GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2024, 20:47, 123-145
DOI: 10.17752/guvenlikstrtj.1403312

Araştırma Makalesi
Research Article

Ordular ve Dijital Dönüşüm: Sorunlar ve Çözümler

Armed Forces and Digital Transformation: Challenges and Prospects

Murat SAĞBAŞ*
Fahri Alp ERDOĞAN**
Mehmet N. UĞURAL***
Arzu UĞURLU KARA****

*Doç.Dr., Millî Savunma Üniversitesi Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü (ATASAREN), Savunma Yönetimi Anabilim Dalı, İstanbul, Türkiye, ORCID: 0000-0001-5179-7425,
e-posta: muratsagbass@gmail.com

** Arş. Gör., Millî Savunma Üniversitesi, Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü (ATASAREN), Savunma Yönetimi Anabilim Dalı, İstanbul, Türkiye, ORCID: 0000-0001-6069-5981,
e-posta: falperdogan98@gmail.com

*** Doç. Dr., İstanbul Kültür Üniversitesi, Mühendislik Fakültesi, İnşaat Mühendisliği Bölümü, İstanbul, Türkiye, ORCID: 0000-0002-8037-7603,
e-posta: mehmetugural@gmail.com

**** Doç. Dr., Milli Savunma Üniversitesi, Kara Astsubay Meslek Yüksekokulu, İşletme Yönetimi Bölümü, Balıkesir, Türkiye, ORCID: 0000-0001-9348-6107,
e-posta: augurlukara@gmail.com

Geliş Tarihi / Submitted:
11.12.2023

Kabul Tarihi / Accepted:
05.03.2024

Öz

Değişen koşullar kaçınılmaz olarak askerî yapıları ve sistemleri etkilemektedir. Tarih boyunca askerî yapılar doktrinel, organizasyonel, stratejik ve teknolojik gelişmeler nedeniyle sürekli olarak değişikliklere uğramıştır. Bu araştırmanın amacı, orduların dijital dönüşüm sürecinde yaşadıkları sorunların tespiti ve bu sorunlara yönelik olası çözüm önerilerini tartışmaktır. Araştırma yöntemi olarak sistematik literatür taraması ile uzman görüşmesine başvurularak hibrit bir yöntem kullanılmıştır. Araştırmanın özgün değeri, orduların dijital dönüşüm sürecinde karşılaştığı pratik ve güncel sorunları ele alması ve bu sorunlara somut, gerçekçi ve uygulanabilir çözüm önerileri sunmasıdır. Araştırmanın sonucunda eski sistemlerin yeni teknolojilere uyum sağlamada sorun yaşadığı, dijital dönüşümün siber güvenlik açıkları oluşturduğu, veri yönetiminde altyapı eksikliği görüldüğü, eğitim ve öğretim alanlarında 10 yıl ve üzeri personelin değişime karşı direnç gösterebileceği tespit edilmiştir. Bu bulguların, silahlı kuvvetlerdeki uygulayıcılara ve karar vericilere, dijital dönüşüm süreci içerisinde teknolojilerdeki değişimler yoluyla orduların örgütsel yapılarındaki dönüşümler, personel istihdamı, yeni beceri ve kapasite gereksinimleri, askerî eğitim sistemleri ve karar alma süreçleri gibi durumlarda öngörülerde bulunmalarına yardımcı olacağı değerlendirilmektedir.

Anahtar Kelimeler: Ordu, Dijitalleşme, Dijital Dönüşüm, Savunma Sanayi, Teknoloji

Abstract

Changing conditions inevitably affect military structures and systems. Throughout history, military structures have constantly undergone changes due to doctrinal, organizational, strategic, and technological developments. This research aims to identify the problems experienced by armies in the digital transformation process and to discuss possible solutions to these problems. As a research method, a hybrid method has been used by applying systematic literature review and expert interviews. The unique value of this research is that it addresses practical and current problems faced by armies in the digital transformation process and offers concrete, realistic, and applicable solutions to these problems. This study has reached the conclusions that old systems had problems adapting to new technologies, digital transformation created cyber security vulnerabilities, there was a lack of infrastructure in data management, and personnel having ten years or more in education and training fields may be resistant to change. These findings will help practitioners and decision-makers in the armed forces to make predictions in situations such as transformations in the organizational structures of armies through changes in technologies during the digital transformation process, personnel employment, new skill and capacity requirements, military training systems, and decision-making processes.

Keywords: Army, Digitalization, Digital Transformation, Defence Industry, Technology

Extended Summary

The digital transformation of armies entails using novel technology and procedures to bolster military operations, heighten efficiency, and boost decision-making. Military companies must undergo digital transformation to adjust to changing threats, enhance operational capabilities, and sustain a competitive edge in an increasingly intricate and technology-oriented global landscape. The convergence of developing technology also amplifies current military capabilities, resulting in unforeseeable ramifications for conflict and strategic equilibrium. The significance of digital transformation in contemporary warfare grows due to the rapid advancement of technology and the evolving dynamics of battles. Military forces can gather, manipulate, and evaluate vast quantities of data from diverse sources such as sensors, satellites, and unmanned aerial vehicles, thanks to digital technology.

The objective of this research is to ascertain the challenges encountered by military forces throughout the process of digital transformation and to provide potential remedies for these issues. The digitalization process of military forces differs significantly from that of civilian institutions and enterprises. Military organizations, which have historically isolated themselves from external influences for security reasons, encounter several challenges from their staff as they undergo the process of digital transformation. The direct expression and disclosure of concerns within these closed systems is not feasible. This study provides distinct value by specifically targeting the practical and contemporary challenges encountered by military forces along their digital transformation journey. It gives tangible, pragmatic, and implementable resolutions to these issues.

A hybrid research strategy has been employed by combining systematic literature review and expert opinions. The literature review has involved a meticulous selection of studies from the Scopus and Web of Science indexes. Additionally, Google Scholar was consulted to ensure that no relevant studies were inadvertently excluded.. A literature review is a methodical process of gathering, examining, and integrating current research, scientific papers, publications, and other pertinent sources to meet the research question and objectives of the study. Research on militaries may give rise to ethical and security concerns. The literature review facilitates the resolution of such issues since it does not need direct human interaction. This strategy also offers benefits in terms of safeguarding the security and confidentiality of sensitive data. This study also utilized the perspectives of ten military professionals from six different countries who actively serve in NATO to uncover the challenges encountered by army troops during the process of digital transformation. As part of the research, these military experts were notified that the interview had been conducted and emphasized the importance of secrecy and voluntary participation. They were also advised that they might choose not to participate by simply indicating their preference. The findings of the literature research were disseminated to military professionals of varying ages and diverse professional backgrounds via an informational memorandum.

The process of digitizing armies enables armed forces to evolve into a more agile, adaptable, and knowledge-driven framework. Nevertheless, it is crucial to efficiently handle this conversion and exert endeavours to surmount the challenges. Through the implementation of strategic planning, technology investments, and people training, armies may enhance their ability to meet future military demands and effectively accomplish their security objectives by embracing digital transformation. Based on the analysis of literature and assessments by military specialists, it has been concluded that outdated systems face difficulties in adjusting to emerging technologies. The process of digital transformation gives rise to vulnerabilities in cyber security. Additionally, there is a deficiency in data management infrastructure.

Furthermore, personnel who have been in education and training for ten or more years may resist changes. The process of substituting outdated systems with modern technology necessitates meticulous strategizing and synchronization across all divisions and individuals with an interest in a sizable corporation.. It is crucial to systematically discontinue outdated systems and substitute them with modern technology in this scenario. Simultaneously, it is also important to offer training and assistance to personnel to help them accept and adjust to this transformation. While digitization enhances the operational capabilities of militaries, it concurrently amplifies the vulnerabilities of cyber security. Military institutions can become susceptible when they are specifically targeted by hackers and cyber-attacks. Robust cyber security protocols should be implemented to mitigate these dangers. These precautions should encompass encryption, firewalls, intrusion detection systems, and periodic training sessions. Regular testing by cyber security professionals is essential for ensuring the security of advanced devices. The abundance of data and diverse data sets can pose challenges for military organizations to make informed decisions and achieve operational effectiveness. Utilizing data analytics tools and methodologies, this data may be enhanced to derive more significance and optimize operational efficiency. Regularly updated techniques and standards should assist the data management process. Organizations often encounter resistance to changes, and this issue is also prevalent in military forces. The implementation of new technologies should be accompanied by supporting strategies to facilitate the troops' adjustment to the changes. Specialized training, effective communication, and active involvement can aid in diminishing resistance among soldiers. To achieve digital transformation, it is necessary to enhance troops' proficiency in digital skills and ensure efficient utilization of emerging technology. Armies must provide soldiers with specialized training and comprehensive digital literacy programs. The training procedure should facilitate troops' comprehension of the intricacies inherent in the evolving digital environment.

Giriş

Dijital teknolojilerin yüksek hızlı değişimi ve gelişimiyle öne çıkan, sıklıkla dijital çağ olarak adlandırılan yeni iş dünyası, kuruluşları kurumsal üretkenliği ve müşteri ihtiyaçlarının memnuniyetini daha iyi artırabilecek yeni ürün ve hizmetler geliştirmeye zorlamaktadır. Bu bağlamda dijital inovasyon, doğru şekilde kodlanıp kullanıldığında şirketler için değerli öngörüler üretebilecek, kararları yönlendirebilecek ve üretilen çıktıları pazar talebine göre hizalayabilecek yüksek miktarda veri ve bilginin üretilmesine katkıda bulunmaktadır. Bu nedenle, dijital teknolojiler ve çözümler, kuruluşların rekabet edebilirliği için giderek daha önemli bir etken olarak kabul edilmektedir.[1] Yeni iş ortamını birçok farklı güç ve eğilim şekillendirmekte ve hızla gelişen dijital teknolojiler, çığır açıcı ve yıkıcı yenilikleri beraberinde getirmektedir. Kuruluşların hayatta kalabilmesi ve başarılı olabilmesi için, iş ortamının evrimine yanıt verecek şekilde işletmeleri ve davranışları dönüştürmeleri, zorlukları gelişim ve büyüme fırsatlarına dönüştürmeleri gerekmektedir.[2] Aslında, bir kuruluşun teknolojik devrimi, kurumsal sermaye, insan kaynakları, yönetim uygulamaları, ürün geliştirme, operasyonlar, süreç mühendisliği ve yönetim kararları dâhil olmak üzere bir dizi ilişki kuruluşun tüm boyutlarını etkiler. Dijital dönüşüm, değer yaratmanın kurumsal yeteneklerini zenginleştirmek ve geliştirmek için teknoloji edinmek ve dijital bilgiyi

1 Tom Goodwin. *Digital Darwinism: Survival of the Fittest in the Age of Business Disruption*, Kogan Page Publishers, London, 2018, s. 48.

2 Ikujiro Nonaka ve Hirotaka Takeuchi, *The Wise Company: How Companies Create Continuous Innovation*, Oxford University Press, Oxford, 2019, s. 11.

özümsemekle ilgilidir. Bu nedenle başarılı dijital dönüşüm girişimlerini analiz etmek, kişilerin ve kuruluşların yetkinliklerini dikkate almak açısından önemlidir. Özellikle kurumsal ve bireysel davranışı etkileyen üst düzey yönetim yeterlilikleri konuyla ilgilidir. Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler süreçlerin dijitalleşmesini zorunlu kılmış ve kaçınılmaz bir süreç olarak dijital dönüşüm hayatımızın her alanında kendisini göstermiştir.

Bir askeri organizasyonun teknolojik yönü, ordunun mevcut silah sistemleriyle ve zafer kazanma kabiliyeti ile ilgilidir.[3] Barış zamanında, yeni teknolojiler geliştirme, bütünleştirme ve kullanma yeteneği, bir devletin rakiplerinin önünde kalabilmesinin veya daha güçlü rakiplerle aradaki farkı kapatabilmesinin başlıca yollarından biridir.[4] Ancak, askeri organizasyonların teknoloji ve bilgi kullanımı, organizasyonun dijital olgunluk seviyesindeki farklılıklar nedeniyle optimal değildir. Örneğin ABD ordusu, kara araçları, sensörler, iletişim cihazları ve silah sistemlerinden oluşan entegre bir sistem olan FCS (*Future Combat Systems*)'ye geçmekte çeşitli zorluklar ile karşılaşmıştır. Teknolojik geliştirme ve donanım edinimi açısından ilerleme kaydedilirken, FCS konseptinin tam entegrasyonu ve operasyonel kullanımı zorluklarla karşılaşmıştır. Birçok asker ve komutan, büyük ölçüde veriye dayalı karar verme ve karmaşık ağ etkileşimlerine dayanan yeni savaş yürütme yöntemine uyum sağlamakta zorlanmıştır.[5]

Konunun önemi göz önünde bulundurularak bu çalışmada, orduların dijital dönüşüm sürecinde yaşadıkları sorunların tespiti ve sorunlara yönelik olası çözüm önerileri oluşturmak amaçlanmıştır. Orduların dijital dönüşüm süreci diğer sivil kurum/kuruluş ve işletmelere benzememektedir. Yıllarca süren gelenek yapısıyla güvenlik kaygılarıyla kendini dış dünyaya birçok noktadan kapatmış ordular dijital dönüşüm sürecinde personeli ile birçok sorun yaşamaktadır.[6] Sorunların da bu kapalı sistemlerde direkt ifade edilmesi ve ortaya konması pek mümkün olmamaktadır. Araştırmanın özgün değeri, orduların dijital dönüşüm sürecinde karşılaştığı pratik ve güncel sorunları ele alması ve bu sorunlara somut, gerçekçi ve uygulanabilir çözüm önerileri sunmasıdır.

1. Dijital Dönüşüm

Dijital dönüşüm günümüzün iş zorunluluğudur[7] ve yeni teknolojiler tarafından yönlendirilen, organizasyonların etkinliğini arttıran, iş yapım süreçlerini iyileştiren dönüşüm türüdür.[8] Dijital dönüşüm, şirketleri ve endüstrileri hayatta kalmak ve gelişmeleri için organizasyonel değişikliklere ve kritik iş uyarlamaları yapmaya zorlar.[9] Rekabetin giderek arttığı küreselleşen dünyada avantajları geliştirmek ve sürdürmek veya yeni müşteriler ve şirketin paydaşları için sürdürülebilir değer yaratmak için teknolojik değişikliklerle hakim olmak gibi kuruluşların

3 Aditya B. Gunawan, Under the Shadow of Army Domination: Defense Transformation in Indonesia, *Yüksek Lisans Tezi,* Heidelberg University, Heidelberg, 2022, s. 16.

4 Evan B. Montgomery, "Signals of Strength: Capability Demonstrations and Perceptions of Military Power", *Journal of Strategic Studies*, 43:2, 2020, s. 309.

5 Christopher G. Pernin vd., "Lessons from the Army's Future Combat Systems Program" Rand Report, 2012, https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1206.sum.pdf, erişim 23.11.2023.

6 Per Martin Norheim-Martinsen "New Sources of Military Change–armed Forces as Normal Organizations", *Defence Studies,* 16:3, 2016, s. 312.

7 Anshu Bhardwaj, "5G For Military Communications", *Procedia Computer Science*, 171, 2020, s. 2671; Giovanni Schiuma, "Managing Knowledge For Business Performance İmprovement", *Journal of Knowledge Management,* 16:4, 2012, s. 516.

8 David Tang, "What Is Digital Transformation?", *EDPACS*, 64:1, 2021, s. 11.

9 Saeed Albukhitan, "Developing Digital Transformation Strategy For Manufacturing", *Procedia computer science*, 170, 2020, s. 664; Jose A., Porfirio vd. "Leadership Characteristics and Digital Transformation", *Journal of Business Research,* 124, 2021, s. 610.

dijital dönüşümü benimsemesinin birçok nedeni vardır.[10] Dijital dönüşümün hedefi, pazardaki gelişmeleri hızlı bir şekilde algılayabilen ve yanıtlayabilen bir kurum olarak sürekli optimizasyondur. [11]

Dönüşüm sürecinin başarılı olarak değerlendirilmesi için kurumların, dijital teknolojiyi genel stratejileriyle uyumlu hale getirmesi gereklidir. [12] Dijital dönüşüm süreci, dinamik yetenekler teorisine dayanmaktadır.[13] Dinamik yetenekler, bir firmanın hızla değişen ortamlara hitap etmek için iç ve dış yetkinlikleri entegre etme, oluşturma ve yeniden yapılandırma becerisini ifade eder.[14] Bu yetenekleri geliştirebilen ve uygulayabilen kuruluşların, dijital dönüşümün karmaşıklıklarında başarılı bir şekilde hareket edebilme ve dijital çağda sürdürülebilir rekabet avantajı elde etme olasılığı daha yüksektir.[15]

Dijital dönüşüm net bir strateji, güçlü liderlik, sürekli öğrenme ve deneme gerektirir. Dijital dönüşüm, çalışanlarının belirsiz ortamda yaratıcı ve yenilikçi yollarla yanıt vermek için sahip olduğu doğru beceriler tarafından yönlendirilen, kırılganlığın yerini esnekliğin aldığı bütünsel bir sürekli değişim sürecidir.[16] Dijital dönüşümü başarmak için, iş yapma biçimini değiştirmek amacıyla dijital varlıkları diğer kurumsal kaynaklarla yeniden birleştirmeye ihtiyaç vardır.[17] Ayrıca kuruluşların bu dinamik yetenekleri kazanabilmesi, sistem ve süreçlerin akıllandırılması ve dijitalleşme vizyonu çerçevesinde Endüstri 4.0'ı yakından takip etmesi ve aşağıda Şekil-1'de gösterilen bir dizi yenilikçi teknolojilerin süreçlere dâhil edilmesi rekabet avantajını kazanabilmesini de kolaylaşacaktır.

Şekil 1. Endüstri 4.0 Teknolojileri [18]

10 Karolin Frankenberger vd., *The Digital Transformer's Dilemma: How To Energize Your Core Business While Building Disruptive Products And Services*, John Wiley & Sons, New Jersey, 2020, s. 31.

11 Murat Sağbaş ve Fahri Alp Erdoğan, "Digital Leadership: A Systematic Conceptual Literature Review", *İstanbul Kent Üniversitesi İnsan ve Toplum Bilimleri Dergisi*, 3:1, 2021, s. 17.

12 Daniel Ellström vd., "Dynamic Capabilities For Digital Transformation", *Journal of Strategy and Management*, 15:2, 2021, s. 272.

13 Jens Konopik vd.,"Mastering The Digital Transformation Through Organizational Capabilities: A Conceptual Framework", *Digital Business*, 2:2, 2022, s. 2.

14 David Teece, Gary Pisano ve Amy Shuen, "Dynamic Capabilities and Strategic Management", *Strategic Management Journal*, 18:7, 1997, s. 509 .

15 Karl S. Warner ve Maximilian Wäger, "Building Dynamic Capabilities For Digital Transformation: An Ongoing Process Of Strategic Renewal", *Long Range Planning*, 52:3, 2019, s. 326 .

16 Gordon Fletcher ve Marie Griffiths, "Digital Transformation During A Lockdown", *International Journal of Information Management*, 55:5, 2020, s. 6.

17 Peter Verhoef vd., "Digital Transformation: A Multidisciplinary Reflection and Research Agenda", *Journal of Business Research*, 122, 2021, s. 889

18 Aslı Duman, "Savunma Sanayiinin Dijitalleşmesi ve Modernleşmesi", Arzu Uğurlu Kara ve Kubilay Baş (ed.), *Savunma Yönetimi: Disiplinlerarası Bir Yaklaşım*, Nobel Yayınevi, Ankara, 2023, s. 281.

2. Orduların Dijital Dönüşümü

Silahlı kuvvetlerin teknolojik gelişmeleri yakından takip etmesi ve bu gelişmelerin gelecekteki yetenek ve tehditleri nasıl etkileyebileceğini değerlendirmesi gerekmektedir.[19] Orduların dijital dönüşümü, askeri operasyonları geliştirmek, verimliliği artırmak ve karar vermeyi iyileştirmek için yeni teknolojilerden ve süreçlerden yararlanmayı içerir. Dijital dönüşüm, askeri kuruluşların gelişen tehditlere uyum sağlaması, operasyonel yeteneklerini geliştirmesi ve giderek daha karmaşık ve teknoloji odaklı bir dünyada rekabet avantajını koruması için gereklidir. Örneğin ileri teknoloji olarak değerlendirilen İHA'ların Rusya- Ukrayna Savaşı'nda kilit bir rol oynadığı görülmektedir.[20] Gelişmekte olan teknolojiler arasındaki etkileşimler, savaş ve stratejik istikrar için öngörülemeyen sonuçlarla birlikte mevcut askeri yetenekleri de geliştirir. Bütün bu faydalarına rağmen ordular, kurumsal kültürleri gereğince değişime direnen muhafazakâr ve riskten kaçınan örgütlerdir. [21] Ordular, büyük teknolojik değişim içeren yeni platformları hızla elde etmede başarılı olabilir, ancak bu yenilikleri benimsemede zorlanır. [22]

Ordulardaki dijital dönüşüm, bilginin senkronize paylaşımını sağlayarak toplu komuta etme imkânını arttırırken[23], karar vermeyi geliştirir ve belirsizliği de azaltır.[24] Bulut bilgi işlem, büyük veri ve yapay zekâ gibi teknolojik avantajları askeri tedarikin yaşam döngüsüne dahil edebilir, teknolojik ilerleme sağlayarak kurumsal optimizasyonu teşvik edebilir. Durumsal farkındalığı arttırmak veya durumsal farkındalığa erişmek için ordular dijital dönüşüme ihtiyaç duyar. Dijital teknoloji ordunun çevikliğini, kalitesini ve verimliliğini arttırır. Askeri teknoloji geliştirmenin amacı, askerin etkinliğini artırmaktır.[25] Orduların dijital dönüşümü, askeri operasyonları geliştirmek, verimliliği artırmak ve karar vermeyi iyileştirmek için yeni teknolojilerden ve süreçlerden yararlanmayı içerir. Gelişmekte olan teknolojiler arasındaki etkileşimler, savaş ve stratejik istikrar için öngörülemeyen sonuçlarla birlikte mevcut askeri yetenekleri de geliştirir veya yeni yetenekler sağlar.[26]

Hızla gelişen teknoloji ve çatışmaların değişen doğası nedeniyle modern savaşta dijital dönüşüm giderek daha önemli hale gelmektedir. Dijital teknoloji, orduların sensörler, uydular ve insansız hava araçları dâhil olmak üzere çeşitli kaynaklardan büyük miktarda veri toplamasına, işlemesine ve analiz etmesine olanak tanır. Bu, orduların savaş alanının daha eksiksiz bir resmine sahip olmasını sağlar, bu da durumsal farkındalığı artırabilir ve karar verme sürecini bilgilendirebilir.[27] Dijital teknoloji, uzun mesafelerde bile askerler ve birimler arasında gerçek zamanlı iletişim ve koordinasyon sağlar. Bu yanıt sürelerini iyileştirebilir

19 Stefan Silfverskiöld, Kent Andersson ve Martin Lundmark. "Does The Method For Military Utility Assessment of Future Technologies Provide Utility?", *Technology in Society*, 67, 2021, s. 6.

20 Dominika Kunertova, "The Ukraine Drone Effect on European Militaries", *CSS Policy Perspectives*, 10:15, 2022, s. 1.

21 Alex Neads, Theo Farrell ve David J.Galbreath, "Evolving Towards Military Innovation: AI And The Australian Army", *Journal of Strategic Studie*s, s. 1.

22 Andrew Hill, "Military İnnovation And Military Culture", *The US Army War College Quarterly: Parameters*, 45:1, 2015, s. 85.

23 Therese Heltberg, ""I Cannot Feel Your Print", How Military Strategic Knowledge Managers Respond To Digitalization", *Journal of Strategy and Management*, 15:2, 2022, s. 220.

24 Mylène Struijk vd., "Navigating Digital Transformation Through An Information Quality Strategy: Evidence From A Military Organisation", *Information Systems Journal*, 33:4, 2023, s. 912.

25 Daniel Billing vd. "The Implications Of Emerging Technology On Military Human Performance Research Priorities", *Journal of Science and Medicine in Sport*, 24:10, 2021, s. 947.

26 Kelley M. Sayler, "Emerging Military Technologies: Background and Issues For Congress". *CRS Report*, October 2021, https://apps.dtic.mil/sti/pdfs/AD1151925.pdf, erişim 23.11.2023, s. 6.

27 Mauro Tortonesi. Leveraging Internet Of Things Within The Military Network Environment—Challenges And Solutions. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 2016, s. 111.

ve operasyonların daha etkili koordinasyonunu kolaylaştırabilir.[28] Dijital teknoloji, orduların hassas saldırıları daha yüksek doğrulukla gerçekleştirmesini sağlayarak ikincil hasarı ve sivil kayıpları azaltır. Bu geleneksel savaş yöntemlerinin daha az etkili olabileceği kentsel ortamlarda özellikle önemlidir.[29] Dijital teknoloji, lojistik ve tedarik zinciri yönetimini iyileştirerek orduların personeli, ekipmanı ve malzemeleri daha verimli bir şekilde taşımasını sağlayabilir. Bu maliyetleri düşürmeye ve askerlerin görevlerini yerine getirmek için ihtiyaç duydukları kaynaklara sahip olmalarını sağlamaya yardımcı olabilir. [30]

Dijital teknoloji, gerçekçi eğitim simülasyonları oluşturmak için kullanılabilir ve askerlerin güvenli ve kontrollü bir ortamda tatbikat yapmasına olanak tanır. Bu, becerilerini ve gerçek dünya operasyonlarına hazır olma durumlarını geliştirmeye yardımcı olabilir. Dijital dönüşüm modern savaşta önemlidir. Çünkü orduların durumsal farkındalığı artırmasına, iletişim ve koordinasyonu geliştirmesine, süreçlerin gizlilikle yürütmesine, lojistik ve tedarik zinciri yönetimini geliştirmesine ve eğitim ve simülasyonu iyileştirmesine olanak tanır. Teknoloji gelişmeye devam ettikçe, orduların savaş alanındaki etkinliklerini sürdürmeleri için dijital dönüşümün daha da kritik hale gelmesi muhtemeldir. [31] Deloitte tarafından yayınlanan "Havacılık ve Savunma 4.0 (*Aerospace and Defense 4.0*)" başlıklı raporda savunma sanayi firmalarının dijital teknolojilerden, çeviklik kazanma, yeni iş modelleri geliştirme, etkin bir tedarik zinciri yönetimi sağlama ve verileri siber saldırılardan koruma amacıyla faydalandıkları ve dijital dönüşümün pazarda farklılaşmanın anahtarı olarak görüldüğü ifade edilmiştir. [32] Bu kapsamda savunma sanayi firmalarının dönüşüm trendini yakalama, son moda teknolojiler ile adaptasyonu sağlanmış süreçler inşa etme, üretilen ürünlerin yeteneklerini artırma ve rakiplerden bir adım önde olma hedefi bu alana yapılan yatırımları etkileyecektir. Savunma sanayinin teknolojik gücü orduların dijital dönüşüm sürecini derinden etkileyecek ve yönlendirecektir. Savunma sanayinde yapay zekâ ve makine öğrenimi, büyük veri analizi, Nesnelerin İnterneti, bulut bilişim, sanal ve artırılmış gerçeklik, otomasyon ve robotik sistemler, Blockchain ve siber güvenlik teknolojileri sıkça kullanılmaktadır. Bahsedilen teknolojilerin kullanılmasıyla askeri istihbarat, planlama, üretim, lojistik ve operasyonel karar verme süreçlerinin etkinliği artmaktadır. Savunma sanayi sektörünün güncel teknolojiler ile donatılması ülkelerin farklı üretim kollarına da etki ederek, sosyal ve teknolojik refaha da katkı sağlamaktadır. [33] **Aşağıda Şekil 2.**'de Endüstri 4.0 teknolojilerinin savunma sanayi sektöründeki kullanımı ile ilgili bilgilendirme yapılmıştır.

28 Denise E. Zheng, and William A. Carter. Leveraging The Internet Of Things For A More Efficient And Effective Military. Rowman & Littlefield, Lanham, 2015, s. 5.

29 Mohamed Emimi, Mohamed Khaleel ve Abobakr Alkrash, "The Current Opportunities And Challenges in Drone Technology", International Journal of Electrical Engineering and Sustainability (IJEES), 3:1, 2023, s. 74.

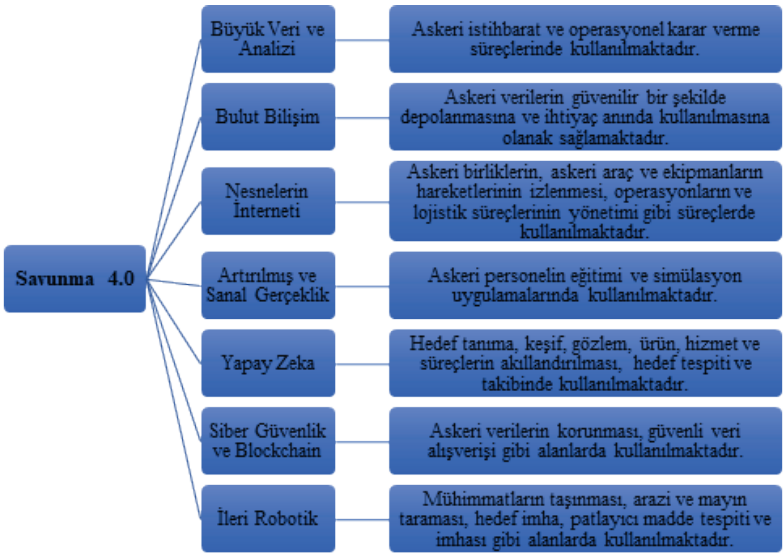
30 Denise E. Zheng ve William A. Carter, Leveraging The Internet Of Things For A More Efficient And Effective Military. Rowman & Littlefield, Lanham, 2015, s. 5.

31 Stefan Silfverskiöld, Kent Andersson ve Martin Lundmark. "Does The Method For Military Utility Assessment Of Future Technologies Provide Utility?", Technology in Society, 67, 2021, s. 4.

32 Deloitte. "Aerospace and Defense 4.0, Capturing the Value of Industry 4.0 Technologies" https://www2.deloitte.com/content/dam/insights/us/articles/4912_Aerospace-and-defense-4-0/DI_A&D_4-0.pdf, erişim 28.11.2023, s. 2.

33 Aslı Duman, "Savunma Sanayiinin Dijitalleşmesi ve Modernleşmesi", Arzu Uğurlu Kara ve Kubilay Baş (ed.), Savunma Yönetimi: Disiplinlerarası Bir Yaklaşım, Nobel Yayınevi, Ankara, 2023, s. 281.

Şekil 2. Endüstri 4.0 Teknolojilerinin Savunma Sanayinde Kullanımı[34]



Orduların dijital dönüşüm süreci operasyonel verimliliği artırırken uzun dönemli savunma maliyetlerini düşürmektedir. Karar verme süreçlerinde kullanılan büyük miktardaki veriler stratejik kararların alınmasına katkı sağlamaktadır.[35] Büyük veri işlenerek, potansiyel sorunlar, saldırı tehditleri ve düşman hareketleri tespit edilebilmekte ve savunma taktikleri geliştirilmektedir. Büyük verinin depolanması noktasında bulut bilişim teknolojilerinden faydalanılmaktadır. Cihazlardan, ağlardan, operasyonel süreçlerden elde edilen verilerin depolanması ve paylaşılması konusunda bu teknoloji önemli bir çözüm aracı olarak karşımıza çıkmaktadır. Nesnelerin İnterneti veri kaynağı, büyük veri toplanan veriden anlamlı sonuçların çıkartılacağı analitik veri platformu ve bulut bilişim tüm bu verilerin saklandığı depolama alanıdır.[36] Askeri operasyonlar ve süreçler ile Nesnelerin İnterneti teknolojisinin entegrasyonu Askeri Nesnelerin İnterneti (*The Internet of Military Things*) kavramı ile açıklanmaktadır. Askeri Nesnelerin İnterneti ile silahlı kuvvetler sorunlu bölgeyi sensörler ile donatılmış kameralar, insansız hava araçları ve dronlar yardımıyla inceleyebilir ve komuta merkezine gerçek zamanlı veri gönderebilir.

NATO tarafından önümüzdeki 20 yıl boyunca savunma sanayinin, akıllı, bağlantılı, dağıtılmış ve dijital özelliklere sahip olacağı özellikler NATO'nun 'Bilim ve Teknoloji Trendleri 2020-2040' başlıklı raporda şu şekilde gösterilmiştir. [37]

34 Age, s. 286.
35 Age, s. 286.
36 Age, s. 286.
37 NATO, "Science & Technology Trends 2020-2040". https://tto.iste.edu.tr/content/files/tto-8faf19a901-73c24.pdf, NATO Report, 2020, erişim 25.11.2023, s. 4.

Tablo 1. Savunma Sanayinin Sahip Olacağı Özellikler[38]

Özellikler	Kullanılan Teknolojiler	Kazanımlar
	Özerklik (Otomasyon)	
Akıllı	**İnsancıl Zekâ (**Yapay zekâ-insan işbirliğini ifade etmektedir)	Yapay zekâ, bilgi odaklı analitik yetenekler ve dijital tabanlı teknolojilerin desteği ile akıllandırılmış ürün ve hizmetlerin savunma sanayisinde kullanımı.
	Bilgi Analitiği	
Bağlantılı	Güvenilir İletişim	Blockchain, kuantum anahtar dağıtımı gibi güvenilir iletişim sunan teknolojilerin kullanılması ve sensörler, siber-fiziksel sistemler, akıllı ağlar ve otonom araçların desteği ile bağlantılı yeni ekosistemlerin oluşturulması.
	Sinerjik Sistemler (Fiziksel ve sanal ekosistemleri içeren karma sistemleri ifade etmektedir)	
Dağıtılmış	Sınır Bilişim (*Edge Computing*)	Nesnelerin İnterneti teknolojisi ve sensörlerin desteği ile merkezi olmayan bir yapı içerisinde, büyük ölçekli depolama, hesaplama, karar verme, araştırma ve geliştirme yeteneklerinin kazanımı.
	Her Yerde Algılama (*Ubiquitous Sensing*)	
	Merkezi Olmayan Üretim	3 Boyutlu ve 4 Boyutlu yazıcıların desteği ile tam zamanlı üretimin gerçekleştirilebilmesi.
Dijital	Dijital İkiz	Dijital ikiz ve yapay gerçeklik teknolojilerinin desteği ile fiziki ve bilişsel gerçekliklerin harmanlanması.
	Dijital Gerçeklik	

Savunma sanayinde kullanılan dönüşüm teknolojilerinin sağladığı faydalar ile birlikte devasa ağların güvenliğinin sağlaması konusu da gündeme gelmektedir.[39] Sanal ortamda tutulan verilerin güvenilir bir şekilde saklanması noktasında siber güvenlik teknolojileri kullanılmaktadır. Bilgi ve iletişim teknolojilerindeki gelişmeler doğrultusunda bilgilerin, belgelerin, dokümanların kısaca bilginin dijitalde saklanması, artan bağlantı sayısı, akıllı ağların her alanda kullanılması ve buradan elde edilen verinin dijitalde saklanması nedeniyle siber güvenlik günümüzün en önemli kavramları arasında yer almaktadır. Siber alanda izinsiz ve kötü niyetle gerçekleştirilen her türlü eylem bir siber saldırıdır ve bu saldırıların, ekonomi, politika ve toplumsal değerler üzerinde yıkıcı etkileri olabilmektedir.[40] Dünya Ekonomik Forumu tarafından hazırlanan Küresel Riskler raporunda teknolojik risk kategorisinde yer alan siber suçlar ve siber güvensizlik hem hükümetleri hem de iş dünyasını etkileyecek riskler arasında ilk onda yer almaktadır.[41] Günümüzde siber saldırılar, daha sık, karmaşık ve yıkıcı hale gelmiştir ve bu saldırıların maliyetleri sürekli artmaktadır. Tek bir siber saldırı ülke demokrasisine, askeri yeteneklere ve ülkeler için kritik düzeyde önem teşkil eden enerji ve güvenlik kurumlarına zarar verebilmektedir.[42]

38 Age, s. 4.

39 Serhat Burmaoğlu, Ozcan Sarıtaş ve Haydar Yalçın "Defense 4.0: The Internet of Things in Military", Dirk Meissner, Leonid Gokhberg & Ozcan Saritas (ed.), Emerging Technologies for Economic Development, Springer Nature Switzerland, 2019, s. 303.

40 Aslı Duman, "Savunma Sanayiinin Dijitalleşmesi ve Modernleşmesi", Arzu Uğurlu Kara & Kubilay Baş (ed.), Savunma Yönetimi: Disiplinlerarası Bir Yaklaşım, Nobel Yayınevi, Ankara, 2023 , s. 281.

41 World Economic Forum, "The Global Risks Report 2023". https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf, erişim 23.11.2023, s. 4.

42 NATO News, "NATO Will Defend Itself" https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en, erişim25.11.2023, s. 4.

3. Yöntem

3.1. Sistematik Literatür Taraması

Araştırma yöntemi olarak sistematik literatür taraması ile uzman görüşüne başvurularak hibrit bir yöntem kullanılmıştır. Literatür taramasında, çalışmaların Scopus ve Web of Science dizininde yer alacak şekilde seçilmesine özen gösterilmiş ve konuyla bağlantılı bazı çalışmaların gözden kaçmaması için Google Scholar'a bakılmış, görüşme yönteminde ise 6 farklı ülkeden 10 askeri uzman ile görüşülmüştür. Bulgular kısmında elde edilen bilgi ve veriler, karma metotla ortaya konulmuştur. NATO'da görev yapan 6 farklı ülke askeri uzmanının görüşlerine başvurulmuştur. Literatür taraması, araştırma sorusunu ve çalışmanın hedeflerini ele almak için mevcut araştırmaları, bilimsel makaleleri, yayınları ve diğer ilgili kaynakları toplamak, analiz etmek ve sentezlemek için sistematik bir yaklaşımdır. Ordularla ilgili araştırmalarda bazı etik ve güvenlik sorunları ortaya çıkabilir. Literatür taraması, insanlar üzerinde doğrudan bir müdahale gerektirmediği için bu tür sorunların üstesinden gelmeyi kolaylaştırır. Bu yöntem, duyarlı verilerin güvenliğini ve gizliliğini korumak açısından da avantajlıdır. Bu metodun kullanılması, farklı coğrafi bölgelerde ve farklı zaman dilimlerinde yapılmış çok sayıda araştırmayı içerir. [43] Böylelikle orduların dijital dönüşümü sürecindeki sorunları ve çözüm önerilerini daha geniş bir perspektiften incelenmesi sağlanmış olur. Ana araştırma soruları aşağıdaki şekilde belirlenmiştir:

- Orduların dijital dönüşüm girişimlerinde yaşadıkları temel zorluklar nelerdir?
- Eski sistemlerden yeni dijital sistemlere geçerken karşılaşılan sorunlar nelerdir?
- Orduya ait verilerin dijital ortamlara aktarılması siber güvenlik tehdidi oluşturur mu?

Literatür Tarama Stratejisi: Çalışmaların Scopus ve Web of Science dizininde yer alacak şekilde seçilmesine özen gösterilmiş ve konuyla bağlantılı bazı çalışmaların gözden kaçmaması için Google Scholar'a bakılmıştır. Arama öncelikle konuyla ilgili "ordular", "askeri", "dijital dönüşüm", "dijital", "siber güvenlik", "teknolojik dönüşüm" anahtar kelimelerin birbirleriyle kombinasyonu sonucu ilgili çalışmalar tespit edilmiştir. Arama işlemi sonucunda Scopus dizininde 52 çalışma tespit edilmiş, bunların 32'si makale, 18'i bildiri, 2 tanesi kitap bölümüdür. Konuya ilişkin Web of Science dizininde 48 çalışma tespit edilmiş, bunlardan 26 tanesinin makale, 22 tanesinin bildiri olduğu tespit edilmiştir. 4 çalışmanın her iki dizinde de bulunduğu belirlenmiştir. Gözden konuya ilişkin herhangi bir çalışmanın kaçmaması için anahtar kelimeler Google Scholar'a yazılmıştır. İlaveten NATO raporları incelenmiştir.

Ekleme ve hariç tutma ölçütleri: Seçilen literatürün alaka düzeyini ve güvenilirliğini sağlamak için özel dâhil etme ve hariç tutma kriterleri uygulanmıştır. Yalnızca hakemli makaleler, bilimsel makaleler, raporlar ve yetkili yayınlar dikkate alınmıştır. İngilizce olmayan makaleler, dil sınırlamaları nedeniyle hariç tutulmuştur. Değerlendirmeler neticesinde 10 çalışmanın konuyla ilişkin ayrıntılı bilgiler sunduğu belirlenmiştir. Tablo 2'de bu çalışmalara yer verilmiştir.

43 Edna Rother, "Systematic Literature Review X Narrative Review", Acta paulista de enfermagem, 20, 2007, s.1.

Tablo 2: Sorun Tespiti ve Çözümü için Değerlendirilen Çalışmalar

Yazar	Yılı	Türü	Dizin Türü	Tema
Bhardwaj	2020	Bildiri	Web of Science Scopus	Siber Güvenlik Riskleri
Billing vd.,	2021	Makale	Web of Science	Değişime Karşı Direnç
Heltberg	2020	Makale	Web of Science	Dijital Becerilerin Eksikliği Maliyet ve Bütçe Kısıtlamaları
Horowitz vd.,	2020	Makale	Web of Science	Mevzuata Uygunluk
Johnson	2019	Makale	Google Scholar	Siber Güvenlik Riskleri
Montgomery	2020	Makale	Web of Science	Değişime Karşı Direnç
NATO	2021	Rapor	Google Scholar	Dijital Becerilerin Eksikliği
Sayler	2020	Rapor	Google Scholar	Mevzuata Uygunluk
Silfverskiöld	2021	Makale	Web of Science Scopus	Dijital Becerilerin Eksikliği
Strujik	2023	Makale	Web of Science	Değişime Karşı Direnç
Ziyadin vd.,	2020	Bildiri	Google Scholar	Değişime Karşı Direnç

Veri Çıkarma ve Sentez: Literatür taramasından sonra tespit edilen makaleler kapsamlı bir şekilde incelenmiştir. Orduların dijital dönüşümde yaşadığı zorluklara ilişkin veriler her kaynak incelenmiştir. Elde edilen bilgiler temalara ve ortak zorluklara göre organize edilmiştir.

Sentez ve Yorum: Literatürden elde edilen bulgular, orduların dijital dönüşüm çabalarında karşılaştıkları zorluklara ilişkin tutarlı bir anlayış geliştirmek için sentezlenmiş ve yorumlanmıştır. Sentez, belirlenen zorluklara ilişkin açık ve bütüncül bir görüş sunmayı amaçlamıştır.

Tartışma: Sentezlenen bulgular, dijital dönüşüm, örgütsel değişim ve askeri çalışmalarla ilgili mevcut bilgi ve teoriler bağlamında tartışılmıştır. Tartışma, belirlenen zorlukların etkileri ve bunların askeri bağlamlarda dijital girişimlerin etkinliği ve başarısı üzerindeki potansiyel etkileri hakkında fikir vermiştir.

3.2. Görüşme

Bu araştırmada ordu çalışanlarının dijital dönüşüm sürecinde karşılaştıkları sorunların neler olduğunun ortaya konulabilmesi amacıyla NATO'da görev yapan 6 farklı ülke askeri uzmanının görüşlerinden faydalanılmıştır. Literatür, araştırmacılar tarafından tespit edildiği kadarıyla konuya ilişkin ayrıntılı bilgi verme noktasında kısıtlı kalmıştır. Bundan dolayı konuya ilişkin derinlemesine bilgiler edinmek, spesifik bağlamları, ince nüansları tespit etmek amacıyla görüşme yöntemi kullanılmıştır. Araştırma tasarımı olarak durum çalışması deseni kullanılmıştır. Askeri uzmanlara uygulama esnasında katılımcılar görüşmenin araştırma kapsamında yapıldığı, gizliliğin ve gönüllülüğün esas olduğu ve katılmak istemediklerinde belirtmelerinin yeterli olduğu konusunda bilgilendirilmiştir. Uzmanlar kolayda örnekleme yöntemi kullanılarak belirlenmiştir. Veri toplama süreci, uzmanlarla yüz yüze gerçekleştirilerek yapılmıştır. Verilerin analizi, temalandırma işlemi kullanılarak gerçekleştirilmiştir. Literatür taraması sonuçları bilgi notu ile farklı yaş ve mesleki tecrübelere sahip askeri uzmanlarla paylaşılmıştır. Tablo 3'te çalışmada yer alan uzmanların demografik bilgileri verilmiştir. Askeri uzmanlara aşağıdaki soru sorulmuştur:

- Dijital dönüşümün 21. Yüzyılın ikinci çeyreğinde hız kazanacağı değerlendirmektedir. Bu dönüşümde ordudaki en temel ve öncelikli çözülmesi gereken sorun nedir?
- Çözüm önerileriniz nelerdir?

Tablo 3: Askeri Uzmanların Demografik Bilgileri

Askeri Uzman	Kodu	Ülke	Cinsiyet	Yaş	Rütbe	Tecrübe
Askeri Uzman 1	AU1	Türkiye	Erkek	44	Albay	24
Askeri Uzman 2	AU2	Yunanistan	Erkek	38	Yüzbaşı	16
Askeri Uzman 3	AU3	Türkiye	Erkek	32	Üsteğmen	10
Askeri Uzman 4	AU4	ABD	Erkek	39	Yüzbaşı	17
Askeri Uzman 5	AU5	Arnavutluk	Erkek	41	Yüzbaşı	19
Askeri Uzman 6	AU6	Türkiye	Erkek	39	Yüzbaşı	18
Askeri Uzman 7	AU7	Yunanistan	Erkek	55	Binbaşı	32
Askeri Uzman 8	AU8	Bulgaristan	Erkek	37	Yüzbaşı	15
Askeri Uzman 9	AU9	Türkiye	Kadın	38	Yüzbaşı	16
Askeri Uzman 10	AU10	İtalya	Erkek	54	Albay	32

Bu araştırma soruları sistematik literatür taramasından elde edilen orduların dijital dönüşümünde yaşadığı sorunların, askeri uzmanların bildirebilecekleri sorunlardan farklı olup olmadığını belirlemek ve bu olası sorunlara çözüm önerileri getirmek için sorulmuştur.

4. Bulgular

4.1. Orduların Dijital Dönüşümünde Yaşadıkları Zorluklar

Literatür incelendiğinde siber güvenlik riskleri[44], eski sistemlerin modernizasyonu[45], değişime karşı direnç[46], dijital becerilerin eksikliği[47], maliyet ve bütçe kısıtlamaları[48] ve mevzuata uygunluk[49] dijital dönüşümde orduların yaşadığı sorun sahalarını oluşturmaktadır.

44 James Johnson, "The AI-Cyber Nexus: Implications For Military Escalation, Deterrence And Strategic Stability", Journal of Cyber Policy, 4:3, 2019, s. 442; Anshu Bhardwaj. "5G For Military Communications", Procedia computer science, 171, 2020, 2665-2674.

45 Stefan Silfverskiöld, Kent Andersson ve Martin Lundmark, "Does The Method For Military Utility Assessment Of Future Technologies Provide Utility?", Technology in Society, 67, 2021, s.4.

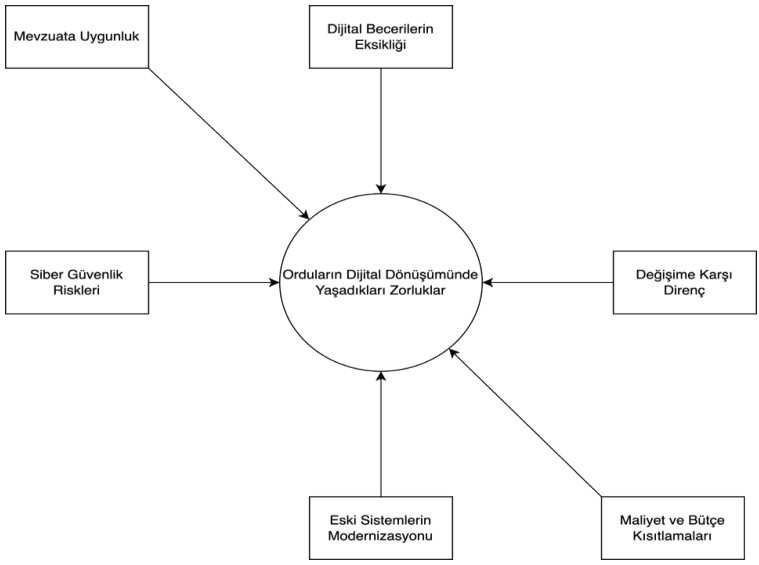
46 Evan B. Montgomery, "Signals Of Strength: Capability Demonstrations And Perceptions Of Military Power", Journal of Strategic Studies, 43:2, 2020, s. 309; Daniel Billing vd. "The Implications Of Emerging Technology On Military Human

47 Performance Research Priorities", Journal of Science and Medicine in Sport, 24:10, 2021, s. 947; Sayabek Ziyadin, Saltanat Suieubayeva And Aliya Utegenova (2020). Digital Transformation in Business. (eds.)Ashmarina Svetlana, Vochozka Marek, Mantulenko Valentina, Digital Age: Chances, Challenges and Future, Springer Cham, s. 408.

48 Therese Heltberg, ""I Cannot Feel Your Print". How Military Strategic Knowledge Managers Respond To Digitalization", Journal of Strategy and Management, 15:2, 2022, s. 220; Stefan Silfverskiöld, Kent Andersson and Martin Lundmark. "Does The Method For Military Utility Assessment Of Future Technologies Provide Utility?", Technology in Society, 67, s. 7; NATO, "Science &Technology Trends: 2020–2040", NATO Report, 2020, https://tto.iste.edu.tr/content/files/tto-8faf19a901-73c24.pdf, erişim 25.11.2023, s. 3.

49 Kelley M. Sayler, "Emerging Military Technologies: Background and Issues for Congress", CRS Report, October 2021, https://apps.dtic.mil/sti/pdfs/AD1151925.pdf, erişim 23.11.2023, s. 4; Micheal C. Horowitz, Lauren Kahn ve Casey Mahoney, "The Future Of Military Applications Of Artificial İntelligence: A Role For Confidence-Building Measures?", Orbis, 64:4, 2020, s. 528.

Şekil 3. Orduların Dijital Dönüşümünde Yaşadıkları Zorluklar (Literatür Taraması)



Siber güvenlik riskleri: Ordular, operasyonlarının ve verilerinin çoğunu çevrimiçi hale getirdikçe, siber saldırılara karşı daha savunmasız hale gelmektedir. Askeri kurumlar, kötü niyetli aktörler tarafından hedef alınabilecek önemli miktarda hassas bilgiye sahiptir. Dijital dönüşüm sırasında ağların ve verilerin güvenliğini sağlanmalıdır. Çekirdek altyapı için çok sayıda bağlı cihaz ve ağ sanallaştırma teknikleri kesinlikle potansiyel saldırı yüzeyini artıracaktır.[50] Yapay zekâ sistemleri, küçük, kasıtlı değişikliklerin hatalı önerilere veya yetersiz eylemlere yol açabileceği siber saldırılara karşı özellikle savunmasızdır.[51] Bu saldırılar kimlik bilgilerinin çalınmasına, verilerin tahrif edilmesine sebebiyet vermektedir.

Eski sistemlerin modernizasyonu: Yeni teknolojileri silah sistemlerine entegre etmek, bunları askeri birliklere uygulamak ve doktrini yeni teknolojilere göre uyarlamak genellikle on yılları alan bir süreçtir. [52] Birçok ordu, daha yeni dijital teknolojilerle kolayca entegre olamayacak olan eski teknoloji sistemlerine sahiptir. Bu, teknoloji altyapısını modernize etmeye çalışırken verimsizliklere ve ek maliyetlere neden olabilir.

Değişime karşı direnç: Gelişmekte olan teknolojilerin tüm savaş alanı rollerini ve görevlerini değiştirmesi beklenmektedir. Bunun sonucunda yeni görevler yaratılacak, eski görevler ortadan kaldırılacak veya en azından daha seyrek gerçekleştirilecek, böylelikle her düzeyde askerin performans gereksinimleri değişecektir.[53] Bazı askeri personel değişime karşı dirençli olabilir ve geleneksel iletişim ve operasyon yöntemlerini kullanmayı tercih edebilir. Askeri kuruluşlar, genellikle mevcut operasyon modlarıyla çatışan alternatif iş yapma yöntemlerini benimseme konusunda isteksizdir.[54] Bu, yeni dijital teknolojilerin ve

50 Anshu Bhardwaj, "5G For Military Communications", Procedia computer science, 171, 2020, s. 2665.
51 NATO, "Science &Technology Trends: 2020–2040", NATO Report, 2020, https://tto.iste.edu.tr/content/files/tto-8faf19a901-73c24.pdf, erişim 25.11.2023, s. 3.
52 Stefan Silfverskiöld, Kent Andersson ve Martin Lundmark, "Does The Method For Military Utility Assessment Of Future Technologies Provide Utility?", Technology in Society, 67, 2021, s. 13.
53 Daniel Billing vd., "The Implications Of Emerging Technology On Military Human Performance Research Priorities", Journal of Science and Medicine in Sport, 24:10, 2021, s. 947.
54 Evan B. Montgomery, "Signals Of Strength: Capability Demonstrations And Perceptions Of Military Power",

süreçlerin uygulanmasını zorlaştırabilir. Dijital dönüşümün başarı ile gerçekleştirilmesi için yöneticilerin vizyon ve teknolojilerin sistemle bütünleşmesine dayanma eksikliğinin olmaması gerekir. [55] Pek çok insan konfor bölgelerini etkilemesi sebebiyle dijital dönüşümün çalışma ortamlarındaki yaptığı değişikliklere direnmeyi tercih etmektedir.[56]

Dijital becerilerin eksikliği: Ordular, yeni teknolojinin tehditlerine karşı koymak için hangi askeri yeteneklere ihtiyaç duyulduğunu tespit etmeleri gerekmektedir.[57] Bazı askeri personel, yeni teknolojileri etkin bir şekilde kullanmak için gereken dijital becerilere sahip olmayabilir. Dijital becerileri geliştirmek için yeterli eğitim ve kaynak sağlamak, başarılı bir dijital dönüşüm için çok önemlidir.[58] İleri teknolojiler, askeri kuvvetlerin paylaşım, toplama, modelleme ve simülasyon, analiz, sınıflandırma, iyileştirme, iletişim ve veri yönetimi için yöntem ve standartların geliştirilmesi yeteneklerine sahip olmasını gerektirecektir.[59] Dijital yetkinlikleri olan uzmanlar, ordunun dijital dönüşüm projelerinde öncü rol almalı ve diğer personeli eğitmek için mentorluk yapılmalıdır.

Maliyet ve bütçe kısıtlamaları: Bir kurumu dijital dönüşüm yolculuğuna yönlendirmek için önemli bir yatırım gerekmektedir.[60] Dijital dönüşüm pahalı olabilir ve birçok ordunun yeni teknolojileri uygulamak için sınırlı bütçeleri olabilir. Dijital dönüşümün maliyetlerini diğer önceliklerle dengelemek zor olabilir.

Mevzuata uygunluk: Askeri kurumlar, veri koruma, gizlilik ve güvenlikle ilgili katı düzenlemelere ve politikalara uymalıdır. Mevcut teknolojilerin insan karar verme/bilişsel süreçlerini doğru bir şekilde kopyalayamamasından dolayı makinelerin karar vermesine izin verme ile ilgili önemli ahlaki, yasal ve etik zorluklar vardır. [61] Gelişmekte olan askeri teknolojiler bir dizi etik hususu gündeme getirebilir.[62] Dijital dönüşüm girişimlerinin bu düzenlemelere uymasını sağlamak karmaşık olabilir. Ordu için kullanılan yapay zekâ tarafından gerçekleşen kazanın gerçekten kasıtsız olduğuna dair güvenilir kanıtlar sunmak mümkün görünmemektedir.[63]

Journal of Strategic Studies, 43:2, 2020, s. 309.

55 Sayabek Ziyadin, Saltanat Suieubayeva ve Aliya Utegenova, "Digital Transformation in Business", Ashmarina Svetlana & Vochozka Marek (ed.), Mantulenko Valentina, Digital Age: Chances, Challenges and Future, Springer Cham, 2020, s. 408.

56 Saeed Albukhitan, "Developing Digital Transformation Strategy For Manufacturing", Procedia computer science, 170, 2020, s. 664.

57 Stefan Silfverskiöld, Kent Andersson ve Martin Lundmark. "Does The Method For Military Utility Assessment Of Future Technologies Provide Utility?", Technology in Society, 67, 2021, s. 4.

58 Therese Heltberg, ""I Cannot Feel Your Print". How Military Strategic Knowledge Managers Respond To Digitalization", Journal of Strategy and Management, 15:2, 2022, s. 220.

59 NATO, "Science &Technology Trends: 2020–2040", NATO Report, 2020, https://tto.iste.edu.tr/content/files/tto-8faf19a901-73c24.pdf, erişim 25.11.2023, s. 2.

60 Saeed Albukhitan, "Developing Digital Transformation Strategy For Manufacturing", Procedia Computer Science, 170, 2020, s. 664.

61 Daniel Billing vd., "The Implications Of Emerging Technology On Military Human Performance Research Priorities", Journal of Science and Medicine in Sport, 24:10, 2021, s. 947.

62 Kelley M. Sayler, "Emerging Military Technologies: Background and Issues for Congress", CRS Report, October 2021, https://apps.dtic.mil/sti/pdfs/AD1151925.pdf, erişim 23.11.2023, s. 6.

63 Micheal C. Horowitz, Lauren Kahn ve Casey Mahoney, "The Future Of Military Applications Of Artificial İntelligence: A Role For Confidence-Building Measures?", Orbis, 64:4,2020, s. 528.

Tablo 4. Orduların Dijital Dönüşümünde Yaşadıkları Zorluklar

(Askeri Uzman Değerlendirmesi)

Askeri uzmanlar	Sorunlar
AU1	Değişime Karşı Direnç
AU2	Siber Güvenlik Riskleri
AU3	Değişime Karşı Direnç
AU4	Eski sistemlerin modernizasyonu
AU5	Siber Güvenlik Riskleri
AU6	Maliyetli Olması
AU7	Dijital Beceri Eksikliği
AU8	Dijital Beceri Eksikliği
AU9	Siber Güvenlik Riskleri
AU10	Eski sistemlerin modernizasyonu

Tablo 4, NATO'da görev alan askeri uzmanların orduların dijital dönüşümde tespit ettikleri en önemli sorunların neler olduğunu göstermektedir. NATO'da görev alan askeri uzmanların değerlendirmelerine göre, orduların kapalı sisteme sahip olması, dijital dönüşümün siber güvenlik riskleri oluşturması, 15 yıl üstü subaylara yeni beceriler kazandırmanın zor olması, yeni teknolojilerin maliyetli olması, orduların dijital dönüşümde yaşadıkları en büyük problemlerdir. AU1'e göre askeri personelin "usulün değişmemesi gerektiği yönünde kanaatinin çoğunlukta" olduğunu belirtmiştir. AU2 ise orduların dijital dönüşümde yaşadıkları en büyük problemin "yeni teknolojilerin güvenlik açığı oluşturarak ülkenin güvenliğini etkileme potansiyeli" olduğunu söylemiştir. AU3, "Üst kademede ve uzun yıllar boyunca faaliyetlerini eski teknolojiyi öğrenmekle geçiren askeri uzmanın yeni sistemi kullanmada direteceğini bunun sonucunda askeri faaliyetlerde birtakım aksamaların oluşabileceğini" söylemiştir. Hatta "bu kişilerin yeni teknolojinin işlerini elinden alma potansiyelini göz önüne alarak faaliyetleri bilerek yavaş yapma, yeni teknolojinin verimsiz olduğunu kanıtlama yönünde girişimlerde bulunabileceğini" ifade etmiştir. AU4 ise "askeri düzenin yeni teknolojilere uyum sağlayabilmesinin uzun sürdüğünü dolayısıyla yeni teknolojilerin uyum sağlama zamanın yeni teknolojiyi eski teknolojiye dönüştürdüğünü" ifade etmiştir. AU5 "orduların yeni teknolojileri benimserken bu teknolojilerin oluşturacağı siber güvenlik açıklarının da yeni olabileceğinin göz önünde bulundurulması" gerekliliğini beyan etmiştir. AU6 "Dijital dönüşüm pahalı bir süreçtir dolayısıyla her ordunun bu tür ileri düzey teknolojileri üretip subaylarına benimsetmesi faydadan çok kaynak israfına doğru götürebilir" ifadesinde bulunmuştur. AU7, ordunun dijital beceri odaklı personel sayısının az olması sebebiyle ordunun dijitalleşme sürecinin çok uzun süreceğini belirtmiştir. AU7'nin görüşlerine benzer olarak AU8, personelin dijital becerilerinin ordunun tümüyle dijitalleşmesi için yetersiz olduğunu belirtmiştir. AU9, "Yeni teknolojilerin oluşturacakları yeni güvenlik tehditlerinin olacağını dolayısıyla ordularda dijital dönüşüm sürecinin dikkatli bir şekilde yürütülmesinin önemli olduğunu" ifade etmiştir. AU10, "Orduların eski sistemlere sahip olduğunu bu sistemlerin uyumlulukların sağlanmasının kolay olmadığını en büyük problemin bu noktadan kaynaklanabileceğini" ifade etmiştir.

Askeri uzmanlar tarafından en fazla bahsedilen sorunun siber güvenlik riskleri olduğu gözlemlenmiştir (3 askeri uzman). En az bahsedilen sorunun ise dijital dönüşümün maliyetli olmasıdır (1 askeri uzman). Askeri uzmanların değerlendirmeleri sonucu tespit edilen zorluklar ile sistematik literatür taraması sonucu elde edilen zorlukların çoğunluğunun

birbirleriyle örtüştüğü gözlemlenmiştir. Askeri uzmanların değerlendirmelerinden farklı olarak sistematik literatür taraması mevzuata uygunluk faktörünün orduların dijital dönüşümü için önemli olduğu belirlenmiştir.

5. Çözüm Önerileri

Dijital dönüşüm, dünya çapındaki orduların modern savaştaki etkinliğini sürdürmesi için bir zorunluluk haline gelmiştir. Ancak dijital dönüşüm sürecinde orduların karşılaşabileceği çeşitli zorluklar bulunmaktadır. Literatür taraması ve NATO'da görev yapan 6 farklı ülke askeri uzmanının görüşleri sonucunda aşağıdaki unsurların orduların dijital dönüşümünde yaşadıkları zorluklar olduğu tespit edilmiştir:

5.1. Eski Sistemler ve Teknoloji

Birçok ordu, yeni dijital sistemlerle uyumlu olmayabilecek eski sistemleri ve teknolojileri kullanmaya devam etmektedir. Eski sistemleri aşamalı olarak ortadan kaldırmak ve bunları daha yeni teknolojilerle değiştirmek, özellikle ordular gibi büyük kuruluşlar için zorlu bir görev olabilir. Farklı departmanlar ve paydaşlar arasında dikkatli planlama, koordinasyon ve iş birliği gerektirir. Ek olarak, eski sistemleri kullanmaya alışkın olan bireyler veya gruplar değişime karşı direnç gösterebilir. Mevcut operasyonları aksatmamak için planlı ve sistematik bir şekilde yapılması gereklidir. İleri teknolojileri mevcut sistemleri entegre edilmesini sağlamak, bu teknolojileri askeri birliklere uygulamak ve doktrini ileri teknolojilere göre uyarlamak uzun zaman almaktadır.[64] Güvenlik açıklarını en aza indirmek için eski sistemlerinin değiştirilmesi oldukça maliyetlidir.[65] Eski sistem ve teknolojinin yenileriyle değiştirilmesinde deneyimli ve kıdemli personel tarafından değişime direnç gösterecekleri yönde cevaplar alınması beklenmektedir. Eski savaş yöntemleri ve eski sistemler, teknolojideki ilerlemeye rağmen geçerliliklerini korumaktadır.[66] İleri teknolojileri mevcut sistemleri entegre edilmesini sağlamak, bu teknolojileri askeri birliklere uygulamak ve doktrini ileri teknolojilere göre uyarlamak uzun zaman almaktadır.[67] Güvenlik açıklarını en aza indirmek için eski sistemlerinin değiştirilmesi oldukça maliyetlidir.[68] Bu, yeni teknolojiyi entegre etmede verimsizliklere ve zorluklara neden olabilmektedir. Eski sistemler, geliştirmeler yoluyla bir uyumluluk durumuna geçirilmelidir.[69] Olası bir çözüm, eski sistemleri kademeli olarak devre dışı bırakmak ve bunları daha yeni teknolojilerle değiştirmektir. Askeri dijital dönüşümler, yavaş ilerlemeli veya kısa adımlarla ve iyileştirilmiş sonuçlar hedeflenmelidir. Eski ve yeni sistemler arasında veri alışverişi sağlamak için ara katmanlar ve uygulama programlama arayüzleri (API'lar) kullanılmalıdır. Mevcut altyapının uyumlu hale getirilmesi için düzenli uyumluluk testleri yapılmalıdır. AU4'e göre eski sistemlerin yeni sistemlere entegre edilmesi işleminin kademeli olarak gerçekleştirilmesi gerektiğini belirtmiş, öncelikle basit faaliyetler kullanılmalı, zamanla daha karmaşık eylemler için kullanılmasını önermiştir. Böylelikle personelin yetenek ediniminin daha kolaylaşacağını belirtmiştir. Ayrıyeten bu

64 Stefan Silfverskiöld, Kent Andersson ve Martin Lundmark, "Does the method for Military Utility Assessment of Future Technologies Provide Utility?", Technology in Society, 67, 2021, s. 4.
65 Martin Libicki. "What Is Information Warfare? Center For Advanced Concepts And Technology". Defense Technical Information Center Report, 1995, https://apps.dtic.mil/sti/pdfs/ADA367662.pdf, erişim 25.11.2023, s. 16.
66 Micheal E. O'Hanlon. "Forecasting Change In Military Technology, 2020-2040", Foreign Policy at Brookings, 2018, s. 1.
67 Stefan Silfverskiöld, Kent Andersson ve Martin Lundmark, "Does The Method For Military Utility Assessment of Future Technologies Provide Utility?", Technology in Society, 67, 2021, s. 12.
68 Martin Libicki, "What Is Information Warfare? Center For Advanced Concepts and Technology", Defense Technical Information Center Report, 1995, https://apps.dtic.mil/sti/pdfs/ADA367662.pdf, erişim 25.11.2023, s. 14.
69 Annette J. Krygiel "Behind The Wizard's Curtain: An Integration Environment For A System Of Systems". Defense Technical Information Center Report, 1999, https://apps.dtic.mil/sti/pdfs/ADA461322.pdf, erişim 25.11.2023.

zaman zarfı içerisinde yeniliklere uygun personellerin alınması gerektiğini ifade etmiştir. AU10 ise çözümün ara sistemler üretmek olduğunu savunmuş, ara sistemler sayesinde eski sisteme ilişkin bilgilerin yeni sisteme aktarılması veya iki sistem arasındaki bilgi alışverişinin sağlanmasını kolaylaştıracağını değerlendirmiştir.

5.2. Siber Güvenlik

Teknoloji ilerledikçe, dünyanın dört bir yanındaki ordular, iletişim, istihbarat ve silah sistemleri gibi kritik işlevler için dijital sistemlere giderek daha fazla güvenmektedir. Bu, şüphesiz operasyonel yeteneklerini geliştirirken, aynı zamanda onları siber saldırılara karşı daha savunmasız hale getirmektedir. Bilgisayar korsanları ister devlet destekli ister bağımsız aktörler olsun, hassas bilgilere erişmek veya hayati operasyonları bozmak için bu sistemlerdeki zayıflıklardan yararlanabilir. Çekirdek altyapı için çok sayıda bağlı cihaz ve ağ sanallaştırma teknikleri kesinlikle potansiyel saldırı yüzeyini artıracaktır.[70] Yapay zekâ sistemleri, küçük, kasıtlı değişikliklerin hatalı önerilere veya yetersiz eylemlere yol açabileceği siber saldırılara karşı özellikle savunmasızdır.[71] Ekipman ve araçların otomasyonu, siber tehditlerin erişimini fiziksel alana genişleterek, sistemleri bozmanın ve kafa karışıklığı yaratmanın ötesine geçerek fiziksel hasara yol açmalarına olanak tanır.[72] Düşman bir iletişim yönlendiricisine, bir veri tabanına yönelik çeşitli siber saldırılar yapma seçeneğine sahiptir.[73] Otomasyon, bir ordunun gizlilik, aldatma ve stratejiye dayalı siber saldırılara karşı savunmasızlığını artırabilir.[74] Teknoloji ilerledikçe, dünyanın dört bir yanındaki ordular, iletişim, istihbarat ve silah sistemleri gibi kritik işlevler için dijital sistemlere giderek daha fazla güvenmektedir. Bu, şüphesiz operasyonel yeteneklerini geliştirirken, aynı zamanda onları siber saldırılara karşı daha savunmasız hale getirmektedir. Üst düzey komuta kademesinde bulunan personelin siber güvenlik riskleri karşısında daha çekingen davranacağı değerlendirilmektedir. Bu doğrultuda verilerin dijital ortamlara aktarılıp işlenmesi sürecinde güvenlik tedbirlerini her şeyin üstünde tutmak isteyeceklerdir. Olası çözümlerden biri, şifreleme, güvenlik duvarları ve saldırı tespit sistemleri dahil olmak üzere sağlam siber güvenlik önlemlerine yatırım yapmaktır. Düzenli eğitim ve bilinçlendirme programları, askerlerin ve personelin riskleri ve bunların nasıl azaltılacağını anlamalarına yardımcı olabilmektedir. AU2, ileri teknolojilerin siber güvenlik açısından düzenli olarak uzman personel tarafınca test edilmesi gerektiğini ve uzmanların, personelin siber güvenliğinin farkındalığını artırmaya yönelik faaliyetlerde bulunmasını önermektedir. AU5 bu işlem için profesyonel ekiplerin görev alması gerektiğini dolayısıyla konuya ilişkin özel şirketlerle koordineli bir şekilde hareket edilmesi gerektiğini savunmaktadır. AU9 ise siber güvenlik biriminin kurulması ve bu birimin sistematik bir şekilde birlikleri siber güvenlik açısından kontrol edip değerlendirmesi gerektiğini ifade etmiştir.

5.3. Veri Yönetimi

Modern ordular tarafından üretilen veri miktarı çok fazladır ve bu verileri yönetmek zor olabilir, ancak etkili karar verme ve görev başarısı için de kritik öneme sahiptir. Gelecekteki savaş durumları optimizasyon kararları daha fazla ve daha çeşitli veriye ve veri türlerine

70 Anshu Bhardwaj. "5G For Military Communications", Procedia Computer Science, 171, 2020, s. 2665.

71 NATO, "Science &Technology Trends: 2020–2040", https://tto.iste.edu.tr/content/files/tto-8faf19a901-73c24.pdf, NATO Report, 2020, erişim 25.11.2023, s. 4.

72 Denise E. Zheng ve William A. Carter, Leveraging The Internet of Things For A More Efficient And Effective Military. Rowman & Littlefield, Lanham, 2015, s. 26.

73 David S. Alberts, John Garstka ve Frederick P. Stein, Network Centric Warfare: Developing And Leveraging Information Superiority. National Defense University Press Washington, DC, 1999, s. 12.

74 James Johnson, "The AI-Cyber Nexus: Implications For Military Escalation, Deterrence And Strategic Stability", Journal of Cyber Policy, 4:3, 2019, s. 442.

dayalı olacaktır. Bu veriler, istihbarat raporları ve gözetleme görüntülerinden lojistik bilgilerine ve iletişim verilerine kadar her şeyi içerir. Büyük veri hacmine ek olarak, modern askeri operasyonların karmaşıklığı, verilerin çok çeşitli kaynaklardan ve birçok farklı formatta geldiği anlamına gelir. Bu, verileri etkili bir şekilde entegre etmeyi ve analiz etmeyi zorlaştırabilir. Sahada verilerin savaş alanındaki ilerlemeyi ne kadar doğru yansıttığı değerlendirilmeden çok fazla veri noktasının toplanmasından kaynaklanan komplikasyonlar ortaya çıkabilme durumu vardır.[75] Modern ordular tarafından üretilen veri miktarı çok fazladır ve bu verileri yönetmek zor olabilir, ancak etkili karar verme ve görev başarısı için de kritik öneme sahiptir. Gelecekteki savaş durumları optimizasyon kararları daha fazla ve daha çeşitli veriye ve veri türlerine dayalı olacaktır. Bu alanda da siber güvenlikteki gibi üst düzey komuta kademesi riskleri minimuma indirmek için hızdan taviz vereceklerdir. Olası çözüm, üretilen çok büyük miktardaki veriyi anlamlandırmaya yardımcı olabilecek veri analitiği araçlarını ve tekniklerini uygulamaktır. Bu, karar verme için değerli bilgiler sağlayabilmekte ve genel operasyonel verimliliği artırabilmektedir.

5.4. Değişime Karşı Direnç

Değişime karşı direnç, herhangi bir organizasyonda yaygın bir sorundur ve ordular da bir istisna değildir. Bazı askerler, özellikle geleneksel yöntemlere alışkınlarsa, yeni teknolojiyi benimseme konusunda isteksiz olabilirler. Askeri kuruluşlar, genellikle mevcut operasyon modlarıyla çatışan alternatif iş yapma yöntemlerini benimseme konusunda isteksizdir.[76] Askeri kurumlarda yapılan dijital dönüşüm girişimlerinin değişime karşı direnç karşılaşılan bir problemdir.[77] Ordular, bu direncin üstesinden gelmek için değişim yönetimine proaktif bir yaklaşım benimsemelidir. Bu, yeni teknolojinin faydalarını özetleyen ve nasıl uygulanacağına dair net rehberlik sağlayan kapsamlı bir değişiklik yönetimi planı geliştirmeyi içerebilir. Plan ayrıca askerler ve diğer paydaşlarla değişikliklerden haberdar olmalarını sağlamak ve sahip olabilecekleri endişeleri gidermek için düzenli iletişimi içermelidir. Ordular, iletişime ek olarak, faydaları vurgulayarak ve uygun eğitim ve desteği sağlayarak askerleri yeni teknolojiyi benimsemeye teşvik edebilir. Bu, ek eğitim fırsatları sunmayı veya yeni sistemlerde yeterlilik gösteren askerleri tanımayı içerebilir. Askerleri en başından değişim yönetimi sürecine dahil etmek önemlidir. Ordular, geri bildirimlerini isteyerek ve onları karar verme sürecine dahil ederek, askerlerin değişikliklere kendilerini kaptırdıklarını ve onları benimseme olasılıklarının daha yüksek olmasını sağlamaya yardımcı olabilir. Potansiyel bir çözüm, askerleri en başından dijital dönüşüm sürecine dahil etmektir. Bu, katılım oluşturmaya ve askerlerin yeni teknoloji konusunda kendilerini rahat hissetmelerini sağlamaya yardımcı olabilmektedir. AU1, ileri teknolojik araçlar ile eski teknolojik araçların ikisinin mevcut düzende yer alması gerektiğini fakat ileri teknolojik aracın kullanılması taktirde ödüllendirecek düzenlemelerin veya teşviklerin oluşturulmasını önermiştir. AU3 ise yeni teknolojik araçların sağladıkları faydaların personele iyi bir şekilde açıklanması gerektiğini belirtmiş, eğitim programlarındaki uzmanların empatik yaklaşım benimsemelerini ifade etmiştir.

5.5. Eğitim ve Öğretim

Son olarak, orduların, askerlerin dijital ortamda faaliyet gösterecek gerekli bilgi ve becerilerle donatılmasını sağlamak için eğitim ve öğretime yatırım yapması gerekmektedir.

75 Gregory A. Daddis, No Sure Victory: Measuring US Army Effectiveness and Progress in the Vietnam War, Oxford University Press, Oxford, 2011, s. 10.

76 Evan B. Montgomery, "Signals Of Strength: Capability Demonstrations And Perceptions Of Military Power", Journal of Strategic Studies, 43:2, 2020, s.309.

77 Mylène Struijk vd., "Navigating Digital Transformation Through An İnformation Quality Strategy: Evidence From A Military Organisation", Information Systems Journal, 33:4, 2023, s. 912.

Bu, belirli sistemler ve teknolojiler hakkında eğitimin yanı sıra daha geniş dijital okuryazarlık programlarını içerebilmektedir. Bu eğitimin kritik bir yönü, askerlere kullanacakları dijital sistemler ve teknolojiler hakkında özel eğitim sağlamaktır. Bu, temel bilgisayar okuryazarlığından karmaşık silah sistemleri veya iletişim teknolojilerine ilişkin özel eğitime kadar her şeyi içerebilir. Bu eğitim, askerlere kullandıkları sistemler ve bunları güvenli ve etkili bir şekilde nasıl çalıştıracakları hakkında derin bir anlayış sağlamak için tasarlanmalıdır. Ordular, sisteme özel eğitime ek olarak, daha geniş dijital okuryazarlık programları uygulamayı da düşünmelidir. Bu programlar, askerlerin dijital teknolojinin daha geniş etkilerini ve modern savaşı nasıl dönüştürdüğünü anlamalarına yardımcı olabilir. Konular, veri gizliliği ve güvenliği, siber tehditler ve askeri operasyonlarda sosyal medyanın kullanımını içerebilir. Ordular, askerlere dijital manzara hakkında kapsamlı bir anlayış sağlayarak, modern savaşın karmaşıklıklarında daha iyi gezinmelerine yardımcı olabilir. Ordular, yeni teknolojinin tehditlerine karşı koymak için hangi askeri yeteneklere ihtiyaç duyulduğunu tespit etmeleri gerekmektedir.[78] İleri teknolojiler, askeri kuvvetlerin paylaşım, toplama, modelleme ve simülasyon, analiz, sınıflandırma, iyileştirme, iletişim ve veri yönetimi için yöntem ve standartların geliştirilmesi yeteneklerine sahip olmasını gerektirecektir.[79] Son olarak, orduların, askerlerin dijital ortamda faaliyet gösterecek gerekli bilgi ve becerilerle donatılmasını sağlamak için eğitim ve öğretime yatırım yapması gerekmektedir. Bu, belirli sistemler ve teknolojiler hakkında eğitimin yanı sıra daha geniş dijital okuryazarlık programlarını içerebilmektedir. Eğitim ve öğretim alanında ise her seviye de ve yaşta farklı cevaplar verilmesi beklenmektedir. Mesleki süreçlerinin sonuna gelmiş personelinde eğitime ve öğretime karşı direnç gösterebileceği düşünülmektedir. Yeni teknolojiler, iletişim hatlarında ve planlama süreçlerinde değişikliklerin yanı sıra organizasyonel yapılarda ve personel niteliklerinde ve eğitimde değişiklikler gerektirebilir.[80] AU7, özellikle genç personelin dijital eğitimlerde daha başarılı olabileceğini bu çeşit eğitimlerde ölçütlerin içerisinde yaş ve meslek olması gerektiğini değerlendirmektedir. AU8, ordu içerisinde dijital dönüşüm ofisi tarzı bir birim oluşturmanın ve bu birimin dijital dönüşüme ilişkin yetkinliğe sahip kişilerden oluşmasını önermektedir. Bu birim birliklere gidecek, dijital dönüşüm eğitimi verecektir.

Sonuç

Dijital dönüşümün, artan verimlilik, gelişmiş durumsal farkındalık ve iyileştirilmiş karar verme gibi ordulara önemli faydaları vardır. Ancak, dijital dönüşüm sürecinde orduların karşı karşıya kalabileceği çeşitli zorluklar da mevcuttur. Orduların dijital dönüşümü, askeri güçlerin daha hızlı, esnek ve bilgi temelli bir yapıya dönüşmesine olanak tanır. Ancak bu dönüşümün etkin bir şekilde yönetilmesi ve zorlukların aşılması için çaba sarf etmek önemlidir. Literatür taraması ve askeri uzmanların değerlendirmeleri sonucunda eski sistemlerin yeni teknolojilere uyum sağlamada sorun yaşadığı, dijital dönüşümün siber güvenlik açıkları oluşturduğu, veri yönetiminde altyapı eksikliği görüldüğü, eğitim ve öğretim alanlarında 10 yıl ve üzeri personelin değişime karşı direnç gösterebileceği tespit edilmiştir. Orduların dijital dönüşüm süreci diğer sivil kurum/kuruluş ve işletmelere benzememektedir. Yıllarca süren bir gelenek yapısıyla güvenlik kaygılarıyla kendini dış dünyaya birçok noktadan kapatmış ordular dijital dönüşüm sürecinde personeli ile birçok sorun yaşamaktadır. Sorunların da bu kapalı sistemlerde direkt ifade edilmesi ve ortaya konması pek mümkün olmamaktadır.

78 Stefan Silfverskiöld, Kent Andersson ve Martin Lundmark. "Does The Method For Military Utility Assessment Of Future Technologies Provide Utility?", Technology in Society, 67, 2021, s. 3.

79 NATO, "Science &Technology Trends: 2020–2040", NATO Report, 2020, https://tto.iste.edu.tr/content/files/tto-8faf19a901-73c24.pdf, erişim 25.11.2023, s. 10

80 Therese Heltberg, ""I Cannot Feel Your Print", How Military Strategic Knowledge Managers Respond To Digitalization", Journal of Strategy and Management, 15:2, 2022, s.220.

Eski sistemlerin yeni teknolojilerle değiştirilmesi, büyük bir organizasyonun tüm departmanları ve paydaşları arasında dikkatli planlama ve koordinasyon gerektirir. Eski sistemleri kullanmaya alışkın olan personelin değişime karşı direnç gösterebileceği bir gerçektir. Bu durumda, eski sistemleri kademeli olarak devre dışı bırakmak ve yeni teknolojilerle değiştirmek önemlidir. Aynı zamanda, personelin bu değişimi benimsemesi ve uyum sağlaması için eğitim ve destek sağlanmalıdır. Dijitalleşme orduların operasyonel yeteneklerini artırsa da siber güvenlik risklerini de artırır. Bilgisayar korsanlarının ve siber saldırganların hedefi olmak, orduların savunmasız kalmasına neden olabilir. Bu riskleri azaltmak için güçlü siber güvenlik önlemleri alınmalıdır. Bu önlemler arasında şifreleme, güvenlik duvarları, saldırı tespit sistemleri ve düzenli eğitim programları yer almalıdır. İleri teknolojilerin siber güvenlik açısından düzenli olarak uzmanlar tarafından test edilmesi gerekmektedir. Büyük veri hacmi ve farklı veri türleri, orduların etkili kararlar almasını ve operasyonel başarıyı sağlamasını zorlaştırabilir. Veri analitiği araçları ve teknikleri kullanılarak bu veriler daha anlamlı hale getirilmeli ve operasyonel verimliliği artırmak için kullanılmalıdır. Veri yönetimi süreci, düzenli olarak güncellenen yöntemler ve standartlarla desteklenmelidir. Değişime karşı direnç, organizasyonlarda yaygın bir sorundur ve ordular da istisna değildir. Yeni teknolojiye geçiş süreci, askerlerin değişime uyum sağlaması için destekleyici bir yaklaşımla yönetilmelidir. Askere özel eğitimler, iletişim ve katılım, direnci azaltmaya yardımcı olabilir. Dijital dönüşüm, askerlerin dijital okuryazarlığını artırmayı ve yeni teknolojileri etkili bir şekilde kullanmalarını gerektirir. Ordular, özel eğitimler ve genel dijital okuryazarlık programlarıyla askerleri donatmalıdır. Eğitim süreci, askerlerin değişen dijital manzaranın karmaşıklığını anlamalarını sağlamalıdır.

Bugün ülkelerin askeri güçleri ile rekabet gücüne sahip olabilme yolu iş süreçlerinin dijital teknolojiler ile entegrasyonundan geçmektedir. Ülkelerin rekabet gücünün önem taşıdığı sektörlerin başında gelen savunma sanayi sektörü sahip olduğu ileri teknolojik ürün ve hizmetler, altyapılar ve sistemler ile dönüşümü desteklemektedir. Çin'in küresel düzeyde elde ettiği güç, Rusya-Ukrayna Savaşı, terör olaylarının yaygınlaşması, saldırı türlerinin çeşitlenmesi (siber saldırlar vb.) gibi olaylar doğrultusunda ülkeler savunma sanayilerinin gücünü artıracak yatırımlar yapmaktadırlar. Tüm bunların yanı sıra sektörün sahip olduğu ileri teknolojik gücü sürdürmesi için yapılan Ar-Ge yatırımları da savunma sanayi harcamalarını artırmaktadır. Savunma sistemlerinin, güçlü, etkili ve çevik olması, maliyet, zaman ve kaynak tasarrufunun sağlanması ve savunma sanayi firmalarının rekabet gücünün koruması noktasında bu yatırımlar önem teşkil etmektedir. Dijitalleşme süreci, savunma sanayinin yenilikçi çözümler geliştirmesine ve sektörün rekabet gücünün korunmasına etki etmektedir. Dijitalleşme sürecinin lokomotif sektörleri arasında yer alan savunma sanayinin sahip olduğu teknolojik güç, aynı zamanda ülkelerin maruz kalabilecekleri tehdit ve tehlikeler karşısında caydırıcılık etkisi yaratmaktadır. Bununla birlikte yüksek teknoloji ve bilgi yoğunluğu yapısına bağlı olarak diğer sektörlere yönelik pozitif bilgi dışsallığı sağlamaktadır. Bu noktada sektörün dijitalleşmesi iktisadi ve sosyal refaha da etki etmektedir. Sonuç olarak, askeri gücün artırılması, savunma yeteneklerinin geliştirilmesi, ulusal güvenliğin sağlanması, savunma sanayinin rekabet gücünün artırılması, yeni teknolojilerin sistem, süreç ve ürünlere hızlı bir şekilde entegre edilebilmesi ve stratejik ortaklıkların geliştirilebilmesi noktasında orduların dijital dönüşümü önem teşkil etmektedir. Dijital dönüşüm sürecinde yaşanan sorunların bir kısmı ülkelerin güvenlik sorunlarını oluşturmaktadır.

Araştırma, uluslararası düzeyde ordunun yaşadığı dijital dönüşüm ile ilgi sorunların ortaya konması neticesinde bu sorunlara çözüm olacak yeni projelerin ortaya konmasına katkı sağlayabilir. Bu çalışma personelin farkındalığı arttırılarak kendi çözümlerini de üretmesinde

yardımcı olabilir. Araştırma yöntemi, literatür taramasının sınırlılıklarını da dikkate almıştır. Literatür taramasında kapsamlı olmaya çalışılırken, ilgili bazı kaynakların atlanmış olması muhtemeldir. Ek olarak, makale, kaynak seçiminin doğasında var olan potansiyel önyargıları ve araştırmacının yorumunun etkisini kabul etmektedir. Bu makale, orduların dijital dönüşüm sürecine ilişkin güncel ve özgün bilgilerle donatılmış olmasıyla, ilgili alanlarda çalışan araştırmacılar, askeri liderler ve politika yapıcılara kaynak olarak değerlendirilebilir.

Çatışma Beyanı:

Araştırmanın yazarları olarak herhangi bir çıkar çatışma beyanımız bulunmamaktadır.

Araştırmacıların Katkı Oranı Beyanı:

Yazarlar araştırmaya eşit oranda katkıda bulunmuştur.

Kaynakça

Basılı Eserler

ALBERTS David S. GARSTKA Joh ve STEIN Frederick P. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority*, National Defense University Press, Washington, DC.

ALBUKHITAN Saeed (2020). "Developing Digital Transformation Strategy for Manufacturing", *Procedia Computer Science*, 170, 664-671.

ARMY OF UNITED STATES. (2001). *Operations (FM 3-0)*. Department of the Army, Washington, DC.

BHARDWAJ Anshu (2020). "5G for Military Communications", *Procedia Computer Science*, 171, 2665-2674.

BILLING C. Daniel FORDY Graham R. FRIEDL Karl E. ve HASSELSTRØM Henriette (2021). "The Implications of Emerging Technology on Military Human Performance Research Priorities", *Journal of Science and Medicine in Sport*, 24:10, 947-953.

BURMAOĞLU Serhat SARITAŞ Ozcan ve YALÇIN Haydar (2019). "Defense 4.0: The Internet of Things in Military", Dirk Meissner, Leonid Gokhberg ve Ozcan Saritas (ed.), *Emerging Technologies for Economic Development,* Springer Nature, Switzerland, 303-320.

DADDIS Gregory A. (2011). *No Sure Victory: Measuring US Army Effectiveness and Progress in the Vietnam War*, Oxford University Press, Oxford.

DUMAN Aslı (2019). Endüstri 4.0 İle Akıllı Üretimin İşletme Performansı Üzerine Etkisi: Vestel Buzdolabı Fabrikası'nda Bir Uygulama*, Yüksek Lisans Tezi,* Manisa Celal Bayar Üniversitesi, Manisa.

DUMAN Aslı (2023). "Savunma Sanayiinin Dijitalleşmesi ve Modernleşmesi", Arzu Uğurlu Kara ve Kubilay Baş (ed.), *Savunma Yönetimi: Disiplinlerarası Bir Yaklaşım*, Nobel Yayınevi, Ankara, 281-307.

ELLSTRÖM Daniel HOLTSTRÖM Johan BERG Emma ve JOSEFSSON Cecilia (2021). "Dynamic Capabilities for Digital Transformation", *Journal of Strategy and Management*, 15:2, 272-286.

EMIMI Mohamed, KHALEEL Mohamed ve ALKRASH Abobakr (2023). "The current opportunities and challenges in drone technology", *International Journal of Electrical Engineering and Sustainability (IJEES)*, 3:1, 74-89.

FLETCHER Gordon ve GRIFFITHS Marie (2020). "Digital Transformation During A Lockdown", *International Journal of Information Management*, 55:5, 102185.

FRANKENBERGER Karolin MAYER Hannah REITER Andreas ve SCHMIDT Markus (2020). *The Digital Transformer's Dilemma: How To Energize Your Core Business While Building Disruptive Products And Services*. John Wiley & Sons, New Jersey.

FRANKIEWICZ Becky ve CHAMORRO-PREMUZIC Tomas (2020). "Digital transformation Is About Talent, Not Technology", *Harvard Business Review*, 6:3, 1-6.

GOODWIN Tom (2018). *Digital Darwinism: Survival of the Fittest in The Age Of Business Disruption*, Kogan Page Publishers, London.

GONG Cheng ve RIBIERE Vincent (2021). "Developing a Unified Definition of Digital Transformation", *Technovation*, 102:3, 102217.

GUNAWAN Aditya B. (2022). Under the Shadow of Army Domination: Defense Transformation in Indonesia, *Yüksek Lisans Tezi*, Heidelberg University, Heidelberg.

HELTBERG Therese (2022). ""I Cannot Feel Your Print", How Military Strategic Knowledge Managers Respond To Digitalization", *Journal of Strategy and Management*, *15*:2, 220-233.

HILL Andrew (2015). "Military Innovation and Military Culture", *The US Army War College Quarterly: Parameters*, 45:1, 85-98.

HOROWITZ Micheal C. KAHN Lauren ve MAHONEY Casey. (2020). "The Future Of Military Applications Of Artificial Intelligence: A Role For Confidence-Building Measures?", *Orbis*, 64:4, 528-543.

JOHNSON James (2019). "The AI-Cyber Nexus: Implications For Military Escalation, Deterrence And Strategic Stability", *Journal of Cyber Policy*, 4:3, 442-460.

KONOPIK Jens JAHN Christoph SCHUSTER Tassilo HOßBACH Nadja ve PFLAUM Alexander (2022). "Mastering The Digital Transformation Through Organizational Capabilities: A Conceptual Framework", *Digital Business*, 2:2, 100019.

KUNERTOVA Dominika (2022). "The Ukraine Drone Effect On European Militaries", *CSS Policy Perspectives*, 10:15, 1-5.

MONTGOMERY Evan B. (2020). "Signals Of Strength: Capability Demonstrations And Perceptions Of Military Power", *Journal of Strategic Studies*, 43:2, 309-330.

NEADS Alex, FARRELL Theo ve GALBREATH David J. (2023). "Evolving Towards Military Innovation: AI And The Australian Army", *Journal of Strategic Studies*, 1-30.

NONAKA Ikujiro ve TAKEUCHI Hirotaka (2019). *The Wise Company: How Companies Create Continuous Innovation*, Oxford University Press, Oxford.

NORHEIM-MARTINSEN Per Martin (2016). "New Sources of Military Change–Armed Forces as Normal Organizations", *Defence Studies*, 16:3, 312-326.

O'HANLON Micheal E. (2018). "Forecasting Change In Military Technology, 2020-2040", *Foreign Policy at Brookings,* 1-30.

PORFÍRIO Jose A. CARRILHO Tiago FELÍCIO Jose A. ve JARDIM Jacinto (2021). "Leadership Characteristics And Digital Transformation", *Journal of Business Research*, *124*, 610-619.

ROTHER Edna T. (2007). "Systematic Literature Review X Narrative Review", *Acta Paulista de Enfermagem*, 20, 1-6.

SAĞBAŞ Murat ve ERDOĞAN Fahri A. (2022). "Digital Leadership: A Systematic Conceptual Literature Review", İstanbul Kent Üniversitesi İnsan ve Toplum Bilimleri Dergisi, 3:1, 17-35.

SCHIUMA Giovanni (2012). "Managing Knowledge For Business Performance İmprovement", *Journal of Knowledge Management*, 16:4, 515-522.

SILFVERSKIÖLD Stefan ANDERSSON Kent ve LUNDMARK Martin (2021). "Does The Method For Military Utility Assessment Of Future Technologies Provide Utility?", *Technology in Society*, *67*, 101736.

STRUIJK Mylène ANGELOPOULOS Spyros OU Carol X. ve DAVISON Robert M. (2023). "Navigating Digital Transformation Through An Information Quality Strategy: Evidence From A Military Organisation", *Information Systems Journal*, 33:4, 912- 952.

TANG David (2021). "What Is Digital Transformation?", *EDPACS*, 64:1, 9-13.

TEECE David J. PISANO Gary ve SHUEN Amy (1997). "Dynamic Capabilities And Strategic Management", *Strategic Management Journal*, 18:7, 509-533.

TORTONESI Mauro MORELLI Alessandro GOVONI Marco MICHAELIS James SURI Niranjan, STEFANELLI Cesare ve RUSSELL Stephen (2016). Leveraging Internet Of Things Within The Military Network Environment-Challenges And Solutions. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT),* 111-116.

VERHOEF Peter C. BROEKHUIZEN Thijs BART Yakov BHATTACHARYA Abhi DONG John Q. FABIAN Nicolai ve HAENLEIN Micheal (2021). "Digital Transformation: A Multidisciplinary Reflection And Research Agenda", *Journal of Business Research*, *122*, 889-901.

WARNER Karl S. ve WÄGER Maximilian (2019). "Building Dynamic Capabilities For Digital Transformation: An Ongoing Process Of Strategic Renewal", *Long Range Planning*, 52:3, 326-349.

ZAOUI Fadwa ve Souissi Nissrine. (2020). "Roadmap For Digital Transformation: A Literature Review", *Procedia Computer Science*, 175, 621-628.

ZHENG Denise E. ve CARTER William A. (2015). *Leveraging the Internet of Things for a More Efficient and*

Effective Military, Rowman & Littlefield, Lanham.

ZIYADIN Sayabek, SUIEUBAYEVA Saltanat ve UTEGENOVA Aliya (2020). "Digital Transformation in Business", Ashmarina Svetlana, Vochozka Marek & Mantulenko Valentina (ed.), *Digital Age: Chances, Challenges and Future,* Springer Cham, 408- 415.

İnternet Kaynakları

DELOITTE. "Aerospace and Defense 4.0, Capturing the Value of Industry 4.0 Technologies" https://www2.deloitte.com/content/dam/insights/us/articles/4912_Aerospace-and-defense-4-0/DI_A&D_4-0.pdf, erişim 28.11.2023.

KRYGIEL Annette J. "Behind The Wizard's Curtain: An Integration Environment For A System Of Systems". *Defense Technical Information Center Report*, 1999, https://apps.dtic.mil/sti/pdfs/ADA461322.pdf, erişim 25.11.2023.

LIBICKI Martin C. "What Is Information Warfare? Center For Advanced Concepts And Technology". *Defense Technical Information Center Report*, 1995, https://apps.dtic.mil/sti/pdfs/ADA367662.pdf, erişim 25.11.2023.

NATO. "Science &Technology Trends: 2020–2040"*, NATO Report*, 2020, https://tto.iste.edu.tr/content/files/tto-8faf19a901-73c24.pdf, erişim 25.11.2023.

NATO News, "NATO Will Defend Itself" https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en, erişim 25.11.2023

PERNIN Christopher G. AXELBAND Elliot DREZNER Jeffrey A. DILLE Brian B. GORDON John IV, J. HELD Bruce J. MCMAHON Scott K. PERRY Walter L. RIZZI Christopher SHAH Akhil R. WILSON Peter A. ve SOLLINGER Jerry M. "Lessons from the Army's Future Combat Systems Program" *Rand Report, 2012*, https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1206.sum.pdf, erişim 23.11.2023.

SAYLER Kelley M. "Emerging Military Technologies: Background and Issues for Congress". *CRS Report,* October 2021, https://apps.dtic.mil/sti/pdfs/AD1151925.pdf, erişim 23.11.2023.

WORLD ECONOMIC FORUM. "The Global Risks Report 2023". https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf, erişim 23.11.2023.