

**Güvenlik Pedagojisini Yeniden Düşünmek: Yapay Zekâ ve Siber Çağında
Dayanıklılık Temelli Bir Eğitim**

Rethinking Security Pedagogy: A Resilience-Based Education Model in the
Age of Artificial Intelligence and Cyber Space

Alp Cenk ARSLAN

Dr. Öğr. Üyesi, Polis Akademisi,

İç Güvenlik Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü,

Assistant Professor PhD., Turkish National Police Academy, Faculty of
Homeland Security, Department of Political Science and Public Administration

alpcenkarslan@gmail.com

ORCID: 0000-0002-5526-2089

DOI: 10.56720/mevzu.1811281

Makale Bilgisi | Article Information

Makale Türü / Article Type: Araştırma Makalesi / Research Article

Geliş Tarihi / Date Received: 26 Ekim / October 2025

Kabul Tarihi / Date Accepted: 13 Şubat / February 2026

Yayın Tarihi / Date Published: 15 Şubat / February 2026

Yayın Sezonu / Pub Date Season: Şubat / February

Atıf / Citation: Arslan, Alp Cenk. “Güvenlik Pedagojisini Yeniden Düşünmek: Yapay Zekâ ve Siber Çağda Dayanıklılık Temelli Bir Eğitim”. *Mevzu: Sosyal Bilimler Dergisi*, 15 (Şubat 2026): 191-216. <https://doi.org/10.56720/mevzu.1811281>

İntihal: Bu makale, ithenticate yazılımınca taranmıştır. İntihal tespit edilmemiştir.

Plagiarism: This article has been scanned by ithenticate. No plagiarism detected.
web: <http://dergipark.gov.tr/mevzu> | <mailto:mevzusbd@gmail.com>

Copyright © CC BY-NC 4.0



Öz

Bu çalışma kavramsal model inşası yöntemiyle güvenlik pedagojisinin eğitim bilimlerindeki konumunu yeniden tartışmaya açarak “Güvenlik Pedagojisi 2.0” adını verdiğimiz teknoloji temelli ve dayanıklılık odaklı bir öğretim modelini önermektedir. Literatürde parçalı biçimde gelişen eleştirel güvenlik pedagojisi, ulusal güvenlik alanında simülasyon temelli yaklaşımlar ve siber güvenlik farkındalık eğitimleri güvenlik pedagojisinin disiplinler arası doğasını ortaya koymaktadır. Ancak bu yaklaşımlar henüz bütüncül bir kavramsal çerçeveye kavuşmamıştır. Güvenlik eğitimi ve pedagojisi geçtiğimiz on yıllarda özellikle Batı ülkelerinde kurumsallaşarak gelişmiş, son on yılda ise Türkiye’de açılan yüksek lisans-doktora programları ve lisans programlarında açılan dersler sayesinde giderek daha güncel ve akademik bir boyut kazanmıştır. Bu eğitimlerin pedagojik açıdan kurumsallaştırılması ve uluslararası tartışmalar içerisindeki yerinin netleştirilmesi, alanın ilerlemesi açısından kritik bir ihtiyaçtır. Makale eleştirel pedagoji, dijital pedagoji ve teknoloji temelli yöntemler olmak üzere üç temel boyutu merkeze almaktadır. Eleştirel pedagoji, öğrencileri güvenlik bilgisinin aktif üreticisi haline getirmeyi içermektedir. Dijital pedagoji, siber güvenlik, dezenformasyon ve yapay zekâ okuryazarlığını çağdaş temel yetkinlikler arasında tanımlamaktadır. Son olarak teknoloji temelli yöntemler ise simülasyon, oyunlaştırma ve yapay zekâ destekli öğrenme analitiği ile güvenlik eğitimi daha erişilebilir, etkileşimli ve direnç artırıcı hale getirmektedir. Bu model uluslararası literatür ve Türkiye örneğinden hareketle, güvenlik pedagojisinin yalnızca mesleki alanlarla sınırlı kalmaması, eğitim bilimlerinin merkezinde yenilikçi bir yaklaşım olarak konumlanması gerektiğini savunmaktadır. “Güvenlik Pedagojisi 2.0” hem demokratikleşme ve etik yönelim ilkeleriyle uyumlu hem de dijital çağın gerektirdiği dayanıklılık kapasitesini güçlendiren bir çerçeve sunmaktadır.

Anahtar Kelimeler: Güvenlik Pedagojisi, Dayanıklılık, Siber Güvenlik, Yapay Zekâ, Güvenlik Stratejileri

Abstract

This study reopens the debate on the place of security pedagogy within the field of educational sciences through a conceptual model-building approach and proposes a technology-based and resilience-oriented instructional

model that we call “Security Pedagogy 2.0.” The fragmented development in the literature of critical security pedagogy, simulation-based approaches in national security, and cyber security awareness training reveals the interdisciplinary nature of security pedagogy. However, these approaches have not yet converged into a holistic conceptual framework. Security education and pedagogy have become institutionalized and advanced, particularly in Western countries over the past decades; in the last ten years, they have gained an increasingly contemporary and academic dimension in Türkiye through the establishment of master’s and doctoral programs as well as courses in undergraduate curricula. The pedagogical theorization of these programs and the clarification of their place within international discussions constitute a critical need for the advancement of the field. The article centers on three core dimensions: critical pedagogy, digital pedagogy, and technology-based methods. Critical pedagogy aims to transform learners into active producers of security knowledge. Digital pedagogy defines cyber security, disinformation, and artificial intelligence literacy as essential contemporary competencies. Finally, technology-based methods render security education more accessible, interactive, and resilience-enhancing through simulation, gamification, and artificial intelligence-supported learning analytics. Drawing on international literature and the Turkish case, the model argues that security pedagogy should not be confined to vocational domains alone but should be positioned as an innovative approach at the heart of educational sciences. “Security Pedagogy 2.0” offers a framework that is compatible with principles of democratization and ethical orientation while strengthening the resilience capacity required by the digital age.

Keywords: Security Pedagogy, Resilience, Cyber Security, Artificial Intelligence, Security Strategies

Etik Beyan	Bu çalışmada, metin düzenleme ve dil düzeltme amacıyla Claude 3.5 Sonnet yapay zekâ modeli kullanılmıştır. Tüm analiz, araştırma tasarımı, kuramsal çerçeve, model geliştirme ve sonuçların yorumlanması tamamen yazara aittir. Yapay zekâ, yalnızca metnin dilsel tutarlılığı, akıcılığı ve biçimsel doğruluğu açısından destekleyici bir araç olarak kullanılmış olup, çalışmanın entelektüel içeriği, özgün fikirleri ve bilimsel katkıları üzerinde herhangi bir etkisi bulunmamaktadır.
------------	--

Giriş

Güvenlik kavramının tarihsel evrimi modern devletlerin yükselişi ve Norbert Elias'ın "sivilizasyon süreci" tezi ile yakından ilişkilidir.¹ Elias'a göre, modern toplumlar, meşru fiziksel şiddetin modern devletler tarafından tekelleştirilmesini ve toplumda dürtülerin kontrolünün artmasını içeren devamlı bir süreçten geçmiştir.² Ancak Elias'ın bazı karşıtları özellikle 1980'lerden sonra fiziksel şiddetteki düşüşle birlikte, bu sürecin tersine döndüğünü ve "sivilizasyon dışı süreçlerin" varlığını iddia etmiştir.³ Bu tarihi arka plan günümüzün Yapay Zekâ (YZ) ve siber çağında güvenlik anlayışının kapsamlı bir şekilde yeniden değerlendirilmesini gerektirmektedir. Geleneksel güvenlik paradigması (Güvenlik Pedagojisi 1.0), fiziksel veya kinetik tehditlere odaklanırken siber çağ, veri ihlalleri, bilişsel manipülasyon ve sistematik dezenformasyon gibi yaygın, kinetik olmayan tehditleri içeren yeni bir alan yaratmıştır.⁴ Bu yeni tehdit ortamında kuruluşlar ve bireyler çevrimiçi gözetimi ve mahremiyet erozyonunu tanımlayabilen ve bunlara yanıt verebilen bir epistemik yetkinlik kazanmak durumundadır.⁵

Bu dönüşümün en somut hissedildiği alanların başında, bilginin üretim merkezi olan eğitim kurumları gelmektedir. Dijital çağda eğitim kurumlarının kendileri de benzersiz güvenlik zorluklarıyla karşı karşıyadır. Bu bağlamda eğitim kurumları hassas verileri koruyan teknik yapılar olmalarının dışında, farklı dijital okuryazarlık düzeylerine sahip kullanıcıların güvenlik pratiklerini içselleştirdiği pedagojik alanlardır. Bu kurumlar ayrıca öğrenci kayıtları, araştırma bulguları ve fikri mülkiyet gibi hassas verileri korumak zorundadır-

¹ Hazel Bryan vd., "Securitizing Education, but from What?," *Journal of Social Science Education* (sowi-online e.V., 2023), sowi-online e.V., 1.

² Bryan vd., "Securitizing Education, but from What?," 1.

³ Bryan vd., "Securitizing Education, but from What?," 1.

⁴ Estee Beck vd., "Critical Digital Literacy as Method for Teaching Tactics of Response to Online Surveillance and Privacy Erosion," *Computers and Composition* 61 (September 2021), 102654, 7.

⁵ Beck vd., "Critical Digital Literacy as Method for Teaching Tactics of Response to Online Surveillance and Privacy Erosion", 3.

lar.⁶ Eğitim sektörü farklı dijital okuryazarlık düzeylerine sahip çeşitli bir kullancı tabanına (öğrencilerden deneyimli araştırmacılara kadar) hizmet verdiği için benzersiz zorluklarla yüzleşmektedir.⁷ Ayrıca akademik etik bağlamında sıkı güvenlik önlemleriyle genellikle çelişen bir açıklık ve bilgi paylaşımı teşvik edilmektedir.⁸ Bu zorluklar finansal kısıtlamalarla birleştiğinde eğitim kurumlarını siber saldırılar için cazip hedefler haline getirmektedir.⁹ Bu noktada güvenlik eğitimi kurumsal bir veri koruma prosedürünün ötesine geçerek, öğrencilerin ve araştırmacıların etik değerler ile güvenlik gereklilikleri arasında denge kurabileceği bir karar verme pratiğine dönüşmek zorundadır.

Mevcut literatürde eğitim kurumlarına yönelik saldırıların yıkıcı etkisi genellikle finansal kayıplar üzerinden okunsa da asıl yıkım paydaş güveninin ve akademik özgürlüğün erozyona uğramasıdır.¹⁰ Bu bağlamda güvenlik eğitimi basit bir teknik uyum sürecinin ötesine geçmektedir. Bu yeni ve karmaşık tehditler karşısında verilecek yanıt basit koruma olamamaktadır. Bu yanıt adaptasyon, toparlanma ve eleştirel düşünme kapasitesinin birlikteliğine karşılık gelen dayanıklılık inşası olarak kurgulanmak durumundadır.¹¹

Güvenlik eğitimindeki pedagojik kayma özellikle dezenformasyonun bir silah olarak kullanıldığı kriz anlarında hayati önem kazanmaktadır. Dezenformasyon yanlış bilgi sorununun ötesinde, bir öğrenme ve algı krizidir. Dezenformasyonun yayılmasına ilişkin artan endişeler göz önüne alındığında araştırmaların bu yayılımı azaltmak için kullanılması giderek daha acil bir

⁶ María José Latorre-Medina - Chaimae Tnibar-Harrus, "Digital Security In Educational Training Programs: A Study Based On Future Teachers' Perceptions," *Information Technologies And Learning Tools* 95/3 (June 30, 2023), 106.

⁷ Latorre-Medina - Tnibar-Harrus, "Digital Security In Educational Training Programs: A Study Based On Future Teachers' Perceptions", 102.

⁸ Latorre-Medina - Tnibar-Harrus, "Digital Security In Educational Training Programs: A Study Based On Future Teachers' Perceptions", 105.

⁹ Latorre-Medina - Tnibar-Harrus, "Digital Security In Educational Training Programs: A Study Based On Future Teachers' Perceptions", 109.

¹⁰ Beck vd., "Critical Digital Literacy as Method for Teaching Tactics of Response to Online Surveillance and Privacy Erosion", 16.

¹¹ Bjarte Rød vd., "Combatting Disinformation - How Do We Create Resilient Societies? Literature Review and Analytical Framework," *European Journal for Security Research*, (March 24, 2025), 18.

ihtiyaç haline gelmiştir.¹² Dezenformasyon krizler sırasında acil durum yöneticileri üzerindeki yükü artırmakta ve kafa karışıklığını en aza indirmek, kamu hizmetlerine duyulan güveni artırmak için önleyici (profilaktik) tedbirlerin (aşılama ve medya okuryazarlığı gibi) etkin kullanımı hayati önem taşımaktadır.¹³ Örneğin ABD’deki bir kasırga sonrasında yanlış bilgilerin yayılması Federal Acil Durum Yönetimi Ajansı’nın (FEMA) karşılaştığı dezenformasyon dalgası yanlış anlatıların fiziksel güvenlik tehditlerine nasıl evrilebildiğini göstermiştir.¹⁴ Bu bağlamda güvenlik eğitiminin temel amacı tehdit yönetimi olmaktan çıkıp, bireyleri ve toplumları demokratik süreçleri ve sosyal adaleti tehdit eden manipülasyonlara karşı güçlendiren bir sosyal adalet sağlama aracına dönüşmüştür.¹⁵

Geleneksel güvenlik eğitimine yönelik eleştiriler bilginin pasif öğrencilere basitçe “yatırıldı” bankacılık modeline dayanmasıyla ilgilidir.¹⁶ Güvenlik alanındaki bu yaklaşım, hızla eskimeye yüz tutan ve öğrencileri karmaşık, yeni veya disiplinler arası tehditlere karşı hazırlamada başarısız olan ezberci teknik uyum eğitimleri şeklinde kendini göstermektedir.¹⁷ Geleneksel pedagoji öğrencileri piyasada ve gerçek dünyada talep edilen uygulamalı, disiplinler arası deneyimden mahrum bırakan, ezbere dayalı bir bilgi birikimiyle baş başa bırakmaktadır. Ezbere dayalı bilgi doğası gereği statiktir ve dinamik siber tehditlere veya incelikli etik-sosyal ikilemlere yanıt verememektedir. Bu durum acilen deneyimsel ve özgürleştirici modellere (simülasyonlar, Eleştirel Pedagoji) geçişi gerektirmektedir.¹⁸ Bu çalışma güvenlik pedagojisinin temel bir dönüşüme uğraması gerektiğini savunmaktadır. Bu dönüşüm eksiklik-uyum modelinden *Dayanıklılık Temelli Eleştirel Çerçeveye* (Güvenlik Pedagojisi

¹² Rød vd., “Combatting Disinformation – How Do We Create Resilient Societies? Literature Review and Analytical Framework”, 8.

¹³ Rød vd., “Combatting Disinformation – How Do We Create Resilient Societies? Literature Review and Analytical Framework”, 14.

¹⁴ Rød vd., “Combatting Disinformation – How Do We Create Resilient Societies? Literature Review and Analytical Framework”, 4.

¹⁵ Journal of Democracy and Security, “About This Journal,” *Tandfonline.Com* (2025).

¹⁶ Sabrina Billings, “Critical Pedagogy,” *EBSCO* (2024).

¹⁷ Joseph Simpson - Aaron Brantly, “Security Simulations in Undergraduate Education: A Review,” *Journal of Cybersecurity Education, Research and Practice* 2022/1 (July 2022), 2.

¹⁸ Simpson - Brantly, “Security Simulations in Undergraduate Education: A Review”, 4.

2.0) geçişi ifade etmektedir. Bu yeni model Eleştirel Pedagoji (EP), Kritik Dijital Okuryazarlık ve Yapay Zekâ Destekli Öğrenme Analitiği (YZDÖA) gibi ileri teknoloji temelli yöntemleri merkezine alarak dayanıklılığı inşa etmeyi amaçlamaktadır.¹⁹ Makalenin temel katkısı jeopolitik hedeflerin pedagojik sonuçları nasıl şekillendirdiğini vurgulamak amacıyla Türkiye ve Batı bağlamlarında karşılaştırmalı bir kurumsal analiz sunmasıdır. Bu analiz Batı ülkelerinde kurumsallaşarak gelişen güvenlik eğitiminin²⁰ ve Türkiye’de son on yılda açılan yüksek lisans ve doktora programları sayesinde akademik boyut kazanan alanın²¹ uluslararası tartışmalar içerisindeki yerini netleştirmeyi amaçlamaktadır. Çalışma evrensel olarak uygulanabilir, etik bir “Güvenlik Pedagojisi 2.0” modelini temellendirmek için zemin hazırlamaktadır. Bu model teknik yeterliliğin ötesinde, etik farkındalığı ve demokratik ilkeleri de güvenlik profesyonellerinin temel yetkinlikleri olarak ele almaktadır.²²

2. Kuramsal Çerçeve: Eleştirelilik, Dijitallik ve Etiği Birleştirme

Güvenlik Pedagojisi 2.0’ı temellendiren kuramsal çerçeve, eleştirel pedagoji (EP), eleştirel dijital okuryazarlık (EDO) ve etik boyutları entegre eden bir argüman inşasını zorunlu kılmaktadır. Bu entegrasyon geleneksel güvenlik eğitiminin güç dengesizliklerini pekiştiren yapısını dönüştürmeyi hedeflemektedir. Dolayısıyla Güvenlik Pedagojisi 2.0, üç temel sütun üzerinde yükselmektedir. Bunlar epistemolojik temel olarak Eleştirel Pedagoji, teknolojik müdahale alanı olarak Eleştirel Dijital ve YZ Okuryazarlığı ve etik-demokratik çerçeve olarak güvenlik-özgürlük dengesidir. Bu kavramlar arasındaki etkileşim güvenlik eğitimi teknik bir uzmanlık alanından çıkarıp özgürleştirici bir toplumsal pratiğe dönüştürmektedir.

EP geleneksel okul yapılarının toplumsal eşitsizlikleri ve güç dengesizliklerini “gizli müfredat” yoluyla pekiştirdiğini eleştiren bir eğitim teorisidir.²³ Bu gizli müfredat çeşitli davranışlar hakkında zımni dersler aktarmaktadır. EP

¹⁹ Billings, “Critical Pedagogy” (2024).

²⁰ Omer Caliskan - Hilal Buyukgoze, “The Internationalisation of Turkish Higher Education: A Critical Analysis of Policy,” *Comparative Education*, (July 16, 2025), 103.

²¹ Caliskan - Buyukgoze, “The Internationalisation of Turkish Higher Education: A Critical Analysis of Policy”, 103.

²² Journal of Democracy and Security, “About This Journal” (2025).

²³ Billings, “Critical Pedagogy” (2024).

öğretmenler ve öğrencilerin bu önyargıların farkında olmaları gerektiği fikrini vurgulamaktadır. EP'nin Brezilyalı eğitimci Paolo Freire'den etkilenen temel bileşenlerinden birisi, "eleştirel bilinç" geliştirmektir. Eleştirel bilinç toplumsal önyargıların farkında olunmasını ve bunu eğitim ve aktivizm yoluyla değiştirme taahhüdünü ifade etmektedir. EP bilginin pasif öğrencilere sadece "yatırıldığı" bankacılık modelinden, aktif katılımı ve eleştirel düşünmeyi teşvik eden özgürleştirici bir modele geçişi savunmaktadır.²⁴ Bu durum Güvenlik Pedagojisi 2.0'ın epistemolojik temelini oluşturmaktadır. Böylelikle güvenlik bilgisi yukarıdan aşağıya dikte edilen bir doktrin olmanın ötesine geçerek öğrencinin kendi güvenliğini çevreleyen güç ilişkilerini çözümlediği bir farkındalık süreci olarak yeniden tanımlanmaktadır.

EP güvenlik alanına uygulandığında, devlet merkezli ve kurumsal uyum odaklı geleneksel güvenlik kurumları içindeki güç yapılarını sorgulamayı içeren eleştirel bir bilinç geliştirmeyi amaçlamaktadır. Güvenlik Pedagojisi 2.0 bu nedenle güvenliği kimin ve kimin yararına tanımladığını sorgulamayı içermektedir.²⁵ EP'nin eleştirel perspektifinin eğitim sürecine dahil edilmesi, küresel ilişkiler ve güvenlik konularına eleştirel yaklaşımları müfredata entegre etmek isteyen eğitimciler için önemli kaynaklar sağlamaktadır.²⁶ Bu sayede güvenlik eğitimi, devlet merkezli realizmden uzaklaşarak insan güvenliği meselesine doğru yönelmektedir. Dolayısıyla Güvenlik Pedagojisi 2.0 güvenliği "devletin bekası" parantezinden çıkararak, bireyin ve toplumun ontolojik güvenliğini merkeze alan pedagojik bir paradigma değişimini sunmaktadır.

EP'nin nihai hedefi eğitim deneyimlerini sosyal adalet araçlarına dönüştürmek, iş birlikçi ve kapsayıcı bir öğrenme ortamı aracılığıyla daha adil bir toplumu teşvik etmektir.²⁷ EP uygulamada öğrencileri meşgul etmek ve öğrenmeyi yaşadıkları deneyimlerle ilişkilendirmek için popüler kültür ve günlük metinler de dahil olmak üzere çeşitli materyallerin kullanımını teşvik etmektedir. Bu bağlamda öğrencilerin klişeleri ve hakim anlatıları tanımasına ve

²⁴ Billings, "Critical Pedagogy" (2024).

²⁵ Billings, "Critical Pedagogy" (2024).

²⁶ Security in Context, "New Paradigms for a Deeper Analysis," *Security in Context* (Accessed October 26, 2025).

²⁷ Billings, "Critical Pedagogy" (2024).

sorgulamasına yardımcı olmak için medya analizi, süreç draması ve günlük metinlerin incelenmesi gibi teknikler kullanılmaktadır.²⁸ Siber çağda eğitim, öğrencileri çevrimiçi gözetimi ve mahremiyet erozyonunu tanımlama, anlama ve bunlara yanıt verme konusunda donatmak durumundadır.²⁹ Bu gerçeklik, siber tehditlere karşı dayanıklılığın temel bir bileşenini oluşturmakta ve Eleştirel Dijital Okuryazarlığı'nı (EDO) gerekli kılmaktadır.³⁰ Böylelikle EDO Güvenlik Pedagojisi 2.0 içerisinde teknik bir beceri seti olmanın ötesine geçmekte, dijital uzamdaki görünmez güç yapılarına ve gözetim pratiklerine karşı bir pedagojik önalıcı çözüm olarak konumlandırılmaktadır.

EDO eğitimcilerin ve öğrencilerin çevrimiçi gözetim ve mahremiyet erozyonuna karşı koyma taktiklerini öğrenmeleri için bir çerçeve sunmakta ve bu çerçeve bir kursun, büyük bir ödevin veya ders dışı projelerin bir parçası olarak kullanılabilir. ³¹ YZ'nin yükselişi uzmanlaşmış okuryazarlık çerçevesi olarak kabul edilebilecek Eleştirel YZ Okuryazarlığını (EYZO) zorunlu kılmaktadır. Öğrenciler YZ ile ilgili yanlış bilgilendirme (misinformation), askeri uygulamalar, işgücü uygulamaları gibi geniş bir perspektifteki etik konuları eleştirel bir şekilde analiz etmeli ve algoritmik sistemler içindeki önyargıyı tanımlayabilmelidir.³² EYZO aynı zamanda bireysel etik davranışı teşvik eden uygulamaları belirlemeyi ve benimsemeyi, ayrıca kolektif etik davranışı teşvik eden yapıları oluşturmayı ve sürdürmeyi de içermektedir.³³ Bu bağlamda EYZO algoritmik sistemlerin tarafsızlığı mitini yıkarak Güvenlik Pedagojisi 2.0'ın teknolojik belirlenimciliğe karşı eleştirel bir duruş sergilemesini sağlamaktadır. Zira etik farkındalıkla donatılmamış bir güvenlik eğitimi, algoritmik önyargıların taşıyıcısı olma riski taşımaktadır.

²⁸ Billings, "Critical Pedagogy" (2024).

²⁹ Beck vd., "Critical Digital Literacy as Method for Teaching Tactics of Response to Online Surveillance and Privacy Erosion", 2.

³⁰ Beck vd., "Critical Digital Literacy as Method for Teaching Tactics of Response to Online Surveillance and Privacy Erosion", 3.

³¹ Beck vd., "Critical Digital Literacy as Method for Teaching Tactics of Response to Online Surveillance and Privacy Erosion", 18.

³² Davy Tsz Kit Ng vd., "Conceptualizing AI Literacy: An Exploratory Review," *Computers and Education: Artificial Intelligence* 2 (2021), 100041, 2.

³³ Ng vd., "Conceptualizing AI Literacy: An Exploratory Review", 9.

Bilişsel dayanıklılık inşa etmek için, yanlış ve yanıltıcı bilginin yayılması-na karşı önleyici tedbirler olarak aşılama (inoculation) ve medya okuryazarlığı gibi müdahalelerin etkin kullanımı hayati önem taşımaktadır.³⁴ Aşılama insanların yanlış bilgilere karşı bir “zihin aşısı” geliştirmelerine yardımcı olmayı amaçlamaktadır. Böylesi bir önleyici yaklaşım, krizler sırasında dezenformasyonun yayılmasını azaltarak kamu hizmetlerine duyulan güveni artırma potansiyeline sahiptir.³⁵ Güvenlik eğitimi artık sadece teknik bir mesele değil, temel olarak ahlaki ve demokratik bir konudur.³⁶ Demokratik toplumlarda güvenlik politikaları, güvenlik ihtiyaçları ile demokratik değerler ve süreçler arasındaki dengeyi bulmayı içeren önemli ahlaki, sosyal ve politik ikilemleri beraberinde getirmektedir.³⁷ Bu tür çabalar demokratik toplumların iç tehditlerle mücadelesi, ulusal güvenliğin ahlaki ve hukuki boyutları, kitle iletişimi ve ulusal güvenlik, sivil toplumun rolü ve ulusal güvenlik kararlarını şekillendirmede yasama organının rolü gibi bir dizi konuyu ele almaktadır. Bu nedenle güvenlik müfredatı ahlaki felsefeyi, hukuku ve siyaset bilimini bütünleştirmeli, teknik bilgi-işlem eğitiminin ötesine geçmelidir.³⁸ Aşılama teorisinin bu çerçeveye dahil edilmesi Güvenlik Pedagojisi 2.0’ı sadece proaktif bir model haline getirmektedir. Böylesi bir sistemde eğitim, bireyi dezenformasyona karşı pasif bir alıcı olmaktan çıkarıp, demokratik kamusal alanı savunan bilişsel bir aktöre dönüştürmektedir.

Küreselleşmiş dünyada ülkeler, ekonomiler ve vatandaşlar arasındaki sürekli bağlantı ve etkileşim özel alanın sürekli daralmasına neden olmaktadır.³⁹ Bu durum vatandaşların kendi bilgilerini kontrol edememeleri ve mahremiyetlerinin sürekli tehdit altında olmasıyla sonuçlanmaktadır. Dolayısıyla, gözetimle ilgili güvenlik ile özgürlük ve erişilebilirlik arasındaki felsefi tartışma

³⁴ Rød vd., “Combatting Disinformation – How Do We Create Resilient Societies? Literature Review and Analytical Framework”, 18.

³⁵ Rød vd., “Combatting Disinformation – How Do We Create Resilient Societies? Literature Review and Analytical Framework”, 18.

³⁶ Journal of Democracy and Security, “About This Journal” (2025).

³⁷ Journal of Democracy and Security, “About This Journal” (2025).

³⁸ Journal of Democracy and Security, “About This Journal” (2025).

³⁹ Gonzalo Herranz de Rafael - Juan S. Fernández-Prados, “The Security Versus Freedom Dilemma. An Empirical Study of the Spanish Case,” *Frontiers in Sociology* 7 (February 8, 2022), 2.

yeniden gündeme gelmektedir. Vatandaşlar daha yüksek algılanan güvenlik karşılığında daha düşük özgürlük derecelerini kabul ediyor mu? Ya da daha basitçe, belli bir millet genel olarak daha yüksek bir vatandaş güvensizliği derecesi algılıyor ve karşılığında daha düşük özgürlük derecelerini kabul ediyor mu?⁴⁰ Bu tür sorular Amerikan ve Avrupa liberalizminin farklı vizyonları veya Bauman'ın kapitalist liberalizminin tüketimci yorumu gibi felsefi ayrımlarla bağlantılı karmaşık bir soru havuzunu oluşturmaktadır.⁴¹ Güvenlik Pedagojisi 2.0 bu felsefi ikilemi bir "sıfır toplamı oyun" olarak görmek yerine, güvenlik ihtiyacının özgürlükleri daraltmak için bir bahane olarak kullanılmasını engelleyecek eleştirel bir muhakeme yeteneği inşa etmeyi hedeflemektedir.

Güvenlik Pedagojisi 2.0 öğrencileri bu takas-değişimi nesnel bir şekilde analiz etmeye, demokratik ve eşitlikçi ahlaki ilkeleri uygulamaya teşvik etmelidir. Zira demokratik sosyal seçim prosedürlerinin kuralları eşitlikçi ahlaki ilkeleri bünyesinde barındırsa da demokratik standartlar meşruiyet için bir şekilde gerekli görülmektedir.⁴² Demokratik öneriler hizmet etmeleri amaçlanan toplumlar için uygun tasarımları gerektirmektedir. Böylece bu öneriler temel siyasi eşitlik ilkesiyle bütünleştirilmelidir.⁴³ Güvenlik Pedagojisi 2.0'ın YZDÖA gibi güçlü teknolojileri kullanma zorunluluğu eleştirel pedagoji ilkeleriyle ciddi bir sürtüşme alanı yaratmaktadır. Eleştirel Dijital Okuryazarlık, öğrencilere çevrimiçi gözetim ve mahremiyet erozyonuna karşı çıkmayı öğretirken⁴⁴, YZDÖA sistemleri öğrencilerin zayıf yönlerini ve öğrenme alışkanlıklarını sürekli olarak değerlendirerek, izleyerek ve profileştirerek çalışmakta-

⁴⁰ Herranz de Rafael - Fernández-Prados, "The Security Versus Freedom Dilemma. An Empirical Study of the Spanish Case", 2.

⁴¹ Herranz de Rafael - Fernández-Prados, "The Security Versus Freedom Dilemma. An Empirical Study of the Spanish Case", 2.

⁴² Patti Tamara Lenard - Terry Macdonald, "Democracy versus Security as Standards of Political Legitimacy: The Case of National Policy on Irregular Migrant Arrivals," *Perspectives on Politics* 19/2 (June 28, 2021), 373.

⁴³ International. Idea, *Democracy, Conflict and Human Security* (International Idea, 2006).

⁴⁴ Beck vd., "Critical Digital Literacy as Method for Teaching Tactics of Response to Online Surveillance and Privacy Erosion", 3.

dır.⁴⁵ Bu durum eleştirel bilinç oluşturma hedefine karşı bir paradoks teşkil etmektedir. Bu nedenle Güvenlik Pedagojisi 2.0'ın temel tasarım unsuru öğrencileri pasif gözetim nesneleri olmaktan çıkarıp, kullandıkları eğitim teknolojisi sistemlerini denetleyebilen ve güvenliğini sağlayabilen eleştirel denetçilere dönüştürmek olmalıdır. Bu imkân modelin özgürleştirici çerçevesini korumak için hayati bir adım olarak ortaya çıkmaktadır.⁴⁶

3. Teknolojik Donanım: Aktif Öğrenme ve Dijital Dönüşümün Enstrümanları

Onlarca yıllık araştırma literatürü simülasyon ve oyunlaştırma yöntemlerinin öğrencilerin bilgisini ve konuya olan ilgisini artırmada son derece etkili olduğunu doğrulamaktadır.⁴⁷ Bu yöntemler ezbere dayalı bilgi ile piyasanın uygulamalı deneyim talebi arasındaki açığı kapatmaktadır. Genellikle dersliklerde yıllarca süren derslerle edinilen ezbere dayalı bilgiyle mezun olan öğrenciler pazara girdiklerinde karmaşık ve çoğu zaman incelikli alanların talepleriyle başa çıkmakta yetersiz kalmaktadır. Oysa bu alanlarda en iyi eğitim genellikle deneyimle kazanılmaktadır. Özellikle siber güvenlik gibi alanlarda simülasyonların “uygulamalı” doğası, öğrencilere genellikle stajlar veya ilk işler yoluyla kazanılan simüle edilmiş bir deneyim sağlamaktadır. Simülasyonlar öğrencileri disiplinlerarası eğitim için gerekli olan geniş sorunlar yelpazesine, perspektiflere ve çözümlere maruz bırakmak için en uygun araçtır.⁴⁸ Güvenlikle ilgili alanlar doğası gereği çok yönlüdür ve disiplinlerarasıdır. Popüler ve umut vaat eden simülasyon programları arasında CyberCEIGE ve SEED Labs/DETERLabs bulunmaktadır. CyberCEIGE siber güvenlik kavramlarından (güvenlik duvarı kurma) fiziksel güvenliğe (sınıflandırılmış alanlara erişimi kontrol etme) kadar güvenlik kavramlarını en kapsamlı şekilde içeren simülasyon olarak kaydedilmiştir. Görsel olarak etkileşimli SimCity benzeri bir simülasyon olarak tanımlanmış ve lisans güvenlik eğitiminde en fazla potansiyeli göstermiştir.⁴⁹

⁴⁵ Shaila Rana - Rhonda Chicone, “AI-Driven Personalized Learning in Cybersecurity Training,” *Fortifying the Future* (Cham: Springer Nature Switzerland, 2025), 25.

⁴⁶ Rana - Chicone, “AI-Driven Personalized Learning in Cybersecurity Training”, 26-27.

⁴⁷ Simpson - Brantly, “Security Simulations in Undergraduate Education: A Review”, 5.

⁴⁸ Simpson - Brantly, “Security Simulations in Undergraduate Education: A Review”, 1.

⁴⁹ Simpson - Brantly, “Security Simulations in Undergraduate Education: A Review”, 17.

SEED Labs üniversitelerde yaygın olarak benimsenirken, DETERLabs da 100'den fazla üniversitede kullanılmıştır. Ancak mevcut simülasyon araçlarının kritik sınırlamaları bulunmaktadır. Bu noktadaki en önemli sınırlama bu incelemeden önce hiçbir simülasyonun güvenliğin tüm yönlerini kapsamadığının tespit edilmiş olmasıdır. Bu durum üniversitelerin müfredatı standartlaştırma çabaları için önemli bir kısıtlamadır. Örneğin bazı oyunlar farkındalık gibi konuları kapsarken, savunma veya saldırgan stratejileri ihmal edebilmektedir.⁵⁰ Diğer sınırlamalar arasında birçok değerli platformun artık mevcut olmaması, üniversiteye özgü olması, ücret gerektirmesi veya güncel olmaması yer almaktadır. Bir literatür taramasında tespit edilebileceği üzere, incelenen 28 simülasyonun sadece dokuzu tamamen ücretsiz ve çevrimiçi kullanıma açıktır. Ayrıca çoğu laboratuvar estetik açıdan çekici veya sürükleyici değildir. Gelecek araştırmalar siber güvenlikten afet müdahalesine kadar güvenlik konularını kapsayan kapsamlı simülasyonların geliştirilmesine odaklanmalıdır.⁵¹

YZDÖA sistemleri adaptif olmayan yöntemlere göre daha üstün sonuçlar sağlayarak yatırım getirisi açısından daha avantajlıdır.⁵² Bu sistemler makine öğrenimi algoritmaları ve üretken YZ yeteneklerini kullanarak öğrenci profillerini, güçlü ve zayıf yönlerini sürekli olarak değerlendirmekte ve kariyer hedefleriyle uyumlu, kişiselleştirilmiş eğitim modülleri sunmaktadır.⁵³ Bu kişiselleştirme kapasitesi Rana ve Chicone (2025) tarafından eğitimin önemli bir katkısı olarak belirtilmiştir. Adaptif sistemlerin sunduğu mekanizmalar dinamik, senaryo tabanlı öğrenmeyi mümkün kılmakta ve otomatik olarak yeni tehdit istihbaratını dahil ederek bilgiyi akılda tutmayı artırmaktadır. YZ destekli çözümler geleneksel e-öğrenme platformlarının statik bilgisine karşın eğitim materyallerini adaptif olarak değiştirmekte ve çalışanların uygun zorluk seviyesinde içerik almasını sağlamaktadır.⁵⁴ Bu sistemler performansla ilgili değerli içgörüler ve analitikler de sunmaktadır. Bu yaklaşımın temel fay-

⁵⁰ Simpson - Brantly, "Security Simulations in Undergraduate Education: A Review", 15.

⁵¹ Simpson - Brantly, "Security Simulations in Undergraduate Education: A Review", 16.

⁵² Jan Vykopal vd., "Smart Environment for Adaptive Learning of Cybersecurity Skills," *IEEE Transactions on Learning Technologies* 16/3 (June 1, 2023), 455.

⁵³ Rana - Chicone, "AI-Driven Personalized Learning in Cybersecurity Training", 26.

⁵⁴ Rana - Chicone, "AI-Driven Personalized Learning in Cybersecurity Training", 27.

daları arasında maliyet etkinliği yer almaktadır. Buna göre adaptif öğrenme bireyselleştirildiği için, çalışanlar yalnızca ihtiyaç duydukları konulara ve becerilere odaklanabilmektedir.⁵⁵ Bu hiper-kişiselleştirme siber güvenlikte önemli bir risk unsuru olan insan faktörüne ait bireysel “zayıf noktaları” hassasiyetle belirleyip düzelterek azaltmaktadır. YZDÖA kuruluşların personel geliştirme ve eğitim için daha az harcama yapmasını sağlayarak maliyet etkinliğini artırmaktadır. Bu sistem insan hazırlığının en düşük olduğu alanlara kaynakları yönlendirerek siber güvenlik bütçelerinin optimizasyonuna yardımcı olmaktadır.⁵⁶ Güvenlik Pedagojisi 2.0 teknik becerileri uygulamanın yanında, etik müzakereyi, politika gerekçelendirmesini ve kriz anlatılarının yapı sökümünü gerektiren senaryoları da içermek durumundadır.

Eleştirel Pedagoji teknikleri (medya analizi, süreç draması, günlük metinlerin incelenmesi)⁵⁷, simülasyon tasarımı entegre edilebilmektedir. YZDÖA’nın Eleştirel Pedagoji ile uyumlu bir şekilde çalışması için, sistemin sadece teknik hataları değil, bilişsel önyargıları, etik karar verme kusurlarını ve (aşılma etkinliği metriklerini kullanarak) dezenformasyona karşı güvenlik açığını da izlemesi gerekmektedir.⁵⁸ YZDÖA’nın uygulanması YZ sistemlerinin kendilerini güvence altına almak için sağlam, sahaya hazır stratejilerin benimsenmesini zorunlu kılmaktadır. SANS’ın Güvenli YZ Taslağı, bu operasyonel çerçeveyi detaylandırmaktadır. Bu çerçevenin unsurları Koruma (Protect), Kullanma (Utilize) ve Yönetmedir (Govern).⁵⁹

Koruma (Protect): Saldırgan manipülasyonu, veri sızıntısını ve istenmeyen davranışları önlemek için sistemlere, veri boru hatlarına ve ajans iş akışlarına koruyucu önlemlerin yerleştirilmesidir. Kullanma (Utilize): Savunma yeteneklerini hızlandırmak için YZ destekli iş akışlarının SOC operasyonlarına entegre edilmesi ve ekiplerin görünürlük, kontrol veya yerleşik güvenlik uygulamalarıyla uyum kaybetmeden hızlanmalarının sağlanmasıdır. Yönetme (Govern): YZ’nin iş ve teknik ortamlarda güvenli, etik ve ölçeklenebilir bir

⁵⁵ Vykopal vd., “Smart Environment for Adaptive Learning of Cybersecurity Skills”, 443.

⁵⁶ Vykopal vd., “Smart Environment for Adaptive Learning of Cybersecurity Skills”, 453.

⁵⁷ Billings, “Critical Pedagogy” (2024).

⁵⁸ Rød vd., “Combatting Disinformation – How Do We Create Resilient Societies? Literature Review and Analytical Framework”, 20.

⁵⁹ SANS, “AI Security Starts Here,” *Sans.Org* (2025).

şekilde benimsenmesini sağlamak için araştırma, uyumluluk ve politika hazırlığının sağlanmasıdır. Bahsi geçen operasyonel çerçeve, Güvenlik Pedagojisi 2.0'ın YZDÖA sistemlerinin eleştirel bir denetimini sürdürme ve özgürleştirici çerçevesini koruma zorunluluğuna hayati bir destek sağlamaktadır.⁶⁰

4. Kurumsallaşma ve Jeopolitik

Güvenlik Pedagojisi 2.0'ın uygulanabilirliği, kurumların ve devletlerin yükseköğretimin uluslararasılaşmasına (YÖÜ) yönelik temel rasyonellerine bağlıdır. Türkiye ve Batı ülkeleri bağlamalarının incelenmesi, pedagojik özgürlük ve müfredat tasarımının üzerindeki jeopolitik baskıları ortaya koymaktadır.⁶¹ Batı (Avrupa/ABD) güvenlik eğitimi, artan bir yükümlülükle, güvenlik politikalarının ahlaki, hukuki ve sosyal çıkarımlarını ele alma eğilimindedir. Bu odak noktası iç demokratik yapıdan kaynaklanmakta ve bireysel özgürlüğün ve sivil toplumun rolünün korunmasını vurgulamaktadır.⁶² Batı'daki YÖÜ gerekçeleri genellikle küresel işbirliği, bilgi ekonomisi gereksinimleri ve demokratik standartlarla uyumludur.⁶³ Kurumsal güvenlik felsefesi açıklığı ve bilgi paylaşımını teşvik eden akademik etiği desteklerken⁶⁴, aynı zamanda gözetim ve güvenlik ihtiyacı arasında bir denge kurmayı amaçlamaktadır.⁶⁵ Batı akademik ortamında güvenlik çalışmaları disiplini tarihsel olarak gelişmiştir ve ulusal güvenlik alanında simülasyon temelli yaklaşımlar⁶⁶ ile siber güvenlik farkındalık eğitimleri⁶⁷ yoluyla disiplinlerarası doğasını ortaya koymaktadır. Ancak bu yaklaşımlar henüz bütüncül bir kavramsal çerçeveye kavuşmamıştır.⁶⁸

⁶⁰ SANS, "AI Security Starts Here" (2025).

⁶¹ Caliskan - Buyukgoze, "The Internationalisation of Turkish Higher Education: A Critical Analysis of Policy", 105.

⁶² Journal of Democracy and Security, "About This Journal" (2025).

⁶³ Simpson - Brantly, "Security Simulations in Undergraduate Education: A Review", 5.

⁶⁴ Latorre-Medina - Tnibar-Harrus, "DIGITAL SECURITY IN EDUCATIONAL TRAINING PROGRAMS: A STUDY BASED ON FUTURE TEACHERS' PERCEPTIONS."

⁶⁵ Herranz de Rafael - Fernández-Prados, "The Security Versus Freedom Dilemma. An Empirical Study of the Spanish Case", 3.

⁶⁶ Simpson - Brantly, "Security Simulations in Undergraduate Education: A Review", 1.

⁶⁷ Beck vd., "Critical Digital Literacy as Method for Teaching Tactics of Response to Online Surveillance and Privacy Erosion", 4.

⁶⁸ Bryan vd., "Securitizing Education, but from What?", 8.

Türkiye'nin YÖÜ gündemi ülkeyi bölgesel bir güç olarak konumlandırmak ve Orta Asya, Balkanlar, Orta Doğu ve Afrika gibi bölgelerle bağları güçlendirmek için stratejik olarak kullanılmaktadır.⁶⁹ Bu yaklaşım ana akım YÖÜ anlatılarından önemli ölçüde ayrılmaktadır. Çalışmalar YÖÜ'nün Türkiye'nin küresel ve bölgesel vizyonu ile bağlantılı stratejileri ve hedefleri keşfettiğini göstermektedir. Alandaki çeşitli politika analizleri burs programları ve yurtdışı eğitim kurumları gibi eğitim araçlarının jeopolitik hedefleri ve yumuşak güç anlatılarını desteklemek için açıkça kullanıldığını göstermektedir. Bu stratejik yaklaşım uluslararasılaşmanın daha eleştirel perspektiflerine katkıda bulunan baskın YÖÜ söylemleriyle desteklenirse çok daha güçlü sonuçlar alınabilmesinin yolunu açma potansiyelini taşımaktadır.⁷⁰ Türkiye'nin yüksek öğretimdeki bu stratejik yönelimi, güvenlik pedagojisinin devlet merkezli güvenlik kaygıları ve stratejik hedefler tarafından güçlü bir şekilde etkilenebileceği anlamına gelmektedir. Bu durum Freireci EP'nin savunduğu eleştirel, özgürleştirici odağın öncelikli olmasına engel olabilmektedir. Bu nedenle aynı stratejik hedeflerin insani güvenlik kavramı merkezinde daha eleştirel hale getirilmesi ülkenin de stratejik hedeflerini besleme imkanını yaratacaktır.⁷¹

Türkiye'nin Soğuk Savaş sonrası stratejik değerindeki farklılaşma sonrasında Batılı ve Avrupalı olarak tanınma arayışı, sivilizasyon söylemini kullanarak Avrupa kimliğini ortaya koyma çabasıyla eğitim politikalarını şekillendirmeye devam etmiştir.⁷² Bu bağlamsal durum güvenlik müfredatının teknik olmanın ötesinde jeopolitik anlatılarla uyumlu bir pedagojiyi de benimsemesine neden olabilmektedir.⁷³ Batı pedagojisi demokratik tercihleri korumak amacıyla dezenformasyona karşı bilişsel dayanıklılık geliştirmeye odaklanırken Türkiye kendi stratejik yönelimi doğrultusunda, ulusal bütünlüğü, toplumsal istikrarı ve bilgi güvenliğini merkeze alan bağımsız bir dayanıklılık

⁶⁹ Caliskan - Buyukgoze, "The Internationalisation of Turkish Higher Education: A Critical Analysis of Policy", 109.

⁷⁰ Caliskan - Buyukgoze, "The Internationalisation of Turkish Higher Education: A Critical Analysis of Policy", 108.

⁷¹ Billings, "Critical Pedagogy" (2024).

⁷² Seckin Baris Gulmez vd., "Europe and Turkey: Identities in Evolution. An Analytical Literature Review," *Open Research Europe* 3 (July 26, 2023), 120.

⁷³ Gulmez vd., "Europe and Turkey: Identities in Evolution. An Analytical Literature Review", 120.

anlayışı inşa etmektedir. Bu yaklaşım dış manipölasyonlara karşı koruma sağlamayı hedeflerken, aynı zamanda ulusal anlatıların sürekliliğini ve kurumsal karar alma süreçlerinin özerkliğini güçlendirmeyi amaçlamaktadır.⁷⁴ Güvenlik Pedagojisi 2.0 modeli kurumsal kısıtlamalar ne olursa olsun, devlet destekli olsun veya olmasın, tüm stratejik bilgilendirme biçimlerine uyarlanmış şekilde “eleştirel dayanıklılığı” açıkça tanımlamak durumundadır. Böylece modelin özgürleştirici bir çerçeve olarak bütünlüğü korunabilmektedir.⁷⁵

5. Güvenlik Pedagojisi 2.0 Modeli

Güvenlik Pedagojisi 2.0 konvansiyonel güvenlik eğitiminin eksikliklerini gidermeyi amaçlayan teorik ve teknolojik olarak entegre bir çerçeve oluşturmaktadır. Bu model eleştirel düşünme, bilişsel dayanıklılık ve adaptif yeterliliği tek bir tutarlı döngüde birleştirerek, statik güvenlik eğitiminden dinamik bir öğrenme ortamına geçişi temsil etmektedir.⁷⁶

Model üç ana direk üzerine kurulmuştur. Bunlar eleştirel bilinç, bilişsel dayanıklılık ve adaptif yeterliliklerdir. Eleştirel bilinç, güvenlik politikasındaki güç, önyargı ve gözetim “gizli müfredatını” yapı sökümüne uğratma yeteneğidir.⁷⁷ Bilişsel dayanıklılık (Dijital Pedagoji), aşılama ve medya okuryazarlığı yoluyla manipölasyona ve dezenformasyona karşı önalcı direnç kapasitesidir.⁷⁸ Adaptif yeterlilik (Teknoloji) ise hiper kişiselleştirilmiş uygulamalı, senaryo tabanlı öğrenme yoluyla belirsizlik altında geliştirilen pratik beceri setidir.⁷⁹ Aşağıdaki tablo bu sütunların teorik dayanaklarını ve pedagojik yöntemlerini detaylandırmaktadır.

⁷⁴ SANS, “AI Security Starts Here” (2025).

⁷⁵ Billings, “Critical Pedagogy” (2024).

⁷⁶ Rana - Chicone, “AI-Driven Personalized Learning in Cybersecurity Training”, 27.

⁷⁷ Billings, “Critical Pedagogy” (2024).

⁷⁸ Rød vd., “Combatting Disinformation – How Do We Create Resilient Societies? Literature Review and Analytical Framework”, 18.

⁷⁹ Simpson - Brantly, “Security Simulations in Undergraduate Education: A Review”, 4-5.

Tablo 1. Güvenlik Pedagojisi 2.0'ın Üç Ana Direği

Sütun	Teorik Dayanak	Birincil Hedef	Pedagojik Yöntem
Eleştirel Bilinç	Eleştirel Pedagoji (Freire)	Güvenlik politikasındaki önyargı, güç ve “gizli müfredatı” yapısöküme uğratmak.	Medya Analizi, Süreç Draması, Gündelik Metinlerin Yapısökümü, Özgürleştirici Model
Bilişsel Dayanıklılık	Eleştirel Dijital Pedagoji, YZ Okuryazarlığı	Dezenformasyona ve manipülasyona karşı profilaktik savunma (bilişsel savaş) ve algoritmik önyargının tespiti.	Aşılama, Medya Okuryazarlığı Müdahaleleri, Etik Karar Analizi
Adaptif Yetkililik	Adaptif Öğrenme Teknolojisi, Simülasyon	Belirsizlik altında hiper kişiselleştirilmiş, uygulamalı, esnek güvenlik becerilerinin geliştirilmesi.	Simülasyon, Oyunlaştırma, Yapay Zekâ Destekli Öğrenme Analitiği, Dinamik Tehdit Entegrasyonu

Tablo 1 modelin üç direğini teorik dayanakları, hedefleri ve yöntemleriyle özetlemektedir. Bu yapı eleştirel bilinci temel alarak dijital dayanıklılığı ve teknolojik adaptasyonu bütünleştirmektedir, böylece güvenlik eğitimi bütüncül bir yaklaşıma dönüştürmektedir. Bu noktada tabloda da görülebileceği gibi somut hedefler ve bu hedeflere ulaşmak için kullanılacak spesifik pedagojik araçları olan bütüncül bir çerçeve sunulmaktadır.

Eleştirel Bilinç sütunu modelin epistemolojik zeminini oluşturmaktadır. Burada amaç öğrencinin güvenlik politikalarındaki görünmez güç mekanizmalarını ve “gizli müfredatı” deşifre edebilecek bilişsel bir yapısöküm yeteneği kazanmasıdır. Bilişsel Dayanıklılık sütunu, modelin savunma hattını temsil etmektedir. Dijitalleşen güvenlik ortamında dezenformasyon ve algoritmik manipülasyonlara karşı bireyi bir “pasif nesne” olmaktan çıkarıp, “aşı-

lama" (inoculation) yöntemiyle hibrit tehditlere karşı proaktif bir savunmacı haline getirmeyi hedeflemektedir.

Adaptif Yeterlilik ise modelin uygulama safhasıdır. Geleneksel eğitimin statik yapısının aksine, YZ destekli simülasyonlar ve dinamik senaryolar aracılığıyla öğrencinin yüksek belirsizlik ve kriz anlarında esnek kararlar alabilme kapasitesini, yani pratik beceri setini, geliştirmeye odaklanmaktadır. Özetle Güvenlik Pedagojisi 2.0'ın zihinsel bir farkındalıkla (Eleştirel Bilinç) başlayan, teknik bir koruma kalkanyla (Bilişsel Dayanıklılık) güçlenen ve sonunda esnek bir uygulama yetkinliğiyle (Adaptif Yeterlilik) tamamlanan evrimsel bir öğrenme döngüsü olduğunu ifade etmek gerekmektedir.

Güvenlik Pedagojisi 2.0, simülasyonları basit geçme-kalma senaryolarının ötesine taşımak için YZDÖA'yı kullanmaktadır. YZDÖA makine öğrenimi algoritmalarını kullanarak öğrenme analitiği yoluyla karmaşık senaryolardaki performansı (örneğin, zaman baskısı altında etik ikilemler veya dezenformasyon anlatılarını tanımlama) sürekli olarak değerlendirmekte ve kesin zayıf yönleri belirlemektedir.⁸⁰ Bu süreç organizasyonel güvenlik duruşunu güçlendiren ve insan riskini önemli ölçüde azaltan sürekli bir geri bildirim döngüsü oluşturmaktadır.⁸¹ Sistem YZDÖA teşhislerine dayanarak öğrenme yolunu otomatik olarak uyarlamakta bireyselleştirilmiş modüller sunarak spesifik teknik boşlukları (örneğin savunma stratejisi) veya eleştirel analiz eksikliklerini (örneğin anlatı önyargısını tanımlama) gidermektedir.⁸² Böylece daha önce tespit edilen dar odaklı simülasyonların⁸³ sınırlamasını ele almaktadır. Her senaryodan sonra öğrencilerin EP tekniklerini kullanarak (örneğin süreç draması, medya analizi) güvenlik eylemlerinin etik ve toplumsal sonuçları üzerine yansıtma yapmaları zorunludur.⁸⁴ Bu yansıtma nitel analitik araçlarla değerlendirilmektedir. Bu döngü eleştirel düşünme becerilerinin teknik yeterlilikle birlikte sürekli olarak geliştirilmesini sağlamaktadır. Adaptif öğrenme, motivasyonu artırmak için oyunlaştırmayı da içermektedir.⁸⁵

⁸⁰ Ng vd., "Conceptualizing AI Literacy: An Exploratory Review", 6.

⁸¹ Vykopal vd., "Smart Environment for Adaptive Learning of Cybersecurity Skills", 450.

⁸² Rana - Chiccone, "AI-Driven Personalized Learning in Cybersecurity Training", 27.

⁸³ Simpson - Brantly, "Security Simulations in Undergraduate Education: A Review", 14.

⁸⁴ Billings, "Critical Pedagogy" (2024).

⁸⁵ Vykopal vd., "Smart Environment for Adaptive Learning of Cybersecurity Skills", 450.

Sistemin işleyiş mekanizması teknik verinin pedagojik sonuca nasıl evrildiğini gösteren dört aşamalı bir döngü üzerine kuruludur. Bu döngüsel akış veri noktaları ve pedagojik çıktıları arasındaki ilişkiyle birlikte Tablo 2’de ayrıntılı olarak sunulmuştur.

Tablo 2. Güvenlik Pedagojisi 2.0 Operasyonel Döngüsü: YZDÖA ve Eleştirel Süreç Entegrasyonu

Döngü Aşaması	Mekanizma/Araç	YZDÖA İşlevi/Veri Noktası	Pedagojik Sonuç
Teşhis	Ön Değerlendirme/Başlangıç Senaryosu	Öğrenci profilini, güçlü ve zayıf yönlerini, öğrenme alışkanlıklarını değerlendirme.	Bireysel insan risk elementlerinin belirlenmesi ve eğitim yolunun kariyer hedefleriyle uyumlandırılması.
Müdahale	Adaptif Simülasyon/Oyunlaştırma	Beceri seviyesine göre eğitim materyallerini değiştirme; yeni tehdit istihbaratını ve senaryoları otomatik olarak dahil etme.	Uygulamalı deneyim ve dinamik bilginin geliştirilmesi; bilginin akılda tutulmasının artırılması.
Eleştirel Yanıtma	Senaryo Sonrası Değerlendirme	Etik seçimleri, anlatı yapı-söküm yeteneğini ve bilişsel önyargı zayıflığını takip etme.	Eleştirel bilincin geliştirilmesi ve gözetim/mahremiyet erozyonunun farkındalığı; baskın anlatıların sorgulanması.
Optimizasyon	Boylamsal Analitik	Öğrenme yolunu sürekli olarak iyileştirme; adaptif kapasiteyi ve etik çerçevelere tutarlılığı izleme.	Kurumsal zayıf noktaların azaltılması; insan unsurunun temel bir savunma gücüne dönüştürülmesi.

Tabloda da görülebileceği gibi, Güvenlik Pedagojisi 2.0’ın teorik iddialarının dijital bir öğrenme ortamında nasıl somutlaştığı ve operasyonel hale geldiği aşamalı olarak sunulmaktadır. Bu döngü öğrenciyi teknik bir kullanıcı olmanın ötesine geçirerek, veriye dayalı geri bildirimlerle sürekli gelişen ve etik muhakeme yapabilen bir güvenlik aktörü olarak konumlandırmaktadır.

Teşhis ve Müdahale Aşamaları olarak isimlendirilen ilk iki evre, modelin “adaptif” karakterini temsil etmektedir. YZDÖA sisteminin öğrencinin öğrenme alışkanlıklarını ve zayıf yönlerini (insan riski elementleri) gerçek zamanlı analiz etmesi, eğitimi standart bir kalıp olmaktan çıkarıp “hiperkişiselleştirilmiş” bir deneyime dönüştürmektedir. Burada teknoloji statik müfredatın hantallığını kırarak, en güncel tehdit istihbaratını anında simülasyona dahil eden dinamik bir motor görevi görmektedir.

Eleştirel Yansıtma Aşaması döngünün en hayati noktasıdır. Çoğu simülasyon tabanlı eğitimde eksik olan “etik derinlik”, bu aşamada devreye girmektedir. Öğrenci sadece doğru teknik hamleyi yapmakla kalmamakta, yaptığı hamlenin toplumsal maliyetini, mahremiyet üzerindeki etkisini ve sistemin kendisine sunduğu anlatının önyargılarını sorgulamaya zorlanmaktadır. Böylece modelin eleştirel pedagoji köklerine sadık kaldığı, teknik yeterliliği etik bilinçle mühürlediği aşama ortaya çıkmaktadır.

Son olarak Optimizasyon Aşaması ise eğitimin anlık bir olay değil, boylamsal (zamana yayılan) bir gelişim süreci olduğunu ortaya koymaktadır. Buradaki veri analitiği sadece öğrenciyi değil, kurumsal güvenlik duruşunu da sürekli iyileştirerek insan unsurunu “zayıf halka” olmaktan çıkarıp stratejik savunma hattına dönüştürmektedir.

Güvenlik Pedagojisi 2.0 için müfredat tasarımı, teknik siber güvenlik ve bilgi savunmasından fiziksel güvenlik protokollerine ve afet müdahalesine kadar güvenliğin tüm yönlerini kapsayan “Bütünsel Güvenlik” senaryolarını içermek durumundadır. Böylece öğrencilere siber tehditlerin yanında, siber saldırıların fiziksel güvenlik ihlallerine veya dezenformasyonun toplumsal düzensizliğe nasıl yol açabileceğini de gösteren hibrit tehdit senaryolarını da öğretmeyi gerektirmektedir.

Bu müfredat güvenlik sonuçları ile demokratik-etik ilkeler arasında bir seçim yapmayı gerektiren senaryolara odaklanmaktadır (örneğin mahremiyete karşı müdahale hızı, kitlesel gözetimden kaçınmaya karşı ulusal güvenlik). Bu durum Güvenlik Pedagojisi 2.0’ı basit uyum eğitiminden ayıran, ölçülebilir bir etik karar verme boyutuna ihtiyaç duymaktadır. Eleştirel pedagoji soyut olarak eleştirel bilinci tanımlasa da Güvenlik Pedagojisi 2.0 YZDÖA tarafından ölçülebilir sonuçlar gerektirmektedir. Dolayısıyla eleştirel yansımının

kalitesini, simülasyonlardaki etik seçimleri ve baskın anlatıları yapısöküme uğratma yeteneğini nicel olarak belirleyen yapılandırılmış bir değerlendirme rubriği geliştirilmesini gerektirmektedir.

Değerlendirme metrikleri salt bildirimsel bilginin ötesine geçmek durumundadır. Değerlendirme öğrencilerin yeni tehditlere ne kadar hızlı adapte olduğunu ve eleştirel-etik karar verme çerçevelerini ne kadar tutarlı bir şekilde sürdürdüğünü gösteren boylamsal adaptif kapasiteyi izlemek zorundadır. Güvenlik Pedagojisi 2.0 bu dayanıklılığa odaklanarak stres altında uyum odaklı sistemlerden daha iyi performans gösteren anti-kırılğan güvenlik sistemleri yaratmaktadır. Sistem YZDÖA aracılığıyla bireysel zayıflıkları sürekli olarak iyileştirerek, bilişsel savaşın öngörülemeyen dinamiklerinde hareket edebilen bir işgücü oluşturmakta, insan unsurunu temel bir savunma gücüne dönüştürmektedir.

Modelin etkin bir şekilde yayılması için kurumsal engellerin aşılması gerekmektedir. İleri düzey simülasyon araçlarının maliyet ve erişilebilirlik sorunlarını gidermek amacıyla, politika yapıcılara açık kaynak geliştirme veya kurumsal paylaşım çerçevelerinin teşvik edilmesi önerilmektedir. Zira birçok üniversiteye özgü ücretli veya artık var olmayan platformlar bulunmaktadır.

Kurumsal politikalar Eleştirel Pedagoji ilkeleriyle (YZDÖA-EP Paradoksu) etik sürtüşmeyi yönetmek için YZDÖA uygulaması bağlamında şeffaflık protokollerini zorunlu kılmak durumundadır. Böylece YZ yönetişiminin (Koruma, Kullanma, Yönetme) eğitim teknolojisi alanına tam olarak uygulanması sağlanmış olmaktadır. Ayrıca devlet merkezli stratejik kaygılar ile liberal-demokratik insan güvenliği çerçeveleri arasındaki boşluğu kapatan küresel akademik diyalogun ve çapraz bağlamsal müfredat geliştirmenin teşvik edilmesi jeopolitik farklılıkları kabul ederken standardizasyonu teşvik edecektir. Küresel çalışmalar uluslararası siyasi ekonomi, eleştirel güvenlik ve militarizm çalışmaları gibi alanlardaki eğitimcilere yönelik kaynakların sağlanması, eleştirel perspektiflerin müfredata dahil edilmesini kolaylaştıracaktır.

Sonuç

Modern güvenlik paradigmasının modern devletin inşasından bu yana geçirdiği en radikal dönüşüm, şiddetin fiziksel alandan dijital ve bilişsel mecralara kaymasıyla yaşanmaktadır. Norbert Elias'ın sivilizasyon sürecinde tarif

ettiği meşru şiddet tekeli, günümüzde yerini verinin, algoritmaların ve anlatıların kontrolüne bırakmıştır. Bu çalışma söz konusu dönüşümün eğitim bilimleri perspektifinden ıskalanan “pedagojik” boyutunu merkeze alarak, statik ve uyum odaklı bir yaklaşımdan (Güvenlik Pedagojisi 1.0), dinamik ve dayanıklılık temelli bir modele (Güvenlik Pedagojisi 2.0) geçişin teorik ve pratik imkânlarını soruşturmuştur. Ortaya konulan model siber çağın yarattığı epistemik krizlere karşı proaktif bir öğrenme pratiği önermektedir.

Geleneksel güvenlik eğitimi öğrenciyi “güvenlik prosedürlerinin pasif bir uygulayıcısı” olarak konumlandırır ve Freire’nin “bankacı eğitim modeli” olarak eleştirdiği ezberci bir yapıya dayanmaktadır. Bu yaklaşım tehditlerin öngörülebilir olduğu kinetik dönemlerde işlevsel görünse de YZ manipülasyonlarının ve dezenformasyon dalgalarının yaşandığı mevcut konjonktürde hem bireysel hem de kurumsal kırılğanlıkları derinleştirmektedir. Çalışmanın en temel bulgularından biri, güvenlik eğitiminin teknik bir beceri setinden ziyade, eleştirel bir bilinç düzeyi gerektirdiğidir. Güvenlik Pedagojisi 2.0 içerisinde Eleştirel Pedagoji (EP) ve Eleştirel Dijital Okuryazarlığın (EDO) entegrasyonu, öğrenciyi güvenlik bilgisinin nesnesi olmaktan çıkarıp, bu bilgiyi çevreleyen güç yapılarını analiz edebilen bir denetçi aktöre dönüştürmektedir. Bu durum bireyin gözetim pratiklerine ve mahremiyet erozyonuna karşı geliştireceği “pedagojik direncin” temelini oluşturmaktadır.

Model teknolojik düzlemde ise Yapay Zekâ Destekli Öğrenme Analitiği’ni (YZDÖA) bir gözetim aracı olarak değil, bir özgürleşme ve adaptasyon aracı olarak yeniden kurgulamaktadır. Literatürde genellikle dar odaklı simülasyonların sınırlamalarından bahsedilse de bu çalışma YZDÖA’nın hiperkişiselleştirilmiş geri bildirim döngüleri sayesinde öğrencinin bilişsel zayıf noktalarını (önyargılar, dezenformasyona duyarlılık vb.) tespit edip iyileştirebileceğini kanıtlamaktadır. Burada kritik olan husus teknik yeterliliğin etik muhakeme ile mühürlenmesidir. Modelin operasyonel döngüsünde yer alan “Eleştirel Yansıtma” aşaması, siber güvenlik eylemlerinin toplumsal ve ahlaki sonuçlarını sorgulatarak, teknolojik belirlenimciliğin yarattığı etik körlüğü ortadan kaldırmayı amaçlamaktadır.

Güvenlik Pedagojisi 2.0’ın jeopolitik bağlamdaki uygulanabilirliği, ülkelerin yükseköğretim politikaları ve stratejik anlatılarıyla doğrudan ilişkilidir.

Türkiye’de son on yılda Polis Akademisi, Milli Savunma Üniversitesi, Jandarma ve Sahil Güvenlik Akademisi ve Milli İstihbarat Akademisi gibi kurumlar başta olmak üzere sivil öğrencilere yönelik güvenlik ve istihbarat eğitimleri yaygınlaşmıştır. Bir diğer deyişle güvenlik eğitiminde sivilleşme trendi söz konusudur. Batı’daki liberal demokratik standartlar ile Türkiye’nin bölgesel güç olma vizyonu arasındaki farklar, güvenlik müfredatının önceliklerini şekillendirmektedir. Ancak çalışma göstermektedir ki devletin stratejik hedefleri (ulusal bütünlük, bilgi güvenliği vb.) ile bireyin eleştirel dayanıklılığı arasında bir karşıtlık olmak zorunda değildir. Aksine dezenformasyona ve dış manipülasyonlara karşı bilinçlendirilmiş, demokratik değerleri içselleştirmiş ve teknolojik sistemleri denetleyebilen bir vatandaşlık profili, ulusal güvenliğin en sağlam noktasıdır. Bu nedenle güvenlik pedagojisinin insani güvenlik ekseninde eleştirel bir boyuta taşınması, jeopolitik dayanıklılığı zayıflatmak yerine, toplumun anti-kırılancık kapasitesini artırmaktadır.

Önerilen modelin kurumsallaşması yolundaki en büyük engel YZDÖA-EP paradoksu olarak adlandırabileceğimiz “özgürleştirici eğitim için gözetim temelli teknolojileri kullanma” zorunluluğudur. Bu paradoksun aşılması için eğitim teknolojilerinin şeffaflık, etik yönetim ve eleştirel denetim protokollerine (Koruma, Kullanma, Yönetme) tabi tutulması elzemdir. Güvenlik eğitimi artık dar bir uzmanlık alanının müfredatına hapsedilememekte, dijitalleşen dünyanın her alanında sivil toplumun rolünü, hukukun üstünlüğünü ve ahlaki felsefeyi içine alan disiplinler arası bir sosyal adalet aracı olarak yeniden konumlandırılmalıdır.

Gelecek araştırmalar için bu çalışma iki temel rota çizmektedir. Birincisi, simülasyonlar sırasında sergilenen “eleştirel bilinç” ve “etik karar verme” performanslarını ölçecek nitel ve nicel değerlendirme kıstaslarının geliştirilmesidir. İkincisi ise, dayanıklılık eğitiminin dezenformasyonun yayılım hızı ve kamu güveni üzerindeki uzun vadeli etkilerini inceleyen boylamsal saha araştırmalarıdır. Nihai olarak Güvenlik Pedagojisi 2.0 YZ ve siber alanın belirsiz sularında bireyi teknik bir operatörün ötesine taşıyarak düşünen, sorgulayan ve siber uzamın karmaşasında kendi etik pusulasını belirleyebilen dirençli bir toplum inşası için kapsamlı bir yol haritası sunmaktadır. Bu modelin hayata geçirilmesi güvenlik eğitimi bir zorunluluktan bir özgürleşme pratiğine dönüştürecektir.

Kaynakça

- Beck, Estee vd. "Critical Digital Literacy as Method for Teaching Tactics of Response to Online Surveillance and Privacy Erosion." *Computers and Composition* 61 (September 2021), 102654. <https://doi.org/10.1016/j.compcom.2021.102654>
- Billings, Sabrina. "Critical Pedagogy." EBSCO. 2024. Accessed October 26, 2025. <https://www.ebsco.com/research-starters/education/critical-pedagogy>
- Bryan, Hazel vd. "Securitizing Education, but from What?" *Journal of Social Science Education*. sowi-online e.V., 2023. sowi-online e.V. <https://doi.org/10.11576/jsse-6365>
- Caliskan, Omer - Buyukgoze, Hilal. "The Internationalisation of Turkish Higher Education: A Critical Analysis of Policy." *Comparative Education*, 1-21. <https://doi.org/10.1080/03050068.2025.2520721>
- Gulmez, Seckin Baris vd. "Europe and Turkey: Identities in Evolution. An Analytical Literature Review." *Open Research Europe* 3 (July 26, 2023), 120. <https://doi.org/10.12688/openreseurope.16176.1>
- Herranz de Rafael, Gonzalo - Fernández-Prados, Juan S. "The Security Versus Freedom Dilemma. An Empirical Study of the Spanish Case." *Frontiers in Sociology* 7 (February 8, 2022). <https://doi.org/10.3389/fsoc.2022.774485>
- Idea, International. *Democracy, Conflict and Human Security*. International Idea, 2006.
- Journal of Democracy and Security. "About This Journal." *Tandfonline.com*. 2025. Accessed October 26, 2025. <https://www.tandfonline.com/journals/fdas20/about-this-journal#aims-and-scope>
- Latorre-Medina, María José - Tnibar-Harrus, Chaimae. "Digital Security In Educational Training Programs: A Study Based On Future Teachers' Perceptions." *Information Technologies and Learning Tools* 95/3 (June 30, 2023), 102-111. <https://doi.org/10.33407/itlt.v95i3.5204>

- Lenard, Patti Tamara - Macdonald, Terry. "Democracy versus Security as Standards of Political Legitimacy: The Case of National Policy on Irregular Migrant Arrivals." *Perspectives on Politics* 19/2 (June 28, 2021), 371-387. <https://doi.org/10.1017/S1537592719003402>
- Ng, Davy Tsz Kit vd. "Conceptualizing AI Literacy: An Exploratory Review." *Computers and Education: Artificial Intelligence* 2 (2021), 100041. <https://doi.org/10.1016/j.caeai.2021.100041>
- Rana, Shaila - Chicone, Rhonda. "AI-Driven Personalized Learning in Cybersecurity Training." *Fortifying the Future*. 25-50. Cham: Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-81780-9_2
- Rød, Bjarte vd. "Combating Disinformation – How Do We Create Resilient Societies? Literature Review and Analytical Framework." *European Journal for Security Research*. <https://doi.org/10.1007/s41125-025-00105-4>
- SANS. "AI Security Starts Here." *sans.org*. 2025. Accessed October 26, 2025. <https://www.sans.org/mlp/artificial-intelligence>
- Security in Context. "New Paradigms for a Deeper Analysis." *Security in Context*. Accessed October 26, 2025. <https://www.securityincontext.com/pedagogy-overview>
- Simpson, Joseph - Brantly, Aaron. "Security Simulations in Undergraduate Education: A Review." *Journal of Cybersecurity Education, Research and Practice* 2022/1 (July 2022). <https://eric.ed.gov/?id=EJ1360328>
- Vykopal, Jan vd. "Smart Environment for Adaptive Learning of Cybersecurity Skills." *IEEE Transactions on Learning Technologies* 16/3 (June 1, 2023), 443-456. <https://doi.org/10.1109/TLT.2022.3216345>