Black Sea Journal of Artificial Intelligence
doi: 10.5281/zenodo.18213751

Open Access Journal
e-ISSN: 3108-4281

Derleme (Review)
Cilt 1 - Sayı 1: 31-34 / Haziran 2025
(Volume 1 - Issue 1: 31-34 / June 2025)

YAPAY ZEKA ÇAĞINDA BİLGİSAYAR AĞLARI YÖNETİMİ VE GÜVENLİĞİ

Serkan VARAN[1]*

[1]*Ondokuz Mayıs University, Çarsamba Chamber of Commerce Vocational School, Department of Computer Technologies, 55200, Samsun, Türkiye*

Özet: Veri miktarının artmasına bağlı olarak, yapay zekanın bilgisayar ağlarıyla olan etkileşimi çok sayıda yeniliğe yol açtı. Ağlar üzerinde büyük miktarda veri akışı, toplumu ileriye taşıyan bir yenilik olarak karşımıza çıktı. Modern toplumda bilgi iletimi ve işlenmesi için önemli bir yöntem olan bilgisayar ağ teknolojisi, muazzam dönüşümler geçirmektedir. Büyük veri kavramı, ağ mimarisi, protokoller ve hatta güvenlik önlemleri için benzeri görülmemiş zorluklar ve fırsatları beraberinde getirmektedir. Aynı zamanda, yapay zeka teknolojilerinin hızla ilerlemesi bu olguyu daha da güçlendirmektedir. Ağ güvenliğinin ve yönetiminin her aşaması, yapay zekanın sunduğu verimliliği ve akıllı çözümleri kullanmaya başlamıştır. Bu sinerji, ağ teknolojisini geleneksel sınırların ötesine taşımakta ve daha fazla zeka ve verimlilik vaat eden bir geleceğe doğru ilerlemektedir.

Anahtar kelimeler: Büyük veri, Yapay zeka, Ağ güvenliği, Ağ yönetimi

Computer Network Management and Security in the Age of Artificial Intelligence

Abstract: Due to the increasing amount of data, the interaction of artificial intelligence with computer networks has led to many innovations. The flow of large amounts of data over networks has emerged as an innovation that moves society forward. Computer network technology, an important method for transmitting and processing information in modern society, is undergoing tremendous transformations. The concept of big data brings with it unprecedented challenges and opportunities for network architecture, protocols, and even security measures. At the same time, the rapid advancement of artificial intelligence technologies further strengthens this phenomenon. Every stage of network security and management has begun to use the efficiency and intelligent solutions offered by artificial intelligence. This synergy is taking network technology beyond traditional boundaries and moving towards a future that promises greater intelligence and efficiency.

Keywords: Big data, Artificial intelligence, Network security, Network management

***Sorumlu yazar (Corresponding author):** Ondokuz Mayıs University, Çarsamba Chamber of Commerce Vocational School, Department of Computer Technologies, 55200, Samsun, Türkiye
E mail: svaran@omu.edu.tr (S. VARAN)
Serkan VARAN https://orcid.org/0000-0001-7669-9709

Gönderi: 09 Mayıs 2025 **Received:** May 09, 2025
Kabul: 30 Mayıs 2025 **Accepted:** May 30, 2025
Yayınlanma: 15 Haziran 2025 **Published:** June 15, 2025

Cite as: Varan, S. (2025). Computer network management and security in the age of artificial intelligence. *Black Sea Journal of Artificial Intelligence*, *1*(1), 31–34.

1. Giriş

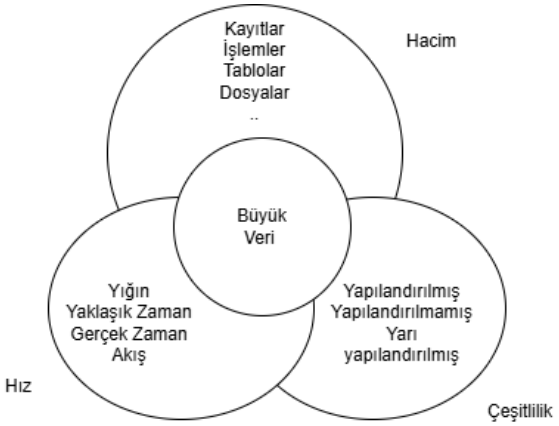
Küresel veri hacimlerinde olağanüstü bir artışla işaretlenen bir çağda, "büyük veri" terimi akademideki kökenlerini aşmış ve kamu bilincine nüfuz etmiş, tanımını yalnızca veri kümeleri koleksiyonunun ötesine taşıyarak teknoloji, sosyal dinamikler ve hatta politika yapımında bir direktifin karmaşık bir birleşimini somutlaştırmıştır. Benzer şekilde, "yapay zeka" bilim kurguya yerleşmiş bir kavramdan çağdaş teknolojilerin ilerlemesini ilerleten temel güç haline gelmiştir. Bu bağlamda, bu varlıklar arasındaki etkileşim artık tek yönlü değil, karmaşık ve etkileşimli bir ilişkiye dönüşmüştür (Nowroozi vd., 2025). Bilgisayar ağ teknolojisi tüm toplumsal katmanları kesiştiren bir yaşam kaynağı olarak hizmet ettiğinden, bu yoğun veri işleyişi ve evrimi, temel roller üstlenmek için yapay zekayı acilen kullanmak zorundadır. Ağ teknolojileri ve toplumsal yaşam arasındaki bu entegrasyon, verimliliği artırmak, güvenliği güçlendirmek ve sunulan sayısız zorlukla yüzleşmek için zorunludur. Bu yeni paradigmaya göre, yapay zekanın bilgisayar ağları alanında uygulanması hem teknik bir bilmece hem de iş ve günlük yaşamı kökten değiştirebilecek kritik bir belirleyici olarak karşımıza çıkmaktadır (Marino vd., 2025).

Bu çalışmanın amacı, büyük verinin karakteristik özelliklerini ortaya çıkararak, bilgisayar ağları yönetimi ve güvenliğinde kullanılan yapay zeka teknolojilerini açıklamaktır.

2. Büyük Verinin Karakteristik Özellikleri

Bilgi çağının gelmesiyle birlikte, bireyler giderek verinin toplumsal başkalaşımı ve 'Büyük Veri' çağının gelişiyle başlayan teknolojik yeniliği ilerleten yeni bir motor olarak ortaya çıktığını fark ettiler. Büyük Veri çağı, internet, Nesnelerin İnterneti ve genişleyen bir dizi akıllı cihaz aracılığıyla üretilen hacimli veri hazineleriyle

karakterize edilir, zorluklar yaratır ve geleneksel veri işleme metodolojileri üzerinde güçlü etkiler uygularken, aynı zamanda sayısız endüstriye dönüştürücü gelişmeler olasılığı sunar (Altunay, 2024). Bu çağın bağlamında, veri hacimlerindeki büyüme en belirgin ayırt edici özellik olarak durmaktadır. Her saniye, sayısız birey ve makine muazzam miktarda veri üretmekte, sosyal medyanın metinlerinden, görüntülerinden ve videolarından ticari işlemlerin kayıtlarına, IoT cihazlarından gelen sensör okumalarına ve kapsamlı tıbbi görüntüleme veri kümelerine kadar bu veri çok çeşitli olarak karşımıza çıkmaktadır (Qiao, 2025). İçeride gizlenen bilgiler terabaytlardan (TB) petabaytlara (PB) ve hatta eksabaytlara (EB) sıçramıştır. Bu noktada bu verilerin yönetimi ve güvenliğinin sağlanması veri merkezleri ortaya çıkmıştır. Veri Merkezi, İnternet ağ altyapısında veri bilgilerini iletmek, hızlandırmak, görüntülemek, hesaplamak ve depolamak için kullanılan belirli ekipmanlardan oluşan küresel bir ağdır. Veri merkezinin elektronik bileşenlerinin çoğu, düşük voltajlı DC güç kaynakları tarafından çalıştırılır. Veri türlerinin çeşitliliği de benzer şekilde gelişmekte olup, çeşitli biçimlerde ve karmaşık yapılarda sunulmaktadır. Veritabanı tabloları gibi geleneksel yapılandırılmış veriler artık tüm talepleri karşılamaya yetmemektedir; metin, resim ve video gibi yapılandırılmamış veri türleri ve e-postalar ile günlük dosyaları gibi yarı yapılandırılmış içerikler Büyük Veri'nin heterojenliğini oluşturmaktadır. Bireylerin davranışsal verileri ve makinelerin operasyonel verileri de dikkate alınmak üzere kapsanmaktadır (Lacava vd., 2025). Hem veri hacmindeki hem de çeşitlilikteki artışla birlikte veri işleme hızlarına yönelik talep de artmaktadır. İşletmeler ve organizasyonlar, piyasa dalgalanmalarına yanıt olarak hızlı kararlar almak için bu geniş veri kümelerini gerçek zamanlı olarak analiz etmeyi arzulamaktadır ve bu da veri işleme teknolojilerine yönelik talepleri artırmaktadır. Örneğin, gerçek zamanlı veri işleme ve akış hesaplamasının gelişen alanı, bu hız arayışını ele almaya hizmet etmektedir. Belki de en heyecan verici değişim, verinin içsel değerinin yükselişinde ve kazılmasında yatmaktadır. Her veri kümesinin içinde keşfedilmeyi bekleyen gizli bir değer bulunmaktadır. Büyük verinin üç temel bileşeni olan hacim, hız ve çeşitlilik kavramları Şekil 1'de gösterilmiştir. İşletmeler ve araştırma kurumları, desenleri belirlemek, eğilimleri tahmin etmek ve devasa veri kümelerinden stratejiler geliştirmek için veri madenciliği, makine öğrenimi ve yapay zekanın güçlerinden yararlanmaktadır. Örneğin, e-ticaret platformları kullanıcı davranış verilerini analiz ederek daha kişiselleştirilmiş ürün önerileri sunabilir; doktorlar hasta sağlık kayıtlarının analizi yoluyla hastalıkları daha yüksek bir hassasiyetle teşhis edebilir. Yine de, bu umut vadeden yeni alan, pek çok zorluğu da barındırmaktadır. Veri güvenliği ve gizliliğin korunması yaygın olarak tartışılan endişeler haline gelmiştir. Bireysel gizliliği korurken verilerin değerini nasıl çıkaracağımız ve veri kullanımının sunduğu kolaylıklardan yararlanırken bilgi ihlallerini nasıl önleyeceğimizle ilgili sorular, sektör uzmanlarının, akademisyenlerin ve politika yapıcıların topluca ele alması gereken konulardır (Altunay, 2025).



Şekil 1. Büyük verinin temel bileşenleri.

3. Yapay Zeka Çağında Network Yönetimi ve Güvenliği

Siber güvenlik, ağ sistemlerini yetkisiz erişimden, saldırılardan ve diğer olası tehlikelerden korumak için teknolojik ve yönetimsel stratejiler kullanan kapsamlı bir kavramdır. Temel ilkeleri yalnızca verilerin bütünlüğünü ve kullanılabilirliğini korumayı değil, aynı zamanda bilgilerin gizliliğini sağlamayı ve böylece hassas ayrıntıların ifşa edilmesini önlemeyi amaçlar. Sürekli gelişen ve evrimleşen bu dijital alemde, yapay zeka siber güvenlik alanında vazgeçilmez bir güç olarak ortaya çıkmıştır. Siber güvenlik alanında titiz ve hassas bir bekçi olarak, yapay zeka teknolojileri, güvenlik tehditlerinin ve savunma önlemlerinin artan karmaşıklığına otomatik olarak uyum sağlamak ve uyum sağlamak için makine öğrenimi algoritmalarını uygular. Veri yığınlarının ortasında, yapay zeka yorulmak bilmeden günlük dosyalarını analiz eder, anormal davranışları izler ve hatta tehditlerdeki eğilimleri tahmin eder. Geleneksel güvenlik yöntemleriyle yan yana getirildiğinde, yapay zeka yeni ortaya çıkan kötü amaçlı yazılımları ve sıfırıncı gün güvenlik açıklarını daha hızlı bir şekilde belirleyebilir ve bunlara yanıt verebilir (Altunay ve Albayrak, 2024). İnternet etkileşimlerinin hareketlerinde, sayısız güvenlik tuzağı gizlidir. Bilgisayar korsanları taktiklerini sürekli olarak geliştirirken, yapay zeka bu zorlukların üstesinden gelmek için devamlı eğitilir. Örneğin, yapay zeka, derin öğrenme becerisi sayesinde, çok sayıda kimlik avı e-postasındaki ince kalıpları ayırt edebilir, böylece bunları filtreleyebilir ve kullanıcıları aldatmadan koruyabilir. Özellikle evrişimli sinir ağları, uzun kısa süreli bellek ve otokodlayıcılar bu alanda kullanılmaktadır. Akıllı sistemler, kendilerini durmaksızın geliştirmek için mevcut bilgilerini kullanır ve böylece giderek daha da aşılmaz bir dijital kale inşa eder. Dahası, yapay zekanın siber güvenlik çözümlerine entegre edilmesi daha karmaşık erişim kontrolüne olanak tanır. Akıllı teknoloji, kullanıcı davranış kalıplarını inceleyerek olası iç

tehditlere daha hızlı tepki verebilir. Belirli kullanıcıların tipik faaliyetlerini tanır ve kullanıcı kimlik bilgilerinin kötüye kullanılması gibi anormal faaliyetleri tespit ettiğinde derhal uyarılar yayınlar ve hassas verilere ve kritik altyapıya uygunsuz erişimi kısıtlar. Somut dünyada, finans kuruluşlarının siber güvenlik uygulamaları öğretici bir örnek sunar. Son yıllarda, birkaç banka finansal dolandırıcılıkla mücadele etmek için yapay zeka destekli güvenlik sistemleri konuşlandırmaya başladı. Sürekli olarak çeşitli işlem verilerinden öğrenen bu sistemler, bir müşterinin olağan modelinden sapan işlemleri anında belirleyebilir ve potansiyel dolandırıcılık eylemlerini derhal önleyebilir, böylece müşterilerin finansal varlıklarını koruyabilir (Lin, 2024).

İnternetin geniş evreninde, ağ yönetimi ve optimizasyonu, hızlı ve verimli bilgi akışını sağlayarak akıllı bir gezgin gibi işlev görür. Bu sistemler, ağ koşullarının dikkatli bir şekilde izlenmesi, veri trafiğinin incelenmesi ve kaynak dağıtımının ayarlanması yoluyla ağ istikrarını ve en yüksek performansı sürekli olarak korur. Yapay zekanın hızlı evrimiyle, ağ yönetimi ve optimizasyonunun tüm yönlerine sızmıştır. Derin öğrenme gibi teknolojileri kullanan yapay zeka tabanlı sistemler, kafa karıştırıcı bir senfonideki melodiyi ayırt etmeye benzer şekilde, ağ verilerinin karmaşıklıkları arasında trafik modellerini ayırt edebilir. Sadece en yüksek kullanım sürelerini tahmin etmekle kalmaz, aynı zamanda olası tehlikeleri önlemek için önceden alarm sinyali veren dikkatli koruyucular olarak hareket ederek anormal trafiği hızla belirlerler. Yapay zeka, ağ kaynak tahsisinde kayda değer ilerlemeler kaydetmiştir. Bant genişliği kullanımını gerçek zamanlı olarak optimize etti ve kaynakların gerektiği gibi kullanıcılar arasında dağıtılmasını sağlamak için veri yönlendirmesini hassasiyetle yürüttü (Yao vd., 2025). Böylece, her veri paketi en verimli rota boyunca yönlendirilir, bu da geniş dijital alemde özel bir yol oluşturmaya benzer. Örneğin, yapay zeka görüntülü konferans talebinde bir artış tespit ettiğinde, derhal ek bant genişliği tahsis eder, kesintisiz iletişimi kolaylaştırmak ve önemli toplantıların sorunsuz bir şekilde yürütülmesini sağlamak için geniş bir bilgi köprüsü oluşturur. Dahası, yapay zeka sürekli öğrenme ve kendini iyileştirmede mükemmeldir, böylece ağ yönetiminin zekasını geliştirir. Yeterli bir geçmiş veri kümesi topladıktan sonra, yapay zeka gelecekteki ağ ihtiyaçlarını daha doğru bir şekilde tahmin edebilir, dalgalanan yükleri karşılamak ve kaynak israfını önlemek için ağ stratejilerini dinamik olarak ayarlayabilir. Böyle bir ağ yönetim sistemi, deneyimli bir stratejistin ağ kaynaklarının verimli kullanımını en üst düzeye çıkarması gibi, sürekli öğrenme, tahmin ve ayarlama yoluyla bilgeliğini keskinleştirir. Bununla birlikte, teknolojik gelişmeler asla izole bir şekilde gerçekleşmez. Ağ optimizasyonunun sağlanmasında da yapay zeka araçları önemli bir yer tutar. Herhangi bir donanım eklemeden gelişmiş araçlar ve özelleştirilmiş ağ yapılandırmaları sayesinde ağ verimliliği arttırılabilmektedir. Yapay zeka ağ optimizasyonunu iyileştirdikçe, gizlilik ve güvenlik hususları en önemli hale gelir. Her ilerleme, veri hassasiyeti ve olası ağ güvenlik açıklarının derinlemesine anlaşılması ve dikkatli bir şekilde değerlendirilmesine dayanmalıdır. Bu nedenle, teknolojinin uygulanmasına devam eden keşif ve olası etik ve güvenlik sorunlarının derinlemesine düşünülmesi eşlik eder ve akıllı optimizasyonun gelecekteki ağ ortamının istikrarı ve güvenliğiyle el ele ilerlemesini sağlar (Effah vd., 2025). Günümüzde pek çok yapay zeka tabanlı araç bilgisayar ağlarının yönetiminde ve güvenliğinin sağlanmasında kullanılmaktadır. Bu araçlar Tablo 1'de gösterilmiştir.

Tablo 1. Bilgisayar ağlarının yönetiminde ve güvenliğinde kullanılan yapay zeka tabanlı araçlar

Araç Adı	Alan
IBM /Watson (Newman, 2018)	Yönetim ve güvenlik
Juniper Networks (Madrid, 2020)	Yönetim ve güvenlik
Balbix Breach Control (Bablix, 2021)	Güvenlik
bioHAIFCS (Demertzis ve Iliadis, 2015)	Güvenlik
CyberSecTK (Calix vd., 2020)	Güvenlik
Vectra Cognito (Vectra, 2021)	Yönetim ve güvenlik
DefPloreX (Balduzzi ve Maggi, 2017)	Yönetim ve güvenlik
IBMQRadar (IBM, 2021)	Güvenlik
StringSifter (Stigsifter, 2020)	Yönetim ve güvenlik
InterceptX (Intercept, 2020)	Güvenlik
TAA (Symantech, 2018)	Yönetim ve güvenlik

4. Tartışma ve Sonuç

Büyük veri ve yapay zeka arasındaki sinerjik etkileşim, bilgisayar ağ teknolojisinin ilerlemesi için sınırsız umutlar müjdelemektedir. Ağ güvenliği, yönetimi, veri analitiği ve hatta bulut bilişim alanlarındaki uygulamalarına derinlemesine inerek, yapay zeka hızla bilgisayar ağlarının entelektüelleştirilmesi için vazgeçilmez bir katalizör haline gelmektedir. Bununla birlikte, verilerin gizliliğini ve güvenliğini korumak, yapay zeka sistemlerinin şeffaflığını ve yorumlanabilirliğini artırmak ve insan uzmanlığıyla en uygun iş birliğini belirlemek de dahil olmak üzere bir dizi zorlukla karşı karşıya kalınması gerekmektedir. İleriye bakıldığında, teknolojik yenilikler bu alanlardaki bilgisayar ağlarının olgunlaşmasını ilerletmeye devam edecek ve yapay zekanın geniş veri depolarıyla entegrasyonuna daha fazla vurgu yaparak, böylece bir bütün olarak toplumsal ilerlemeyi hızlandıracaktır.

Katkı Oranı Beyanı

Yazarın katkı yüzdeleri aşağıda verilmiştir. Yazar makaleyi incelemiş ve onaylamıştır.

%	N.K.
K	100
T	100
Y	100
VTI	100
VAY	100
KT	100
YZ	100
GR	100
PY	100

K= kavram, T= tasarım, Y= yönetim, VTI= veri toplama ve/veya işleme, VAY= veri analizi ve/veya yorumlama, KT= kaynak tarama, YZ= Yazım, GR= gönderim ve revizyon, PY= proje yönetimi.

Çatışma Beyanı

Yazar bu çalışmada hiçbir çıkar ilişkisi olmadığını beyan etmektedirler.

Kaynaklar

Altunay, H. C. (2024). Analysis of cyber attacks using honeypot. *Black Sea Journal of Engineering and Science*, *7*(5), 954–959. https://doi.org/10.52704/bsscience.1481075

Altunay, H. C. (2025, April 24–25). *Dijital ekonomi ve blok zinciri uygulamaları* [Bildiri sunumu]. 5. Uluslararası Yapay Zeka ve Veri Bilimi Kongresi, İzmir, Türkiye.

Altunay, H. C., & Albayrak, Z. (2024). SMS spam detection system based on deep learning architectures for Turkish and English messages. *Applied Sciences*, *14*(24), 11804. https://doi.org/10.3390/app142411804

Balbix. (2021). *Balbix BreachControl*. https://www.balbix.com/product-overview/

Balduzzi, M., & Maggi, F. (2017). *DefPloreX: A machine-learning toolkit for large-scale eCrime forensics*. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/defplorex-machine-learning-toolkit-large-scale-ecrime-forensics/

Calix, R. A., Singh, S. B., Chen, T., Zhang, D., & Tu, M. (2020). Cyber security tool kit (CyberSecTK): A Python library for machine learning and cyber security. *Information*, *11*(2), 100. https://doi.org/10.3390/info11020100

Demertzis, K., & Iliadis, L. (2015). A bio-inspired hybrid artificial intelligence framework for cyber security. In N. Daras & M. Rassias (Eds.), *Computation, cryptography, and network security* (pp. 161–193). Springer. https://doi.org/10.1007/978-3-319-18275-9_7

Effah, E. Q., Osei, E. O., Jnr, M. D., & Tetteh, A. (2024). Hybrid approach to classification of DDoS attacks on a computer network infrastructure. *Asian Journal of Research in Computer Science*, *17*(4), 19–43. https://doi.org/10.9734/ajrcos/2024/v17i4427

FireEye. (2020). *StringSifter: A machine learning tool that ranks strings based on their relevance for malware analysis* [Computer software]. GitHub. https://github.com/mandiant/stringsifter

IBM. (2021). *QRadar Advisor with Watson*. https://www.ibm.com/in-en/products/cognitive-security-analytics

Lacava, A., Bonati, L., Mohamadi, N., Gangula, R., Kaltenberger, F., Johari, P., & Melodia, T. (2025). dApps: Enabling real-time AI-based Open RAN control. *Computer Networks*, *254*, 111342. https://doi.org/10.1016/j.comnet.2024.111342

Lin, Y. (2024). Application and challenges of computer networks in distance education. *Computer Performance and Communication Systems*, *8*(1), 17–24.

Madrid, S. (2020). *Juniper strengthens connected security portfolio with new risk-based access control capabilities and remote access VPN*. Juniper Networks. https://blogs.juniper.net/en-us/security/juniper-strengthens-connected-security-portfolio-with-new-risk-based-access-control-capabilities-and-remote-access-vpn

Marino, D. L., Wickramasinghe, C. S., Rieger, C., & Manic, M. (2025). Self-supervised and interpretable anomaly detection using network transformers. *IEEE Transactions on Industrial Informatics*, *21*(5), 4252–4261. https://doi.org/10.1109/TII.2024.3414920

Newman, L. H. (2018). AI can help cybersecurity—If it can fight through the hype. *Wired*. https://www.wired.com/story/ai-machine-learning-cybersecurity

Nowroozi, E., Haider, I., Taheri, R., & Conti, M. (2025). Federated learning under attack: Exposing vulnerabilities through data poisoning attacks in computer networks. *IEEE Transactions on Network and Service Management*, *22*(1), 822–831. https://doi.org/10.1109/TNSM.2024.3444055

Qiao, W. (2025). Comprehensive framework for collaborative decision-making in evaluating computer network security using interval neutrosophic information. *Neutrosophic Sets and Systems*, *76*, 520–537.

Sophos. (2020). *Intercept X: Stop unknown threats*. https://www.sophos.com/en-us/products/intercept-x

Symantec. (2018). *Targeted attack analytics*. Broadcom. https://docs.broadcom.com/doc/targeted-attack-analytics-en

Vectra AI. (2021). *Cognito Platform: Network detection and response built on artificial intelligence*. https://www.vectra.ai/products/cognito-platform

Yao, K., Pan, F., Liang, H., Zhang, X., Li, L., Song, L., & Lu, W. (2025). Shifting d-band center: An overlooked factor in broadening electromagnetic wave absorption bandwidth. *Advanced Functional Materials*, *35*(3), 2413639. https://doi.org/10.1002/adfm.202413639