni zayıflatabilir ve kutuplaşmayı istismar edebilirler. RAND (2016) araştırmacıları tarafından ortaya atılan “firehose of falsehood” (Yoğun Yalan Hortumu) adlı Rus stratejisi, bu yaklaşımı örneklemektedir. “Firehose of falsehood” dört farklı özellik ile karakterize edilmektedir: yüksek hacimde çalışmaktadır, birden fazla kanal kullanmaktadır, hızlı ve süreklidir ve gerçeğe veya iç tutarlılığa bağlılık göstermemektedir. Tek bir inandırıcı anlatı kullanmak yerine, devletin sahip olduğu medya kuruluşları, proxy (vekalet) siteler, sosyal medya platformları, botlar ve influencer'lar aracılığıyla yayılan çok sayıda yanlış, bazıları kısmen doğru ve bazıları birbiriyle çelişen anlatılarla izleyicileri boğmaktadır. Asıl amaç, gerçeklerin doğrulanmasında zafer kazanmak değil, kafa karıştırmak, dikkati başka yöne çekmek ve doğrulama çabalarını boşa çıkarmaktır. Sonuç olarak, bunun etkisi yalanlara olan inancı teşvik etmek değil, gerçeğe olan inancı aşındırmaktır. Esasen, bu kampanyalar izleyicilerin gerçeğe ilişkin algılarını manipüle etmeyi ve bilişsel süreçlerini karıştırmayı amaçlamakta ve stratejide bir değişiklik olduğunu vurgulamaktadır.

Bu değişim, bilişsel kırılganlığın doğasını dönüştürmektedir. Bu sadece belirli yanlış iddialara karşı duyarlılık değil, aynı zamanda epistemik otoritenin aşınmasıyla da ilgilidir. Operasyonun doruk noktasında, demokratik sistemlerin temel direklerine olan güveni geri dönülmez bir şekilde aşındıran semantik bir saldırı yatmaktadır. Vatandaşlar artık medyaya, uzmanlara, kurumlara güvenmediğinde demokratik süreçler zayıflamaktadır.

Seçimler, meşru sonuçların ortak kabulüne bağlıdır; halk sağlığı, bilimsel uzmanlığa duyulan güvene dayanmaktadır; kriz yönetimi, yetkili bilgilere kolektif inanç gerektirmektedir. Bu nedenle, epistemik güvenin çöküşü doğrudan siyasi istikrarsızlığa yol açmaktadır. Ayrıca, nüfusun sosyal dayanışmasını da etkilemekte ve toplumun direncini doğrudan etkilemektedir.

Yapay zekânın ortaya çıkışı, daha az çaba ve daha fazla ikna gücüyle bu operasyonları genişletmek için etkili bir platform sağladı. Deepfake, ses klonlama (voice cloning) ve büyük ölçekli metin üretimi gibi üretken yapay zekâ teknolojileri, manipülatif içeriğin hızını, ölçeğini ve inandırıcılığını artırmaktadır. Ukrayna Cumhurbaşkanı Volodymyr Zelensky'nin 2022'de teslimiyeti çağrıştıran bir deep fake videosu, sentetik medyanın duyusal algıdaki bilişsel güveni nasıl hedef alabileceğini göstermektedir (Smalley, 2022). Ses klonlama teknolojileri, finansal dolandırıcılıkta zaten kullanılmaktadır ve siyasi kargaşaya yol açmak için de kolaylıkla kullanılabilir. Yapay zekâ destekli sohbet robotları ve ikna motorları, bireylerin bilişsel zayıflıklarını gerçek zamanlı olarak istismar ederek kişiselleştirilmiş diyaloglar başlatabilir. Algoritmik küratörlük (algorithmic curation), bu tür manipülasyonların hassas hedef kitlelere duygusal olarak yankı uyandıran anlatılar sunarak kesin bir şekilde hedeflenmesini sağlar (ABD Federal Ticaret Komisyonu, 2023, 2024; Damiani, 2019).

Ortam teknolojileri (ambient technologies) akıllı telefonlar ve bedenlerin interneti (Internet of Bodies - IoB), akıllı hoparlörler ve diğer sürekli dinleme mikrofonları, Wi-Fi/RF algılama ve sürükleyici genişletilmiş gerçeklik (XR) dahil olmak üzere, algılama ve harekete geçirme özelliklerini günlük ortamlara ve vücuda yerleştirerek bu yetenekleri genişletir. Algılama aşamasında, cihazlardan ve altyapıdan gelen pasif veriler, varlık, hareket, rutinler ve stres veya uyarılmanın fizyolojik göstergeleri hakkında sürekli sinyaller üretir. Sistematik incelemeler, akıllı telefon ve giyilebilir cihaz tabanlı dijital fenotiplemenin, ruh hali ve stresle ilişkili hareketlilik ve uyku düzenini etkili bir şekilde izleyebildiğini göstermektedir (Bufano vd., 2023; Choi vd., 2024). IoB analizleri, bu veri katmanını besleyen sağlıkla ilgili giyilebilir ve takılabilir cihazların politika ve güvenlik açısından etkilerini vurgulamaktadır (Lee ve ark., 2020). Buna paralel olarak, IEEE 802.11bf protokolü, Wi-Fi (802.11) standardına, sıradan Wi-Fi sinyallerini yalnızca veri iletimi için değil, aynı zamanda ortamda nesne ve insanların varlığını, hareketini, jestlerini, mesafesini ve ilgili özelliklerini algılamak için kullanan resmi ve birlikte çalışabilir bir Wi-Fi algılama çerçevesi ekleyen bir tadilat niteliğindedir (Ropitault vd., 2023; Sahoo ve ark., 2024). Akıllı cihazların günlük hayatımızda her yerde bulunması, önemli miktarda verinin toplanmasına yol açmıştır. Bu veriler, profil oluşturma alanındaki veri analistleri için değerli bir kaynak görevi görmektedir.

Akıllı hoparlörlerin yanlış çalıştırılması konusunda yapılan son araştırmalar, wake-word (akıllı cihazları uyandırma anahtarları: Hey Siri, Hi Samsung vs) hatalarının ortam sesini veya meta verileri istemeden yakalama potansiyelini ortaya koymuştur. Bu fenomen, davranışsal çıkarımların kapsamını genişleterek kullanıcı verilerinin gizliliği ve güvenliği konusunda endişeleri artırmaktadır (Dubois vd., 2020). Operasyonel açıdan, ortam yığınları, açık bir ikna mesajı gösterilmeden önce bile "doğru anı" ve "doğru mikro kitleyi" bulma maliyetini düşürmektedir.

Dağıtım aşamasında, algoritmik küratörlük algorithmic curation (sıralama, bildirim planlama, coğrafi sınırlı uyarılar) içeriği, öngörülen duyarlılık anlarında dikkat çekiciliği en üst düzeye çıkaracak biçimde sıralar. Aynı zamanda, XR, sürükleyici olmayan formatlara kıyasla varlığı ve tanımlamayı geliştirir, bu da belirli bağlamlarda daha güçlü tutum veya davranış değişikliğine yol açabilir (Makransky & Petersen, 2021). Birçok sistem, video, ses, metin veya fizyolojik akışlardan elde edilen tahmini uyarılma/değerlere göre başlıkları, görüntüleri veya tonu uyarlayan duygusal bilgi işlem teknolojisini içerir. Ancak, önde gelen incelemeler, yüz ifadelerinden ayrı duyguları çıkarsamanın bağlamlar arasında genellikle güvenilmez olduğu konusunda uyarıda bulunmaktadır (Barrett vd., 2019).

Nöroteknoloji, hattın hem algılama hem de modülasyon uçlarında ek kaldıraçlar eklemektedir. Nöroteknoloji, hem algılama hem de etkileme aşamalarında sürece yeni kontrol unsurları eklemektedir. Algılama/segmentasyon için, invaziv olmayan beyin-bilgisayar arayüzleri (non-invasive brain–computer interfaces- BCIs) ve tüketici sınıfı nöro-giyilebilir cihazlar (EEG/fNIRS) dikkat düzeyi ya da bilişsel yük gibi daha kabaca ölçülen durumları izleyebilmektedir. Neuralink, Synchron ve Paradromics (Dawson, 2022) gibi beyin-bilgisayar arayüzü (BCI) şirketlerinin sayısının artması, geleceğin bilişsel güvenlik üzerindeki derin etkisini de vurgulamaktadır. Öte yandan Çin, 2030 yılına kadar beyin-bilgisayar arayüzü (BCI) endüstrisinde küresel lider olmak için ayrıntılı bir ulusal strateji uygulamaktadır. Plan, temel teknolojilerin ilerletilmesine ve yüksek performanslı ürünlerin geliştirilmesine odaklanırken, aynı zamanda güçlü bir endüstriyel ekosistem oluşturmayı ve katı etik ilkelere bağlı kalmayı hedeflemektedir. Ana hedefi, BCI'yi terapötik ve tıbbi uygulamalar için kullanmak ve aynı zamanda tüketiciye yönelik ürün geliştirmeyi teşvik etmektir ([China] Ministry of Industry and Information Technology, 2025).

Klinik alanda, invaziv konuşma amaçlı nöroprotezler, konuşma girişimlerini neredeyse gerçek zamanlı olarak deşifre ederek beyin sinyallerinin deşifre edilmesinde hızlı (ancak tıbbi) ilerlemeyi göstermektedir (Moses vd., 2021; Card vd., 2024). Teslimat/modülasyon için, transkraniyal manyetik stimülasyon (TMS) belirli psikiyatrik endikasyonlar için klinik

olarak onaylanmıştır (örneğin, obsesif-kompulsif bozukluk için FDA pazarlama onayı). Buna karşılık, transkraniyal elektrik stimülasyonu (tDCS/tACS), sağlıklı bireylerde küçük, değişken ve bağlama bağlı etkiler sergiler ve daha güvenilir kazanımlar genellikle yapılandırılmış eğitim rejimleriyle ilişkilidir (U.S. Food and Drug Administration, 2018; Horvath vd., 2015; Price vd., 2015). Savunma Ar-Ge'si, mevcut invaziv olmayan sistemler düşük bant genişliği ve gürültülü olmaya devam etse de nöroteknolojinin çift kullanımlı gidişatını vurgulayarak, açıkça cerrahi olmayan yüksek performanslı arayüzleri (örneğin, DARPA'nın N3'ü) takip etmiştir (DARPA, 2019). Bu nedenle, acil güvenlik endişesi zihin kontrolünden çok, durum farkındalığına sahip operasyonlarla, özellikle de sinirsel/fizyolojik göstergelerden elde edilen hedefleme, zamanlama ve kişiselleştirme ile ilgilidir.

Optimizasyon aşaması döngüyü tamamlar: çok değişkenli testler ve yüksek performanslı kombinasyonların pekiştirilmesi, çeşitli mikro kitleler için hangi anlatımın, formatın ve zamanlamanın ikna edici olduğunu yinelemeli olarak iyileştirir. Bu süreç, çevresel algılama (IoB, Wi-Fi, akıllı hoparlörler), duygulanım göstergeleri (affect proxies) (Kalp atışı ve kalp atış hızı değişkenliği, cilt iletkenliği (EDA), yüz ifadeleri, ses tonu ve perde yüksekliği, vücut duruşu veya mikro hareketler, göz hareketleri veya gözbebeği genişlemesi, yazma ritmi ve etkileşim kalıpları gibi) ve nöro-bitişik (neuro-adjacent) sinyallerle birleştiğinde doğrulama maliyetlerinde asimetriler yaratabilir; böylelikle operatörler için yineleme ucuzlarken, kamu ve kurumlar için doğrulama ve karşı koyma maliyetleri yüksek hâle gelir. Politika perspektifinden bakıldığında bu durum (i) nöral/duygulanımsal çıkarımlar ve bağlamlar arası taşınabilirliği açıkça kapsayan bir veri koruma yaklaşımını, (ii) devlet açısından kritik bilgi akışları ve platform sıralama girdileri için denetlenebilir köken (kaynak) bilgisini (provenance), ve (iii) tasarımla gizlilik (privacy-by-design) ve hız sınırlandırmayı altyapıya gömebilmek amacıyla standartlara (örn. 802.11bf) erken katılımı savunmaktadır (Lee vd., 2020; OECD, 2019, 2025).

Bu yetenekler, yapay zekâ destekli dezenformasyonla birleştiğinde, onları önceki propaganda biçimlerinden ayırt eder. Geleneksel dezenformasyon, ikna edici hikâyeler üretmeye ve bunları kitle iletişim araçları üzerinden yaymaya dayanıyordu. Yapay zekâ ise kitlesel kişiselleştirmeyi mümkün kılar: bireyler bilişsel önyargılarına, duygusal tetikleyicilerine ve sosyal ağ yapılarına göre özelleştirilmiş bir anlatı alabilir. Sorun yalnızca yanlış içeriğin daha "gerçeğe benzer" görünmesi değildir; aynı zamanda çok daha yüksek bir ilgililik ve rezonans (resonance) düzeyiyle sunulmasıdır. Sonuç ise yeni bir düzeyde bilişsel nüfuz ve ikna kapasitesidir.

Askeri doktrinler her zaman bilgi operasyonlarının varlığını kabul eder (Department of the Army, 2023). Küresel ölçekteki gelişmeler, bu tekniklerin stratejik kullanımını göstermektedir. Rusya ve Çin, hibrit savaş stratejilerinin bir parçası olarak bilgi düzensizliğini sistematik biçimde silah hâline getirmiş, dezenformasyonu Ukrayna'da, Avrupa'da ve ötesinde algıları şekillendirmek için kullanmıştır. Çin, diasporaları etkilemek, demokratik kurumları zayıflatmak ve kendi yönetişim modelini tanıtmak için giderek daha fazla sentetik anlatılar kullanmaktadır (Hao, 2018). Aşırılıkçı gruplardan kâr amaçlı dezenformasyon girişimcilerine kadar devlet dışı aktörler, aynı araçları işe alım ve etki için kullanmaktadır. Algoritmalar doğruluktan çok etkileşimi öncelikli kıldığından, küresel iletişim platformlarının özelleştirilmiş yapısı bu çabaları daha da güçlendirmektedir.

Avrupa Birliği, platformları sorumlu tutmak ve müdahaleleri koordine etmek amacıyla Dezenformasyonla Mücadele Uygulama Kuralları (Code of Practice on Disinformation) ve Hızlı Uyarı Sistemi (Rapid Alert System) gibi girişimlerle yanıt verdi. NATO, düşmanların fiziksel ve bilişsel zayıflıkları istismar ettiğini kabul ederek, bilişsel dayanıklılığı hibrit savaş doktrinine dahil etmeye başladı. Türkiye ise hem dış dezenformasyon kampanyalarıyla hem de iç kutuplaşmayla karşı karşıya kaldı ve bu da tehdidin ikili doğasını ortaya koydu. Seçimler sırasında, dini ve ulusal kimlikleri istismar eden sentetik anlatılar yaygın bir şekilde dolaştı ve demokratik süreçlerin dayanıklılığını sınadı. 2023 depremleri gibi krizlerde, dezenformasyon çevrimiçi olarak hızla yayılmış, yardım çabalarını zorlaştırmış ve resmi iletişime olan güveni zedelemiştir.

Bu örnekler, bilişsel kırılganlığın eşit dağılmadığını göstermektedir. Sosyal, siyasi ve kurumsal bağlamlar bu kırılganlığı şekillendirir. Yüksek düzeyde kutuplaşmış toplumlar, düşmanların içlerindeki bölünmeleri istismar edebileceği için manipülatif anlatılara daha duyarlıdır. Kurumlara güveni düşük olan toplumlar, epistemik erozyona karşı daha savunmasızdır. Medya okuryazarlığı sınırlı olan toplumlar ise sentetik manipülasyonu fark etmekte ve direnmekte zorlanabilir. Dolayısıyla bilişsel güvenlik, tek tip bir koşul değil, demokratik kurumların dayanıklılığına, sivil toplumun sağlamlığına ve bilgi ekosistemlerinin bütünlüğüne bağlı, ilişkisel bir koşuldur.

Post-truth durumu, politika tepkileri için de derin etik ikilemler yaratmaktadır. Bilişsel güvenliği korumaya yönelik çabalar, kolaylıkla paternalizm veya sansüre dönüşebilir. Otoriter rejimler, genellikle güvenlik adına bilgi kontrolünü meşrulaştırarak muhalefeti bastırır ve anlatıları tekelleştirir. Demokrasiler bu uygulamaları tekrarlamaktan kaçınmalıdır. Buradaki zorluk, özgürlüğü zedelemeden bilişsel güvenliği savunmaktır. Bu da şeffaflık, hesap verebilirlik ve insan haklarına bağlılık gerektirir. Bilişsel dayanıklılık, vatandaşları maruz kalmaktan korumakla değil, karmaşıklığı yönlendirmek ve manipülasyona direnmek için onları donatmakla inşa edilmelidir.

Umut verici bir yaklaşım, "prebunking"(önceden çürütme) olarak da bilinen psikolojik aşılama kavramıdır. Van der Linden ve arkadaşlarının (2017) araştırması, bireyleri zayıflatılmış yanlış bilgi biçimlerine ve manipülatif tekniklerin açıklamalarına maruz bırakmanın, gelecekteki girişimlere karşı direnç oluşturduğunu göstermektedir. Anlatı direnci bir başka kritik boyuttur: demokratik değerlere dayanan güvenilir anlatıları güçlendirmek, manipülatif alternatiflere karşı koyabilir. Bu yaklaşımlar, reaktif doğruluk kontrolünün ötesine geçerek proaktif bilişsel güçlendirmeye yönelir.

Sonuç olarak, post-truth çağında bilgi düzensizliği ve bilişsel zafiyeti (cognitive vulnerability) dinamikleri, belirleyici mücadelenin içerik değil süreç üzerinde olduğunu ortaya koymaktadır. Yanlış iddiaları tespit etmek ve ortadan kaldırmak yeterli değildir. Daha derin bir zorluk, özerklik, güven ve muhakeme gibi bilişsel koşulları korumaktır. Rini'nin (2020) savunduğu gibi, yanlış bilgi temelde bir güven krizidir: epistemik otoritelere güven olmadan vatandaşlar ortak gerçekler etrafında koordinasyon sağlayamazlar. Dolayısıyla bilişsel güvenlik, güveni yeniden inşa eden, dirençliliği güçlendiren ve demokratik süreçlerin bütünlüğünü koruyan stratejiler gerektirmektedir.

Bu bölümde, post-truth durumunun bilgi düzensizliğinin doğasında niteliksel bir dönüşüm oluşturduğu savunulmuştur. Epistemik otoriteyi aşındırarak ve bilişsel kırılganlıkları istismar ederek, düşmanlar tek bir kurşun bile sıkmadan toplumları istikrarsızlaştırabilirler. Yapay zekâ, hız, ölçek ve inandırıcılığı artırarak bu dinamikleri güçlendirmektedir. NATO, AB ve Türkiye'deki politika tepkileri, içeriğe odaklanmaya devam ederek bilişsel zayıflıkların daha derinlerine değinmemektedir. Bu nedenle, bir sonraki bölümde, sentetik etki çağında bilişsel direnç oluşturmak için politikaların nasıl yeniden şekillendirilebileceği sorusu ele alınacaktır.

3. Bilişsel Dirençlilik Geliştirme: Sentetik Etkilerin Hâkim Olduğu Bir Dünyada Politika Tepkileri

İlk iki bölümde, bilişin yeni ortaya çıkan stratejik bir alan olduğu ve yapay zekanın bilgi düzensizliğinin doğasını dönüştürdüğü incelenmiştir; bir sonraki adım, toplumların bu gelişmeye nasıl tepki verebileceğini sormaktır. Buradaki zorluk, sadece zararlı içeriği tespit etmek veya kaldırmak değil, sentetik etkiye karşı direnç geliştirmektir. Bilişsel direnç, bireylerin ve toplumların dikkat, güven, hafıza ve karar verme süreçlerini istikrarsızlaştırmaya yönelik manipülatif girişimlere karşı direnme, uyum sağlama ve bunlardan kurtulma kapasitesini ifade eder. Bu, demokrasinin zihinsel ve kurumsal bağışıklık sistemidir ve çok katmanlı bir politika çerçevesi gerektirir.

Güvenlik politikası tarihinde direnç, genellikle fiziksel altyapı açısından ele alınmıştır. Kritik altyapının korunması, yedeklilik, sağlamlık ve kesintilerden hızla kurtulma kapasitesini içerir. Bu mantık, bilişsel alana da genişletilebilir. Enerji şebekelerinin yedek sistemlere ihtiyacı olduğu gibi, toplumların da bilişsel yedeklere (cognitive backups) ihtiyacı vardır: güvenilir anlatılar, dirençli kurumlar ve manipülasyona karşı koyabilen eğitimli vatandaşlar. Bu nedenle, politikanın görevi, teknik, eğitimsel, kurumsal ve toplumsal olmak üzere birçok düzeyde bilişsel bağışıklık sistemini güçlendiren önlemler tasarlamaktır.

Teknik düzeydeki zorluk, yapay/üretilmiş medyayı tespit edebilen ve izini sürebilen araçlar geliştirmektir. Yapay zekâ tarafından üretilen içerikler, çoğu zaman yapaylık izleri, tutarsızlıklar ya da istatistiksel kalıpların adli analizi yoluyla tespit edilebilir. Araştırmacılar, yapay/üretilmiş görüntülere veya videolara görünmez sinyaller yerleştiren ve bunların doğrulanmasını sağlayan dijital filigran teknikleri geliştirmiştir. Burada uluslararası iş birliği çok önemlidir: sentetik içerik sınırların ötesine yayılır ve tespit araçları birbiriyle uyumlu olmalıdır. Avrupa Birliği, dijital içerik için menşe standartlarını araştırmaya başlamıştır ve Content Authenticity Initiative (İçerik Orijinalliği Girişimi) gibi girişimler, teknoloji şirketlerini, medya kuruluşlarını ve sivil toplumu bir araya getirerek ortak protokoller geliştirmiştir. NATO da özellikle sentetik anlatıların askeri operasyonları veya ittifakın uyumunu zedeleyebileceği krizlerde hızlı tespitin önemini kabul etmiştir.

Ancak tespit etmek tek başına yeterli değildir. Önceki bölümde de belirtildiği gibi, deepfake'in sahte olduğu ortaya çıktığında güvene verilen zarar geri döndürülemez hale gelmiş olabilir. Bu nedenle, teknik katman, bilişsel direnci vurgulayan proaktif önlemlerle entegre edilmelidir. Bu önlemlerden biri, prebunking olarak da bilinen psikolojik önden çürütme yöntemidir. Araştırmalar, bireyleri zayıflatılmış yanlış bilgi biçimlerine ve manipülatif tekniklerin açıklamalarına maruz bırakmanın, gelecekteki girişimlere karşı direnç oluşturduğunu göstermiştir. Google ve Cambridge Üniversitesi, günah keçisi ya da

duygusal manipülasyon gibi yaygın retorik hileleri açıklayan prebunking videolarını test etmiş ve izleyicilerin daha sonra yanlış bilgilere karşı daha az duyarlı hale geldiğini tespit etmiştir. Ulusal hükümetler, bu deneylerden yararlanarak kendi kültürel ve siyasi bağlamlarına uygun prebunking kampanyaları geliştirebilirler.

Eğitim, dirençliliğin ikinci kritik katmanını oluşturur. Bireylere doğru ile yanlış bilgiyi ayırt etmeyi öğreten geleneksel medya okuryazarlığı programları, "bilişsel okuryazarlık" olarak adlandırılabilecek bir aşamaya evrilmelidir. Bilişsel okuryazarlık, güvenilir kaynakları belirlemenin ötesine geçer; dikkat, önyargı ve ikna gibi psikolojik süreçleri anlamayı da içermektedir. Vatandaşlar, yanlış bilgileri ve bilişsel kısayollarının nasıl istismar edilebileceğini fark edebilecek donanıma sahip olmalıdır. Bilişsel okuryazarlığı okul müfredatına, kamu hizmeti eğitimine ve askeri eğitime entegre etmek, toplum genelinde uzun vadeli bir direnç oluşturur. NATO ve AB üye ülkeleri için bu tür programlar standartlaştırılabilir ve sınırlar ötesinde paylaşılabilir, böylece bilişsel direnç için ortak bir temel oluşturulabilir. Eleştirel düşünmeyi ve kültürlerarası anlayışı teşvik eden eğitim, kutuplaşma ve kimlik temelli anlatıların özel bir kırılganlık yarattığı Türkiye'de özellikle hayati önem taşımaktadır.

Kurumsal düzeyde ise zorluk, koordinasyonda yatmaktadır. Bilişsel güvenlik şu anda birçok alana yayılmış durumdadır: siber güvenlik kurumları teknik savunmaya odaklanırken, eğitim bakanlıkları okuryazarlığı ele almakta, sağlık kurumları halk sağlığı alanındaki yanlış bilgileri ele almakta, savunma kuruluşları hibrit tehditleri izlemekte ve düzenleyiciler teknoloji platformlarını denetlemektedir. Eksik olan, bu çabaları tutarlı bir bütün halinde birleştiren bütüncül bir stratejidir. Bazı ülkeler, yanlış bilgi veya hibrit tehditlerle mücadele için ulusal merkezler kurmaya başlamıştır; ancak çok azı bilişsel güvenliği bir organizasyon kavramı olarak açıkça benimsemiştir. Ulusal Bilişsel Güvenlik Merkezleri (National Cognitive Security Centers) kurulması, istihbarat kurumlarını, eğitim kurumlarını, sivil toplum kuruluşlarını ve teknoloji şirketlerini bir araya getirerek koordinasyon için bir odak noktası sağlayabilir. Bu tür merkezler tehditleri izleyip dayanıklılık programları tasarlayacak, müdahaleleri koordine edecek ve alınan önlemlerin demokratik değerlere uygun olmasını sağlayacaktır.

NATO ve AB de kurumsal düzeyde rol oynamaktadır. NATO, bilişsel alanı yeni ortaya çıkan rekabet alanı olarak kabul etmiştir, ancak bu kabulü operasyonel hale getirecek stratejileri henüz kurumsallaştırmamıştır. Siber veya hibrit savaş doktrinlerine benzer bir bilişsel güvenlik doktrini geliştirmek, üye ülkelere takip edebilecekleri bir çerçeve sağlayacaktır. AB ise Dijital Hizmetler Yasası (Digital Services Act) ile platform düzenlemelerini ilerletmiştir;

ancak bilişsel güvenlik hususlarını da dahil ederek düzenleme gündemini daha da geliştirebilir. NATO-AB ortak girişimleri, sentetik etki kampanyalarına karşı sınır ötesi hızlı müdahale mekanizmaları kurabilir, bilişsel okuryazarlık konusunda iyi uygulamaları paylaşabilir ve tespit teknolojileri konusunda araştırmaları koordine edebilir.

Toplumsal katman en zorlu ama aynı zamanda en önemli katmandır. Bilişsel direnç yukarıdan dayatılamaz; alt kademeden yetiştirilmelidir. Uyumlu, kapsayıcı ve yüksek düzeyde güvene sahip toplumlar manipülasyona karşı daha az savunmasızdır. Tersine, kutuplaşma, eşitsizlik ve güvensizlikle karakterize edilen toplumlar, sentetik anlatıların verimli birer zemini oluşturmaktadır. Bu nedenle, toplumsal direnç oluşturmak için sosyal uyum, topluluk temelli güven ağları ve şeffaf hükümet iletişimi alanlarına yatırım yapılması gerekmektedir. Bağımsız doğruluk kontrolcüleri, sivil toplum kuruluşları ve yerel medya bu ekosistemde hayati roller oynamaktadır. Hükümetler finansman, kapasite geliştirme ve yasal korumalar yoluyla bu kurumları destekleyebilir. Ancak güven, nihayetinde performansa bağlıdır: kurumlar yozlaşmış, etkisiz veya tepkisiz olarak algılandığında, hiçbir iletişim stratejisi güvenilirliği geri kazandıramaz.

Türkiye bu konuda da çarpıcı bir örnek teşkil ediyor. 2023 depremleri sırasında, sosyal medyada yanlış bilgiler hızla yayıldı ve resmi yardım çalışmalarına olan güveni sarsıldı. Bu yanlış bilgilerin bir kısmı dışarıdan kaynaklanıyordu, ancak çoğu iç kutuplaşmayı ve kurumlara karşı şüpheciliği yansıtıyordu. Bu olay, bilişsel dirençliliğin daha geniş kapsamlı yönetişim ve meşruiyet meselelerinden ayrı düşünülemeyeceğini göstermektedir. Bu nedenle, Türkiye'de bilişsel güvenliği güçlendirmek için teknik tespit araçları, eğitim programları ve kurumsal güveni ve demokratik hesap verebilirliği artıracak reformlar gereklidir.

Etik boyut sürecin her aşamasında merkezi bir öneme sahiptir; bilişsel güvenliği koruma çabaları, dikkatli biçimde tasarlanıp uygulanmadığı takdirde paternalizme ya da sansüre kayma riski taşır. Demokrasiler, otoriter bilgi kontrolünü taklit etme eğilimine karşı direnmelidir. Şeffaflık çok önemlidir: vatandaşlar, içeriğin nasıl ve neden denetlendiğini, algoritmaların beslemelerini nasıl düzenlediğini ve onları korumak için hangi önlemlerin alındığını anlamalıdır. Teknoloji şirketleriyle kamu-özel sektör ortaklıkları, hesap verebilirliği sağlamak için, kesin denetim mekanizmaları ve suistimale karşı önlemler içerecek şekilde yapılandırılmalıdır. Amaç, vatandaşları maruz kalmaktan korumak değil, karmaşıklığı özerk bir şekilde yönlendirmeleri için onlara yetki vermektir.

Bu çok katmanlı teknik, eğitimsel, kurumsal ve toplumsal çerçeve nihai bir çözüm sunmamaktadır. Bilişsel güvenlik, bir kez ve sonsuza kadar çözülmesi gereken bir sorun değil, sürekli olarak yönetilmesi gereken bir durumdur. Siber güvenlik, gelişen tehditlere sürekli uyum gerektirdiği gibi, bilişsel dayanıklılık da gereklidir. Aradaki fark, siber güvenlik ağları ve sistemleri korurken, bilişsel güvenlik toplumların toplu olarak düşünme, karar verme ve hareket etme kapasitesini koruduğudur. Bu nedenle, bu dar bir teknik konu değil, demokratik dayanıklılığın temel bir direğidir.

Karşılaştırmalı bir bakış açısıyla, böyle bir çerçeveye duyulan ihtiyaç açıktır. NATO'nun bilişsel alanı tanıması, bu alanın stratejik önemini vurgulamaktadır, ancak operasyonel doktrinler hala yeterince gelişmemiştir. AB'nin düzenleyici girişimleri önemli bir adımdır, ancak uygulama düzensizdir ve odak noktası bilişsel alan yerine içerik üzerinde kalmaktadır. Türkiye'nin deneyimi hem dış manipülasyon hem de iç kutuplaşmanın zafiyetler yarattığı bu sorunun ikili doğasını vurgulamaktadır. ABD'den Asya demokrasilerine kadar birçok ülke benzer ikilemlerle karşı karşıyadır. Sentetik etkinin küresel niteliği, hiçbir ülkenin bu sorunu tek başına çözemeyeceği anlamına gelir. Bu nedenle bilişsel güvenlik hem ulusal bir sorumluluk hem de uluslararası iş birliği gerektiren kolektif bir değer olarak anlaşılmalıdır.

Bu bölümde, bilişsel dayanıklılık oluşturmanın çok katmanlı bir yaklaşım gerektirdiği savunulmuştur. Dijital Filigranlama (watermarking) ve tespit gibi teknik araçlar gereklidir; ancak tek başlarına yeterli değildir. Eğitim programları, vatandaşları manipülasyona dirençli hale getirecek şekilde bilişsel okuryazarlığa doğru gelişmelidir. Kurumsal koordinasyon, parçalanmayı önlemek ve bütünsel stratejilerin uygulanmasını sağlamak için çok önemlidir. Güven, uyum ve şeffaflığa dayanan toplumsal direnç, istikrarlı bir toplumun temel dayanağıdır. Bu önlemleri demokratik değerlere ve insan özerkliğine saygı ile dengelemek, temel normatif zorluktur. Bir sonraki bölümde, bilişsel güvenliğin daha geniş bir paradigmasının gelişimi incelenerek, bunun 21. yüzyıl güvenlik mimarisine nasıl entegre edilebileceği ele alınacaktır.

4. Yirmi Birinci Yüzyıl için Bilişsel Güvenlik Paradigmasına Doğru

Önceki bölümlerde, bilişsel güvenliğin ayrı bir alan olarak ortaya çıkışı, Post-Truth çağında bilgi düzensizliğinin dönüşümü ve çok katmanlı politika tepkilerinin gerekliliği ele alınmıştır. Bu içgörüleri eyleme geçmek için sağlam bir temele oturtmak için daha geniş bir paradigma değişikliği gereklidir. Thomas Kuhn'un (1962) hatırlattığı gibi, paradigma bir dizi teoriden daha fazlasıdır; gerçekliğin algılandığı ve düzenlendiği bir mercektir. Bu anlamda, bilişsel güvenlik, devletlerin ve toplumların yirmi birinci yüzyılda güvenliğin doğasını nasıl anladıklarına dair bir yeniden yönlendirme gerektirmektedir.

Geleneksel güvenlik paradigmaları, maddi tehditler etrafında inşa edilmiştir. Askeri güç, orduların, tankların, gemilerin ve uçakların büyüklüğü ve yetenekleriyle ölçülüyor. Siber güvenlik, bu mantığı dijital alana genişleterek ağlara ve altyapılara odaklanmıştır. Benzer şekilde, bilgi güvenliği de verilerin ve içeriğin bütünlüğüne odaklanır. Bu paradigmalar, tehditlerin ağırlıklı olarak fiziksel veya teknik nitelikte olduğu bir dönem için yeterliydi. Ancak, çatışmanın belirleyici alanının bilişsel olduğu bir çağda maalesef yetersiz kalmaktadırlar.

“Bilişsel alan” (cognitive domain)" kavramı yalnızca metafor değildir. Huang ve Zhu (2023) tarafından da belirtildiği gibi, biliş, doğal zayıflıklara ve kasıtlı manipülasyona maruz kalan karmaşık bir sosyo-teknik sistemin parçasıdır. Zihin izole değildir; iletişim ağlarına, sosyal etkileşime ve teknolojik arabuluculuğa gömülüdür. Bu anlamda, bilişsel güvenlik sadece siber güvenliğin bir uzantısı değil, kendi doktrinlerini, politikalarını ve kurumlarını gerektiren ayrı bir alandır.

Bu paradigma değişimini kavramsallaştırmanın bir yolu, kritik altyapı analojisidir. Enerji şebekeleri, finansal sistemler ve ulaşım ağları modern toplumların işleyişi için ne kadar önemliyse, bilişsel bütünlük de o kadar önemlidir. Vatandaşlar algılarına, anılarına veya yargılarına güvenemezlerse, bir toplumun müzakere etme ve kolektif kararlar alma kapasitesi çöker. Bu anlamda, bilişin kendisi kritik altyapı olarak ele alınmalıdır. Onu korumak için teknik savunma ve kültürel, eğitimsel ve kurumsal yatırımlar gerekir.

Paradigma değişimini çerçevelendirmenin bir başka yolu da dayanıklılık merceğinden bakmaktır. Geleneksel güvenlik yaklaşımları genellikle önleme ve caydırıcılığı önceliklendirmektedir: saldırı gerçekleşmeden önce onu durdurmak veya misilleme tehdidiyle düşmanları harekete geçmekten caydırmayı esas alır. Buna karşılık, bilişsel güvenlik esnek-dayanıklılığı vurgular. Manipülatif anlatılar tamamen önlenemez; sentetik medya tamamen ortadan kaldırılamaz, algoritmik ikna tamamen etkisiz hale getirilemez. Bu nedenle amaç, tehditleri ortadan kaldırmak değil, güven veya özerkliğin felaketle sonuçlanacak bir kaybına yol açmadan bunları absorbe etme kapasitesini geliştirmektir. Bu, kontrol mantığından uyum mantığına bir kaymadır.

Uluslararası güvenlik kuruluşları için bunun etkileri çok derindir. NATO, kara, deniz, hava, siber ve uzayı uzun zamandır ayrı savaş alanları olarak tanımaktadır. Bilişsel alanı tanımak, bu çerçevenin önemli ölçüde genişletilmesi anlamına gelir. Bu, bilişsel savunma doktrinlerinin geliştirilmesini, askeri personelin bilişsel dirençlilik konusunda eğitilmesini ve bilişsel konuların operasyonel planlama ve uygulamaya entegre edilmesini gerektirir.

Bilişsel güvenlik savaş alanının ötesinde toplumun dokusuna da uzandığından, sivil kurumlarla yakın iş birliği de gerektirir.

Avrupa Birliği de benzer bir zorlukla karşı karşıyadır. Dijital Hizmetler Yasası gibi düzenleyici girişimleri, algoritmik küratörlük (algoritmic curation) zararlarından platformları sorumlu tutmak için gerekli adımları temsil etmektedir. Ancak, bilişsel güvenlik paradigması daha geniş bir yönelim gerektirmektedir: sadece içeriği ve platformları düzenlemekle kalmayıp, vatandaşların bilişsel dayanıklılığına yatırım yapmak, bağımsız medyayı desteklemek ve epistemik güveni teşvik etmek de gerekmektedir. Bu, bilişsel güvenliği dezenformasyonun niş bir sorunu olarak değil, demokratik esnek-dayanıklılığın temel bir boyutu olarak ele almak anlamına gelir.

Bilişsel güvenlik sadece Batı'nın değil, tüm dünyanın ortak bir sorunudur. Türkiye'nin çok sayıda etki ekosistemine maruz kalması — Rus dezenformasyonu, Batı anlatıları, bölgesel mezhepçi propaganda ve iç kutuplaşma — bilişsel tehditlerin çok yönlü ve birbiriyle kesiştiğini göstermektedir. Bilişsel güvenlik paradigması, Türkiye'nin iç direnç stratejilerini NATO'daki rolü ve AB ile ilişkisiyle bütünleştirmesine olanak tanıyarak, onu farklı bölgeler ve gelenekler arasında bir köprü olarak konumlandıracaktır.

Paradigma değişiminin etik boyutları da vardır. Rouvroy ve Stiegler (2016) tarafından da belirtildiği gibi, dijital çağ, gücün zorlama veya ikna yoluyla değil, dikkat, davranış ve seçimlerin modülasyonu yoluyla kullanıldığı yeni bir "algoritmik yönetimsellik" (algorithmic governmentality) ortaya çıkarmıştır. Bu nedenle, bilişsel güvenlik sadece stratejik açıdan değil, normatif açıdan da anlaşılmalıdır. Bilişi korumak, özerkliği, haysiyeti ve demokratik iradeyi korumak anlamına gelir. Bunun riski, devletlerin bilişi savunmak için bu değerleri zedeleyen paternalist veya otoriter önlemler almaya yönelmeleri olabilir. Bu nedenle, bilişsel güvenlik paradigması insan hakları ve demokratik ilkelere açıkça dayandırılmalıdır.

Bu paradigmanın kavramsal temelleri halen geliştirilme aşamasındadır. Bone (2017) ve Bone ve Lee (2023) gibi araştırmacılar, bilişsel risk yönetimini vurgulamakta ve bilişsel kırılganlıkları tespit edilmesi ve azaltılması gereken örgütsel riskler olarak ele almaktadır. Huang ve Zhu (2023) karmaşık uyarlanabilir sistemler içinde bilişi konumlandıran sistem bilimsel bir yaklaşım önermektedir. Rouvroy ve Stiegler (2016) algoritmik yönetişimin insan özerkliği üzerindeki etkilerini vurgulamaktadır. Bu bakış açıları farklı olmakla birlikte, bilişin hem stratejik bir varlık hem de normatif bir değer olduğu konusunda birleşmektedir.

Bilişsel güvenlik paradigmasına doğru ilerlemek, bu içgörüleri politika ve uygulamaya entegre etmeyi gerektirir. Bu, bilişi bir güvenlik alanı olarak gören doktrinler geliştirmek,

teknik, eğitimsel, kurumsal ve toplumsal katmanlarda işleyen dayanıklılık çerçeveleri tasarlamak ve özerkliği ve demokrasiyi koruyan etik önlemler almak anlamına gelir. Bu, bilişsel güvenliğin geçici bir dezenformasyon sorunu değil, dijital çağın kalıcı bir koşulu olduğunu kabul etmek anlamına gelir.

Bu bölümde, bilişsel güvenliğin güvenlik düşüncesinde bir paradigma değişikliğini temsil ettiği savunulmuştur. Geleneksel paradigmalar fiziksel ve teknik alanlara odaklanırken, bilişsel güvenlik stratejik bir alan olarak insan zihnine odaklanır. Bu değişim, bilişi kritik bir altyapı olarak ele almayı, kontrol yerine dirençliliği vurgulamayı ve etik hususları stratejik planlama ve karar alma süreçlerine entegre etmeyi gerektirir. NATO, AB ve Türkiye, bu paradigmanın aciliyetini ve küresel önemini örneklemektedir. Sonraki bölümlerde, bilişsel güvenliği yirmi birinci yüzyılın dirençliliğinin kalıcı bir ayağı olarak pekiştirmek için gerekli olan gelecekteki zorluklar ve araştırma gündemleri ele alınacaktır.

5. Bilişsel Güvenliğin Geleceği: Zorluklar, Fırsatlar ve Araştırma Gündemi

Bilişsel güvenlik, 21. yüzyılın çatışma ve yönetişim alanını belirleyen bir unsur olarak giderek daha fazla kabul görürken, politika yapıcılar ve akademisyenler, bu alanın gelecekteki gidişatını öngörme zorluğuyla karşı karşıya kalmaktadır. Teknolojik değişimin hızlı temposu, düşmanların gelişen stratejileriyle birleşince, bugünün zorluklarının yarının zorluklarıyla aynı olmayacağı kesinleşmektedir. Aynı zamanda, dayanıklılığı güçlendirmek, uluslararası iş birliğini geliştirmek ve koruyucu önlemlerde yeniliği teşvik etmek için yeni fırsatlar ortaya çıkmaktadır. Bu bölüm, sentetik etki çağında yol almak için gerekli olan önemli zorluklar, potansiyel fırsatlar ve araştırma gündemine odaklanarak bilişsel güvenliğin gelecekteki manzarasını incelemektedir.

İlk zorluk, yapay zekânın hızla gelişmesinden kaynaklanmaktadır. Üretken modeller, algılama yeteneklerini geride bırakan bir hızla ilerlemektedir. Bir zamanlar kolayca tanınabilir olan deep fake'ler artık giderek daha kusursuz hale geliyor ve sadece bireylerin görsel görünümünü değil, seslerini, davranışlarını ve hatta kendine özgü konuşma kalıplarını da taklit edebiliyor. Büyük dil modelleri, insan yazılarından ayırt edilemeyen ikna edici metinler üretebiliyor. Büyük dil modelleri, insan yazılarından ayırt edilemeyen ikna edici metinler üretebilir. Kişiselleştirme motorlarıyla entegre edildiğinde, milyonlarca kişiye aynı anda özelleştirilmiş anlatılar sunabilirler. Teknolojik gelişimin gidişatı, bu yeteneklerin sadece daha da gelişeceğini ve sentetik etkinin tespit edilmesini zorlaştırarak etkisini daha ikna edici hale getireceğini gösteriyor.

İkinci bir zorluk ise saldırı ile savunma arasındaki asimetridir. Sentetik medya üretmek nispeten ucuz ve ölçeklenebilirken; bunu tespit etmek ve çürütmek ise kaynak yoğun ve

ve çoğu zaman yavaş ilerleyen bir süreçtir. Bu asimetri, bilgi ortamını düşük maliyetle manipülatif içerikle doldurabilen hasımların lehine çalışır. Buna karşılık savunma önlemleri gelişmiş teknolojiler, insan uzmanlığı ve kurumsal koordinasyon gerektirir. Ortaya çıkan şey, toplumları sürekli olarak geride kalma riskine açık bırakan yapısal bir dengesizliktir.

Üçüncü zorluk ise sorumluluk tespitidir. Sentetik etki kampanyalarının kaynağını tespit etmek son derece güçtür. Devlet ve devlet dışı aktörler, kökenlerini gizleyebilir, operasyonlarını birden fazla aracı üzerinden yürütebilir ve dijital ortamın anonimlik avantajından yararlanabilir. Güvenilir bir atıf olmaksızın caydırıcılık neredeyse imkânsız hâle gelir. Net sorumluluk sınırlarına dayanan uluslararası hukuk, makul inkâr edilebilirlik (plausible deniability) ve dağıtılmış manipülasyonun hâkim olduğu bir dünyaya uyum sağlamakta zorlanmaktadır. Bu durum, düşmanların nispeten cezasız kalabilecekleri müsamahakâr bir ortam yaratmaktadır.

Dördüncü zorluk ise aşırı müdahale riskidir. Bilişsel güvenliği korumaya yönelik çabalar, özellikle otoriterleşme baskılarının zaten yoğun olduğu bağlamlarda, kolaylıkla paternalizme ya da sansüre kayabilir. Yurttaşları manipülasyondan korumaya çalışırken, devletlerin ifade özgürlüğünü kısıtlama, muhalefeti bastırma ya da anlatı tekelini elinde toplama tehlikesi vardır. Bu durum yalnızca demokratik değerleri baltalamakla kalmaz; güveni de aşındırarak, paradoksal biçimde, bilişsel dirençliliği güçlendirmek yerine zayıflatır.

Tüm bu engellere rağmen, bilişsel güvenliğin geleceği aynı zamanda fırsatlar da sunmaktadır. Sentetik etkiyi mümkün kılan teknolojilerin kendisi savunma amaçlı olarak da kullanılabilir. Yapay zekâ manipülatif içeriği tespit etmek, kökenini izlemek ve olası etkisini modellemek için kullanılabilir. Makine öğrenmesi, henüz geniş çaplı dolaşıma girmeden yükselmekte olan anlatıları belirleyebilir; böylece önleyici karşı-önlemlerin geliştirilmesini mümkün kılar. Doğal dil işleme ise “prebunking” kampanyalarını destekleyerek, bireyleri manipülasyona karşı “aşılayan” özelleştirilmiş pedagojik materyaller üretebilir. Bu fırsatlar yatırım gerektirir; ancak aynı zamanda teknolojik yeniliğin doğası gereği yıkıcı olmak zorunda olmadığını da gösterir: yenilik, dirençlilik için —hatta faydalı yönlendirme için— kullanılabilir.

Bir başka fırsat da uluslararası iş birliğinde yatmaktadır. Bilişsel güvenlik, sınır ötesi bir sorundur: sentetik anlatılar sınırları aşar ve düşmanlar küresel platformları istismar eder. Bu durum, devletler, uluslararası kuruluşlar ve teknoloji şirketleri arasında iş birliği için güçlü bir teşvik oluşturur. NATO, bilişsel direnci hibrit savaş stratejisine entegre etmek için adımlar atmış, Avrupa Birliği ise platform düzenlemesi ve sınır ötesi uyarılar için mekanizmalar geliştirmiştir. Bu girişimlerin daha kapsamlı bir bilişsel güvenlik çerçevesine genişletilmesi,

sentetik etki kampanyalarına karşı kolektif koruma sağlayabilir. Birden fazla etki ekosisteminin kesişme noktasında bulunan Türkiye, bilişsel güvenlik konusunda Batı ve Batı dışı yaklaşımlar arasında diyalogu teşvik ederek bu boşluğu doldurabilir.

Toplumsal düzeyde, bilişsel güvenliğin geleceği demokratik direncin yenilenmesi için bir fırsat sunmaktadır. Bilişsel okuryazarlığa yatırım yaparak, bağımsız medyayı destekleyerek ve sosyal uyumu teşvik ederek toplumlar manipülasyona direnme yeteneklerini artırabilirler. Post-Truth durumu kaçınılmaz değildir; kurumsal başarısızlıklar, teknolojik teşvikler ve bilişsel zayıflıklardan kaynaklanır. Bu temel koşulları ele almak, güveni yeniden inşa edebilir ve demokrasinin zihinsel temellerini yeniden kurabilir. Bu anlamda, bilişsel güvenlik hem savunma açısından bir gereklilik hem de olumlu bir projedir ve daha bilgili, dirençli toplumlar için bir vizyon sunar.

Bilişsel güvenliğe yönelik araştırma gündemi de buna paralel olarak geniştir. Dikkat gerektiren birkaç temel alan bulunmaktadır. İlk olarak, güvenliğin zihinsel boyutu daha sistematik bir biçimde kuramsallaştırılmalıdır. Huang ve Zhu (2023), bilişi sosyo-teknik sistemin bir parçası olarak çerçeveleyerek bu çalışmaya başlamıştır. Ancak, sinirbilim, psikoloji, sosyoloji ve siyaset biliminden elde edilen bilgileri entegre etmek için daha fazla araştırma yapılması gerekmektedir. Bilişsel önyargılar algoritmik düzenlemeyle nasıl etkileşime girer? Sosyal kutuplaşma, kırılganlığı nasıl artırır? Kurumlara duyulan güven, manipülasyona yatkınlığı nasıl şekillendirir? Bunlar, disiplinler arası araştırma gerektiren sorulardır.

İkincisi, esnek-dayanıklılık (resilience) önlemlerinin etkinliği test edilmelidir. Psikolojik aşılama ve prebunking umut vericidir, ancak uzun vadeli etkileri halen belirsizdir. Aşılama teknikleri zamanla etkinliğini yitirir mi? Belirli koşullar altında ters etki yapabilir mi? Farklı kültürel ve politik bağlamlara nasıl uyarlanabilir? Cambridge Sosyal Karar Verme Laboratuvarı (Cambridge Social Decision-Making Lab) tarafından yürütülen çalışmalar gibi büyük ölçekli saha deneyleri, bu araştırma için bir model sunmaktadır. Yine de farklı toplumlarda daha sistematik çalışmalar yapılmasına ihtiyaç vardır.

Üçüncüsü, bilişsel güvenliğin etik boyutları dikkatli bir şekilde incelenmelidir. Rouvroy ve Stiegler (2016) tarafından da belirtildiği gibi, algoritmik yönetişim, emir vermek yerine dikkat ve davranışları şekillendirerek işleyen yeni bir güç biçimidir. Bilişsel yeteneklerin korunması, özerklik, rıza ve devlet müdahalesinin sınırları hakkında sorular ortaya çıkarır. Demokrasiler, ifade özgürlüğünü zedelemeden vatandaşlarını nasıl koruyabilir? Bilişsel güvenlik önlemlerinin kötüye kullanılmasını önlemek için hangi önlemler gereklidir? Bu sorular politika yapıcılar, etik uzmanları, hukukçular ve sivil toplum tarafından ele alınmalıdır.

Dördüncü olarak, teknoloji şirketlerinin rolü incelenmelidir. Facebook, Twitter ve TikTok gibi platformlar tarafsız bilgi kanalları değildir. Algoritmaları, kullanıcıların gördüklerini ve inandıklarını etkileşim şekillendirir. Etkileşimi önceliklendiren iş modelleri, genellikle manipülatif içeriği güçlendirir. Bu nedenle, onları sorumlu tutmak bilişsel güvenlik için çok önemlidir. Peki bu hesap verebilirlik ne şekilde olmalı? Düzenleme bir seçenek olabilir, ancak bu, inovasyonu engelleyebilir veya platformları daha zayıf kurallara sahip yargı bölgelerine yönlendirebilir. Kamu-özel sektör ortaklıklarından başka seçenekler olabilir, ancak bunların etkili olabilmesi için güven ve şeffaflık gereklidir. Öte yandan bu süreci yönetebilmek için de en etkili yönetişim modellerini araştırmak ve inşa etmek gerekmektedir.

Son olarak, bilişsel güvenliğin küresel boyutu sürekli dikkat gerektirir. Sentetik etkinin dinamikleri kültürel ve siyasi bağlamlara göre değişiklik gösterir. Liberal demokrasilerde zorluk, özgürlüğü zedelemeden özerkliği ve güveni savunmaktır. Otoriter rejimlerde ise bu durum bilişsel güvenliğin baskı için bir gerekçe olarak kullanılabilmesine dönüşür. Jeopolitik rekabetlerin dini ve etnik bölünmelerle kesiştiği Orta Doğu gibi bölgelerde bilişsel güvenlik farklı biçimler alır. Bu nedenle, bu farklılıkları anlamak ve bağlama duyarlı stratejiler geliştirebilmek için karşılaştırmalı araştırmalar oldukça önemlidir.

Bilişsel güvenliğin geleceği yalnızca teknoloji tarafından belirlenmeyecektir. Teknolojik yenilikler, bilişsel kırılganlıklar, kurumsal tepkiler ve normatif seçimlerin etkileşimi de bilişsel güvenliği şekillendirecektir. Hızla gelişen yapay zekâ, saldırı-savunma asimetrileri, kaynak tespiti güçlükleri ve etik ikilemler gibi zorlukların var olduğu muhakkak. Fakat savunma için teknolojiden yararlanmak, uluslararası iş birliğini teşvik etmek, demokratik direnci yenilemek ve disiplinler arası araştırmayı ilerletmek gibi fırsatların var olduğu da unutulmamalıdır.
Bone ve Lee'nin (2023) savunduğu gibi, bilişsel risk, dijital çağda kuruluşların ve toplumların direncini belirleyecek olan güvenliğin yeni sınırlarıdır. Bilişsel güvenliğin aşınması, yalnızca siyasi istikrarı değil, aynı zamanda olasılığı da tehdit etmektedir. Daha önce de altını çizdiğim gibi bilişsel dirençliliğe yatırım yaparak toplumlar, kırılganlığı güce dönüştürebilirler. Manipülasyona karşı direnç gösterme, yeni zorluklara uyum sağlama ve vatandaşlarının özerkliğini koruma kapasitesini geliştirebilirler.

6. Sonuç – Yapay Zekâ Çağında Bilişsel Alanın Güvenliğini Sağlamak

Önceki bölümlerde bilişsel güvenliğin kavramsal olarak ortaya çıkışı, Post-Truth çağında bilgi düzensizliğinin dönüşümü, yapay zekanın yıkıcı potansiyeli ve çok katmanlı bir dirençlilik çerçevesinin ana hatları ele alınmıştır. Birlikte ele alındığında, güvenlik anlayışında derin bir dönüşümü ortaya koymaktadırlar: biliş, yani dikkatimizi, güvenimizi, hafızamızı ve karar verme süreçlerimizi kapsayan alan, artık stratejik bir boyut hâline gelmiştir. Bu farkındalık hem bir uyarı hem de harekete geçme çağrısı niteliğindedir. Bilişsel alanı savunacak sağlam politikalar ve uygulamalar olmadan, demokrasiler gerçek, güven ve özyönetimin sistematik olarak aşındığı sentetik etki çağına girme riskiyle karşı karşıyadır.

Bu makalede öne sürülen ilk temel argüman, bilişsel güvenliğin geleneksel bilgi güvenliği ve siber güvenlik kavramlarından farklı, ancak bunları tamamlayıcı bir kavram olarak anlaşılması gerektiğidir. Önce de vurgulandığı gibi bilgi güvenliği, içeriğin bütünlüğünü sağlamaya odaklanır, yani verilerin doğru, korunmuş ve güvenilir olmasını sağlar. Siber güvenlik ise teknik altyapıları izinsiz giriş, sabotaj ve bozulmalara karşı korumaya odaklanır. Her ikisi de gereklidir, ancak hiçbiri bilişin kendisinin zayıflıklarını ele almaz. İnsanlar rasyonel bilgi işlemcileri değildir; düşmanların manipüle edebileceği sezgisel yöntemlere, duygulara ve sosyal ipuçlarına güveniriz. Kahneman ve Tversky'nin (1974) onlarca yıl önce gösterdiği gibi, bilişsel önyargılar insan muhakemesinin doğasında var olan bir özelliktir. Dördüncü Sanayi Devrimi'nin dijital ortamında, bu önyargılar istismar edilebilir saldırı yüzeyleri haline gelmiştir. Algoritmaya dayalı iletişimin yükselişi, zihni tartışmalı açık bir alan haline getirerek, korunması mecburiyetini ortaya koymuştur.

İkinci temel argüman, yapay zekanın dezenformasyonun doğasını içerik sorunundan biliş sorununa dönüştürdüğüdür. Daha önceki propaganda biçimleri, izleyicileri belirli anlatılara ikna etmeye çalışıyordu. Buna karşılık, günümüzün yapay zekâ destekli manipülasyonları çoğu zaman gerçeğin kendisine dair olasılık algısını aşındırmayı amaçlıyor. Deep fake'ler gerçeklik ve uydurma arasındaki sınırı bulanıklaştırır; ses klonlama duyusal algıya olan güveni sarsar; büyük dil modelleri bilgi ortamını ikna edici ancak yanıltıcı metinlerle büyük ölçekte doldurabilir. Pomerantsev (2019) tarafından da belirtildiği gibi, birçok modern etki kampanyası gerçeği yalanla değiştirmek değil, vatandaşların neye inanacaklarını bilemedikleri bir epistemik kaos ortamı yaratmayı amaçlamaktadır. İkna etmekten kafa karıştırmaya, anlatı kontrolünden anlatı aşırı yüklemesine doğru bu geçiş, bilgi düzensizliği gibi niteliksel bir dönüşümü temsil etmektedir.

Üçüncü temel argüman, mevcut politika araçlarının bu zorlukların üstesinden gelmek için yetersiz olduğudur. Doğruluk kontrolü ve içerik denetimi, değerli olmakla birlikte, temelde reaktif niteliktedir. Yanlış bilginin yayılmasından sonra içeriği ele alırlar, ancak bireyleri ilk etapta savunmasız hale getiren bilişsel zayıflıkları ele almazlar. Yasal çerçeveler genellikle teknolojik yeniliklerin gerisinde kalır, sentetik medyaya yönelik düzenlemeler sınırlıdır ve platformlarda hesap verebilirlik mekanizmaları yetersizdir. Kurumsal sorumluluklar çeşitli sektörlere dağılmış durumda ve bu da koordinasyon ve etkinlik açısından boşluklara yol açmaktadır. Demokrasiler, düşman devletlerin dış manipülasyonlarına karşı savunmasız kalmanın yanı sıra, yapay zekâ destekli anlatılarla daha da güçlenen iç kutuplaşmaya da karşı savunmasızdır.

Dördüncü temel argüman, gerçek esnek-dayanıklılığın sadece ağları değil, zihinleri de savunmayı gerektirdiğidir. Bilişsel esnek-dayanıklılık, bir tür bağışıklık olarak anlaşılabilir: manipülatif girişimleri tanıma, direnme ve bunlardan kurtulma yeteneği. Bu, çok katmanlı bir çerçeve gerektirir. Teknik katmanda dijital filigran (watermarking), köken (kaynak) bilgisi ve tespit araçları esastır. Eğitim düzeyinde, bilişsel okuryazarlık programları vatandaşlara manipülasyonu tanıma ve önyargılarına karşı koyma becerilerini kazandırmalıdır. Kurumsal katmanda, ulusal bilişsel güvenlik merkezleri istihbarat kurumları, eğitim sistemleri, düzenleyiciler ve sivil toplum arasında çabaları koordine etmelidir. Toplumsal düzeyde güven, şeffaflık ve uyuma yatırım yapmak çok önemlidir.

Karşılaştırmalı bir bakış açısıyla, NATO, AB ve Türkiye, bu tür bir dirençlilik oluşturmanın hem zorluklarını hem de fırsatlarını göstermektedir. Yukarıda da değindiğim gibi, NATO, bilişsel alanı yeni ortaya çıkan bir rekabet alanı olarak kabul etmeye başlamıştır; ancak, bilişsel güvenliği operasyonel doktrinlerine henüz tam olarak entegre etmemiştir. Avrupa Birliği, Dijital Hizmetler Yasası (Digital Services Act) ile platformları düzenlemek ve dezenformasyonu izlemek için adımlar atmıştır. Yine de bu çabalar esas olarak içeriğe odaklanmaya devam etmektedir. Türkiye, dış manipülasyon ve iç kutuplaşmanın benzersiz bir kombinasyonuyla karşı karşıya olup, teknik, eğitimsel, kurumsal ve toplumsal önlemleri entegre eden bütüncül bir bilişsel güvenlik stratejisinin gerekliliğini vurgulamaktadır. Fakat Dezenformasyon Mücadele Merkezi dışında hayata geçirilen bir adımı yoktur.

Yapay zekanın giderek sofistike hale gelmesi, sentetik etkinin tespit edilmesini daha zor ve etkisini daha ikna edici hale getirmektedir. Saldırı ve savunma arasındaki asimetri, büyük ölçekte ve düşük maliyetle manipülatif içerik üretebilen düşmanlara avantaj sağlamaktadır.

Saldırıların kaynağını kesin olarak belirlemek hâlâ zor, bu da caydırıcılığı ve hesap verebilirliği karmaşık hale getirmektedir. Aşırıya kaçmanın etik riskleri ise ciddi: bilişsel güvenliği korumaya çalışırken demokrasiler, savunmak istedikleri özgürlüklerin altını oyma tehlikesiyle karşı karşıya kalabilir. Ancak gelecek aynı zamanda fırsatlar da sunmaktadır. Manipülasyonu mümkün kılan teknolojiler savunma amaçlı da kullanılabilir. Yapay zekâ, sentetik medyayı tespit etmek, anlatı yayılımını modellemek ve önleyici müdahaleler oluşturmak için kullanılabilir. NATO ve AB gibi kuruluşlar aracılığıyla uluslararası iş birliği, ulusötesi etki kampanyalarına karşı toplu koruma sağlayabilir. Eğitim, medya okuryazarlığı ve sivil dirençlilik alanlarına yapılan yatırımlar, güveni yeniden inşa edebilir ve demokrasinin bilişsel temellerini yeniden kurabilir.

Bu nedenle, bilişsel güvenlik alanındaki araştırma gündemi hem acil hem de disiplinler arası bir nitelik taşımaktadır. Psikoloji, nörobilim, bilgisayar bilimi, hukuk ve siyaset bilimi gibi çeşitli alanlarda iş birliği gerektirir. Önleyici tedbirlerin ve prebunking stratejilerinin uzun vadeli etkinliği dahil olmak üzere, esnek-dayanıklılık önlemlerinin titiz bir şekilde test edilmesini gerektirir. Koruyucu önlemlerin insan haklarını ve demokratik ilkeleri zedelememesini sağlamak için, bilişsel güvenliğin etik ikilemleriyle eleştirel bir şekilde ilgilenilmesini mecbur kılar. Ayrıca, bilişsel zayıflıklar ve stratejilerin kültürel, politik ve kurumsal bağlamlara göre değiştiğini kabul ederek, bölgeler arasında karşılaştırmalı araştırma yapılmasını büyük bir ihtiyaçtır.

Demokrasiler için bu zorunluluk özellikle önemlidir. Demokratik yönetişim, vatandaşların bilinçli kararlar alma, toplu olarak müzakere etme ve kurumlara güvenme kapasitesine bağlıdır. Bu bilişsel temeller zayıflatılırsa, demokrasinin kendisi tehlikeye girer. Sentetik etki çağı, bu temellere doğrudan bir meydan okuma oluşturmaktadır. Deep fake'ler, ses klonlama, algoritmik ikna ve sentetik anlatılar sadece rahatsız edici unsurlar değildir; bunlar güveni aşındırmak, kafa karışıklığı yaratmak ve toplumları istikrarsızlaştırmak için tasarlanmış stratejik silahlardır.

Bu nedenle, harekete geçme çağrısı açıktır. Demokrasiler, siber savunma veya fiziksel korumaya yatırım yaptıkları kadar acil olarak bilişsel güvenliğe de yatırım yapmalıdır. Bu, ulusal bilişsel güvenlik stratejileri geliştirmeyi ve finanse etmeyi, bilişsel okuryazarlığı eğitime dahil etmeyi, koordinasyon için kurumsal mekanizmalar oluşturmayı ve toplumsal dayanıklılığı teşvik etmeyi gerektirir. Uluslararası tehditleri ele almak ve iyi uygulamaları paylaşmak için, özellikle NATO ve AB içinde uluslararası iş birliği gereklidir.

Bu adımlar atılmazsa, sonuçları ağır olabilir. Toplumlar, gerçeğin yalandan ayırt edilemez hale geldiği, kurumlara olan güvenin çöktüğü ve demokratik süreçlerin içi boşaldığı sentetik etki dönemine girebilir. Böyle bir ortamda, düşmanlar tek bir kurşun bile sıkmadan hedeflerine ulaşabilirken, demokrasiler belirsizlik ve bölünme nedeniyle felç olur. Dolayısıyla bilişsel güvenliğin aşınması, dijital çağda demokratik özyönetimin hayatta kalması için önemsiz bir sorun değil, merkezi bir tehdittir.

Aynı zamanda, temkinli bir iyimserlik için de nedenler vardır. Bilişsel yetenekleri stratejik bir alan olarak kabul ederek, toplumlar dijitalleşmenin zorluklarını aşmak için gerekli olan esnek-dayanıklılığı geliştirebilirler. Bilişsel güvenlik, yalnızca savunma açısından bir gereklilik değil, aynı zamanda olumlu bir hedef sunar: vatandaşların karmaşıklıkla baş edebildiği, manipülasyona direnebildiği ve demokratik yaşama anlamlı biçimde katılabildiği bir toplum. Bu vizyonda teknoloji, insan özerkliğini zayıflatmak yerine güçlendirir, uluslararası işbirliği ise güveni aşındırmak yerine pekiştirir.

Sonuç olarak, yapay zekâ çağı güvenlik manzarasını dönüştürmüştür. Çatışmanın belirleyici alanı artık sadece savaş alanı veya ağ değil, insan zihnidir. Bilişsel güvenlik, bu zorluğun üstesinden gelmek için ulusal ve uluslararası direncin merkezi bir ayağı olarak kabul edilmelidir. Bu görev acildir, ancak aşılamaz değildir. Bilişsel dirençliliğe yatırım yaparak, demokrasiler altyapılarını ve kolektif özyönetim kapasitelerini savunabilirler. Demokrasinin geleceği, bilişsel alanı güvence altına alma becerimize bağlıdır.

KAYNAKÇA

Barrett, L. F., Adolphs, R., Marsella, S., Martinez, A. M., & Pollak, S. D. (2019). Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements. *Psychological Science in the Public Interest,* 20(1), 1–68. https://doi.org/10.1177/1529100619832930

Bone, J. (2017). *Cognitive Hack: The New Battleground in Cybersecurity—the Human Mind.* CRC Press.

Bone, J., & Lee, J. H. (2023). *Cognitive Risk.* CRC Press.

Bufano, P., Rumi, G., & Terlizzi, S. (2023). Digital phenotyping for monitoring mental disorders: A systematic review. *Diagnostics,* 13(21), 3296. https://doi.org/10.3390/diagnostics13213296

Cambridge Social Decision-Making Lab. (2022). *Prebunking interventions in the field: Evidence from randomized experiments.* University of Cambridge.

Card, N. S., Moses, D. A., Chartarifsky-Lewis, R., vd. (2024). An accurate and rapidly calibrating speech neuroprosthesis. *Nature Communications,* 15, 5372. https://doi.org/10.1038/s41467-024-43292-2

Choi, A., Ooi, A., & Lottridge, D. (2024). Digital phenotyping for stress, anxiety, and mild depression: Systematic literature review. *JMIR mHealth and uHealth,* 12, e40689. https://doi.org/10.2196/40689

Damiani, J. (2019, 3 Eylül). A voice deepfake was used to scam a CEO out of $243,000. *Forbes.* https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/

DARPA. (2019, 20 Mayıs). *Six paths to the nonsurgical future of brain–machine interfaces (N3 awards).* https://www.darpa.mil/research/programs/next-generation-nonsurgical-neurotechnology

Dawson, R. (2022, 8 Kasım). *Leading Brain-Computer Interface Companies*. RossDawson.com.https://rossdawson.com/futurist/companies-creating-future/leading-brain-computer-interface-companies-bci/

Department of the Army. (2023, 27 Kasım). *Army Doctrine Publication 3-13, Information*. Army Publishing Directorate. Erişim adresi https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN39736-ADP_3-13-000-WEB-1.pdf

Dubois, D. J., Kolcun, R., Mandalari, A. M., Paracha, M. T., Choffnes, D. R., & Haddadi, H. (2020). When speakers are all ears: Characterizing misactivations of IoT smart speakers. *Proceedings on Privacy Enhancing Technologies,* 2020(4), 255–275. https://doi.org/10.2478/popets-2020-0069

European Commission. (2018). *Action Plan Against Disinformation.* European Union.

European Commission. (2022). *The Digital Services Act.* European Union.

Hao, J. (2018, 25 Mart). *China's "Three Warfares" in Theory and Practice in the South China Sea.* Georgetown Security Studies Review. Erişim adresi https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/

Horvath, J. C., Forte, J. D., & Carter, O. (2015). Quantitative review finds no evidence of cognitive effects in healthy populations from single-session tDCS. *Brain Stimulation,* 8(3), 535–550. https://doi.org/10.1016/j.brs.2015.01.400

Huang, L., & Zhu, Q. (2023). *Cognitive Security: A System-Scientific Approach.* Springer.
Kahneman, D., & Tversky, A. (1974). Judgment under uncertainty: Heuristics and biases. Science, 185(4157), 1124–1131.

Kuhn, T. S. (1962). *The Structure of Scientific Revolutions.* University of Chicago Press.

Lee, M., Posard, M. N., Bond, C. A., & Miller, L. L. (2020). *The Internet of Bodies: Opportunities, risks, and governance* (RR-3226). RAND Corporation. https://www.rand.org/pubs/research_reports/RR3226.html

Makransky, G., & Petersen, G. B. (2021). The cognitive and motivational effects of immersive virtual reality in education: A systematic review and meta-analysis. *Computers & Education,* 157, 103. https://doi.org/10.1016/j.compedu.2020.103010

Ministry of Industry and Information Technology, National Development and Reform Commission, (2025). *Implementation opinions of seven departments on promoting the innovative development of the brain-computer interface industry.* Chinese Government Website. Erişim adresi https://www.gov.cn/zhengce/zhengceku/202508/content_7035603.htm

Moses, D. A., Leonard, M. K., Makin, J. G., & Chang, E. F. (2021). Neuroprosthesis for decoding speech in a paralyzed person with anarthria. *New England Journal of Medicine,* 385(3), 217–227. https://doi.org/10.1056/NEJMoa2027540

NATO. (2021). *NATO 2030: United for a New Era.* NATO Public Diplomacy Division.

Nyhan, B., & Reifler, J. (2010). When corrections fail: The persistence of political misperceptions. *Political Behavior,* 32(2), 303–330.

OECD. (2019). *Recommendation on Responsible Innovation in Neurotechnology.* Organisation for Economic Co-operation and Development. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457

OECD. (2025). *Neurotechnology policy toolkit.* Organisation for Economic Co-operation and Development. https://www.oecd.org/sti/emerging-tech/neurotech-toolkit.pdf

Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War Against Reality.* PublicAffairs.

Price, A. R., McAdams, H., Grossman, M., & Hamilton, R. H. (2015). A meta-analysis of tDCS effects on language measures. *Cortex,* 73, 251–261. https://doi.org/10.1016/j.cortex.2015.09.005

RAND Corporation. (2016). *The Russian "firehose of falsehood" propaganda model.* RAND Research Reports.

Rini, R. (2020). *Deepfakes and the epistemic backstop.* Philosophy & Technology, 33(4), 1–21.

Rouvroy, A., & Stiegler, B. (2016). The digital regime of truth: From the algorithmic governmentality to a new rule of law. *La Deleuziana: Online Journal of Philosophy,* 3, 6–29.

Ropitault, T., vd. (2023). IEEE 802.11bf: Enabling the widespread adoption of Wi-Fi sensing. *NIST Publications.* https://www.nist.gov/publications/ieee-80211bf-enabling-widespread-adoption-wi-fi-sensing

Sahoo, A., vd. (2024). Sensing performance of the IEEE 802.11bf protocol and its overhead. *NIST Technical Note.* https://doi.org/10.1109/VTC2024-Fall63153.2024.10757977

Smalley, S. (2022). *Zelenskyy deepfake crude, but still might be a harbinger of dangers ahead.* CyberScoop. https://cyberscoop.com/zelenskyy-deepfake-troubles-experts/

U.S. Federal Trade Commission. (2023, 20 Mart). *Scammers use AI to enhance their family emergency schemes.* https://www.consumer.ftc.gov/consumer-alerts

U.S. Federal Trade Commission. (2024, 8 Nisan). *Family emergency scams.* https://www.consumer.ftc.gov/consumer-alerts

U.S. Food and Drug Administration. (2018, August 17). *FDA permits marketing of transcranial magnetic stimulation for treatment of obsessive–compulsive disorder.* https://www.fda.gov/news-events/press-announcements/fda-permits-marketing-transcranial-magnetic-stimulation-treatment-obsessive-compulsive-disorder

Van der Linden, S., Leiserowitz, A., Rosenthal, S., & Maibach, E. (2017). Inoculating the public against misinformation about climate change. *Global Challenges,* 1(2), 1600008.

Van der Linden, S., Roozenbeek, J., & Compton, J. (2020). Inoculating against fake news about COVID-19. *Frontiers in Psychology,* 11, 566790.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science,* 359(6380), 1146–1151.

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making.* Council of Europe.

CREATING SOCIETAL
COGNITIVE RESILIENCE
AGAINST INFORMATION
DISORDERS

resaid

JEAN MONNET
CENTRE OF EXCELLENCE

Bu politika belgesi, Avrupa Komisyonu Jean Monnet Mükemmeliyet Merkezleri Programı tarafından desteklenen Bilgi Düzensizliğine Karşı Toplumsal Bilişsel Dirençlilik Yaratmak Projesi (Creating Societal Cognitive Resilience Against Information Disorders - RESAID) kapsamında hazırlanmıştır.

Avrupa Birliği tarafından ortak finanse edilmektedir