Yapay Zekâ ve Endüstri 4.0 İlişkisinin Siber Güvenlik Perspektifinden Analizi

Ahmet EFE[1]

Makale Geçmişi
Başvuru Tarihi:11.05.2021
Kabul Tarihi:15.06.2021

Article History
Date of Application:11.05.2021
Acceptance Date:15.06.2021

Özet

Günümüzde, iş performansının etkinliği ve verimliliği, dijital rekabet faktörlerine ve akıllı yönetim bilişim sistemleriyle (YBS) dijitalleşme ışığında kurumsal kabiliyetleri dönüştürme yeteneğine ve endüstri 4.0'da (4IR) yapay zekâ (YZ) kullanımına bağlı hale gelmiştir. Bundan böyle hızla yaygınlaşan nesnelerin interneti (IoT) üzerinden siber-fiziksel sistemler, değer zincirinin katılımcıları tarafından hem dahili olarak hem de kurumsal hizmetler genelinde gerçek zamanlı olarak etkileşimde bulunmak ve iş birliği yapmak durumundadır. Bunu sağlayan 4IR'ın tasarım ilkeleri olan "*birlikte çalışabilirlik*", "*bilgi şeffaflığı*", "*teknik yardım*" ve "*YZ yardımıyla merkezi olmayan kararlar*" dır. Bu tasarım ilkelerinin her biri, çevik YZ uygulamalarından faydalanan kötü niyetli saldırganlar tarafından kullanılabilecek yeni saldırı alanları oluşturma potansiyeli sunmaktadır. Bu zafiyetlerden çıkan zorluklar, kolayca azaltılabilen veya göz ardı edilebilen basit tehditlerden, tüm sistemi kullanılamaz hale getirebilecek APT tehditlerine kadar değişen bir yelpazededir. Bu çalışmada, 4IR çağında küresel iş operasyonları için otomatikleştirilmiş sistemlerin gelişen rolü, YZ ve siber güvenlik perspektiflerinden değerlendirilmektedir. İddiamız, 4IR'da kullanılan YZ modellerinin, bilgisayar korsanı makine öğrenimiyle mücadele etmek, gizliliği korumak ve derin öğrenme sürecini güvenli hale getirmek gibi amaçlar için belirli IoT siber güvenlik savunma ve koruma teknolojilerine ihtiyaç duyacağı noktasındadır.

Anahtar Kelimeler: Endüstri 4.0, yapay zeka, siber güvenlik, YBS

Jel Kodları: M11, M15, O32, Q55

Analysis of the Relationship between Artificial Intelligence and Industry 4.0 from the Cyber Security Perspective

Abstract

Today, the effectiveness and efficiency of business performance have become dependent on digital competition factors and the ability to transform corporate capabilities in the light of digitalization via intelligent management information systems (MIS) and artificial intelligence (AI) in Industry 4.0 applications. Through the Internet of Things, cyber-physical systems have to interact and collaborate in real-time with the value chain participants, both internally and across corporate services. That is achieved through the design principles of Industry 4.0, "*interoperability*", "*information transparency*", "technical assistance," and "decentralized decisions" with the help of "*artificial intelligence*". However, each of these design principles offers the potential to create new attack areas that can be exploited by malicious attackers using agile AI-based tools and techniques. The challenges that arise from these vulnerabilities range from simple threats that can be easily mitigated or ignored to APT threats that can render the entire system unusable. In this study, the evolving role of automated systems for global business operations in the age of Industry 4.0 is evaluated from the perspectives of artificial intelligence and cybersecurity combination. We claim that AI models used in Industry 4.0 will need specific IoT cybersecurity defense and protection technologies for purposes such as combating hacker machine learning, protecting privacy, and securing the deep learning process.

Keywords: Industry 4.0, artificial intelligence, cybersecurity, MIS

Jell Codes: M11, M15, O32, Q55

[1] Dr., CISA, CRISC, PMP, İç Denetçi, Ankara Kalkınma Ajansı, icsiacag@gmail.com, ORCID: 0000-0002-2691-7517

1. Giriş

Kitlesel verilerin analitik olarak işlenerek otomatik akıllı süreçlerin işletilmesi endüstriyel bakımda kilit bir faktör haline gelirken, öngörücü algoritmaların hızlı bir şekilde iyileştirilmesi ve büyük veri analitiği ile YZ'nin geliştirilmesi endüstriyel süreçlerde derin bir dönüşüm sağlamıştır. Günümüzde veri analizi çözümleri, tahmin hesaplama modelleri vb. sunan birçok endüstriyel uygulama bulunmaktadır. Sanayi sektörü için bu teknolojiler gerçek ekonomik ve yapısal zorluklar sunmaktadır.

Yeni nesil yenilikçi endüstriyel sistemler, yani 4IR, büyük veri, akıllı fabrikalar, siber-fiziksel sistemler, nesnelerin interneti ve tüm tedarik zincirinin dijitalleştirilebileceği birlikte çalışabilirlik gibi birçok farklı araştırma alanını ve anahtar teknolojileri kapsamaktadır. Bu yeni sistemde, bir fabrika sadece tam otomatik değil, aynı zamanda tüm makineleri tek bir sistem içinde dijital olarak birbirine bağlı ve yeni kararlar için birbirileriyle etkileşim halinde çalışmaktadır. Fiziksel sistemler hem birbirleriyle hem de insan işçilerle uzaktan iletişim kurmak ve iş birliği yapabilmek durumundadırlar. Böylesine akıllı bir fabrika, tüm fiziksel süreçleri gerçek zamanlı olarak izlemeyi ve merkezi olmayan etkili kararlar almayı mümkün kılmak noktasında pek çok avantajlar sağlayabilmektedir. YZ ve makine öğrenimi gibi araçlar, sağlık hizmetlerinde dünya çapında hayat kurtaran ilerlemelere yol açarken, bu ve diğer yenilikçi teknolojiler de daha fazla iş akışı verimliliğine yol açmak ve onları takip etmeyi seçenler için yeni, daha ilginç profesyonel fırsatlar sağlamak gibi cezbedici yönlere de sahiptirler. Ancak, bunlar sağladığı yararlar yanında dünyayı yeni ve karmaşık siber risklere de maruz bırakabilmektedirler (Süzen, 2020). Çünkü her gülün dikeni olduğu gibi her kolaylığın bir zorluğu, her fırsatın da bir riski vardır. 2016 yılında Stanford Üniversitesi'nden Profesör Andrew Ng*, "YZ'nin yeni elektrik olduğu*"nu iddia etmiştir (Lynch, 2017). Böyle bir benzetme, aslında YZ'nin işletmeler ve toplum üzerindeki etkilerinin önümüzdeki yıllarda beklenen büyüklüğünü göstermektedir. Bu güçlü iddianın YZ araştırmacıları ve uygulayıcıları arasında çok makbul olduğu anlaşıldığından dolayı kitle iletişim araçlarında ve sosyal medyada sık sık buna alıntı yapılmıştı. Zekanın doğasına ve bilgisayar yazılımının sunduğu imkanlara ilgi duyarak başlayan YZ sürecinde insan zekasını tamamlayacak veya onu taklit edebilecek sürdürülebilir bir algoritma geliştirmek amaçlanmaktadır (Simon, 1995).

YZ alanı önemli ilerleme kaydetmekle birlikte YZ' nin kesin bir tanımı, kavramları ve uygulamaları yaymakla ilgilenenler için hala bir zorluk teşkil edebilmektedir. Bu alanda ciddi araştırmalar yapmış olan Simon (1995), YZ aracılığıyla zekanın özelliklerini gerçeğe dönüştürmekle ilgilenen bir bilgisayar bilimi dalı olarak tanımlarken, Stone ve ark. (2016) bunu hem bir bilim hem de insanların hissetmek, öğrenmek, akıl yürütmek ve hareket etmek için sinir sistemlerini ve bedenlerini kullanma biçiminden esinlenerek bundan farklı bir dizi hesaplama teknolojisi olarak görmüştür. Literatürdeki YZ ile ilgili 1000 civarındaki farklı tanımlamayı gözden geçiren Sweeney'e (2003) göre YZ hakkında insan düşüncesi, insan davranışı, ideal düşünme, ideal davranış ve hayvan davranışı şeklinde en az beş farklı bakış açısı vardır.

Şekil 1. YZ ile ilgili olarak beş farklı bakış açısı

YZ yalnızca teori ve vaat olmadığından gerçek hayatta onlarca yıldır YZ'dan yararlanılmaktadır. Örneğin, sağlık hizmetleri ve işletme yönetimi gibi birçok alanda gelişmeleri teşvik ederek hayatımızı önemli ölçüde etkileyebilmektedir. Bununla birlikte, ilerlemenin çoğu, garip paradoks adı verilen bir etkisi nedeniyle YZ etkisi tam olarak anlaşılmıyor (Stone ve diğerleri, 2016). Bu nedenle YZ için uygun ve genel kabul gören bir tanımlama kesin olarak verilememiştir ve YZ araştırmacıları hala çözülmemiş zor sorunlar üzerinde çalışmaya devam etmektedirler (McCorduck, 2009).

YZ tanımlamasında olduğu gibi 4IR da farklı şekilde tanımlanabilmektedir. Dördüncü sanayi devrimi olarak da bilinen 4IR, insanlar ve makineler için tamamen yeni yetenekler içeren siber-fiziksel sistemlerin ortaya çıkışı olarak en genel anlamda tanımlanabilir (Schwab 2015). Bu yetenekler üçüncü sanayi devriminin teknolojilerine ve altyapısına bağlıyken, dördüncü endüstri devrimi (4IR) teknolojisinin toplumlara ve hatta nano çiplerle insan vücuduna da gömüldüğü tamamen yeni yolları temsil ediyor (Schwab 2015). 4IR, fiziksel, dijital ve biyolojik dünyalar arasındaki çizgileri bulanıklaştıran teknolojilerin füzyonu olarak tanımlanmaktadır (Schwab 2015; Moloi 2020). 4IR terimi ilk olarak Dünya Ekonomik Forumu'nun kurucusu ve icra başkanı Klaus Schwab tarafından icat edildi. "*4IR bazen yaklaşmakta olan bir fırtına olarak tanımlanır, uzaktan görülebilen, hazırlık için çok az zaman sağlayan bir hızda gelen, kapsamlı bir değişim modeli. Bazı insanlar, değişime cesaret etmek ve etkilerinden yararlanmak için gerekli araçlarla donatılmış zorluklarla yüzleşmeye hazırken, diğerleri bir fırtınanın yaklaştığından bihaber*" (Deloitte 2018a). Dolayısıyla aslında 4IR, günlük yaşamımızın hemen hemen her yönünü etkilemektedir. Bireylerin teknolojiyle ilişkilerini etkileyerek üretim süreçlerini, istihdam biçimlerini ve işin nasıl ve nerede yapıldığını değiştirebiliyor (Schwab 2019). 4IR'ı anlamanın bir başka yolu da bu devrimde kullanılan teknolojiyi takdir etmektir. Teknolojilerden bazıları arasında YZ ve robotik, her yerde bulunan bağlantılı sensörler, sanal ve artırılmış gerçekler, katmanlı üretim, blok zinciri ve dağıtılmış defter teknolojisi, gelişmiş malzemeler ve nanomateryaller, enerji yakalama, depolama ve iletim, yeni hesaplama teknolojileri, biyoteknolojiler, jeomühendislik, nöroteknoloji, uzay teknolojileri. 21. yüzyılda dördüncü sanayi devrimini yönlendiren bunlardan bazılarıdır (Schwab 2019; Moloi 2020).

Bu çalışmamızda endüstri 4.0 (4IR) ile YZ ilişkisi üzerinde durulurken, bu füzyonun getirdiği siber güvenlik risklerine dikkat çekilmekte ve bu alanda alınması gereken önlemler, yapılması gereken çalışmalar ve geliştirilmesi gereken kontroller için analiz ve değerlendirmeler yapılmaktadır. Çalışmamız alandaki literatür bilgisi irdelendikten sonra

güvenlik ile ilgili sorunsal tanımlaması ve değerlendirmesinden sonra alınabilecek makul önlemler için çeşitli çıkarsamalarla sonuçlandırılmaktadır.

2. Araştırma Problemi

Yukarıdaki literatür analizinden de anlaşılacağı üzere, dördüncü sanayi devriminin veya daha yaygın olarak bilinen 4IR'ın ortasındayız. Elbette, büyük bir fırsatla birlikte büyük zorluklar da gelir. 4IR, üretim teknolojilerindeki süper otomasyon bilgisi, etkileşimi ve iletişimine dayanmaktadır. Fikir siber-fiziksel sistemleri, nesnelerin internetini (IoT) ve bulut bilişimini içerir. Esasen 4IR, karanlık ama akıllı fabrika denen şeyi öne sürmektedir. Ayrıntılı olarak açıklamak gerekirse, dijital teknoloji sanayi ve imalat dünyasının çehresini değiştirdi. IoT, YZ ve robotların yakınsaması, diğer gelişmelerin yanı sıra akıllı fabrikaların 4IR'a kuantum sıçramasını da mümkün kılmıştır. Bu, fiziksel ve yazılımın üretimle ve hizmet sektörüyle entegrasyonunu içermektedir. Amazon, Uber, Facebook, "akıllı fabrikalar" ve 3D baskı, yeni sanayi devriminin modern öncüleri arasındadır. 4IR hızla gelişiyor ve yarının dünyasında rekabet edebilmek için teknoloji şirketlerinin zamanla birlikte gelişmesi gerekmektedir.

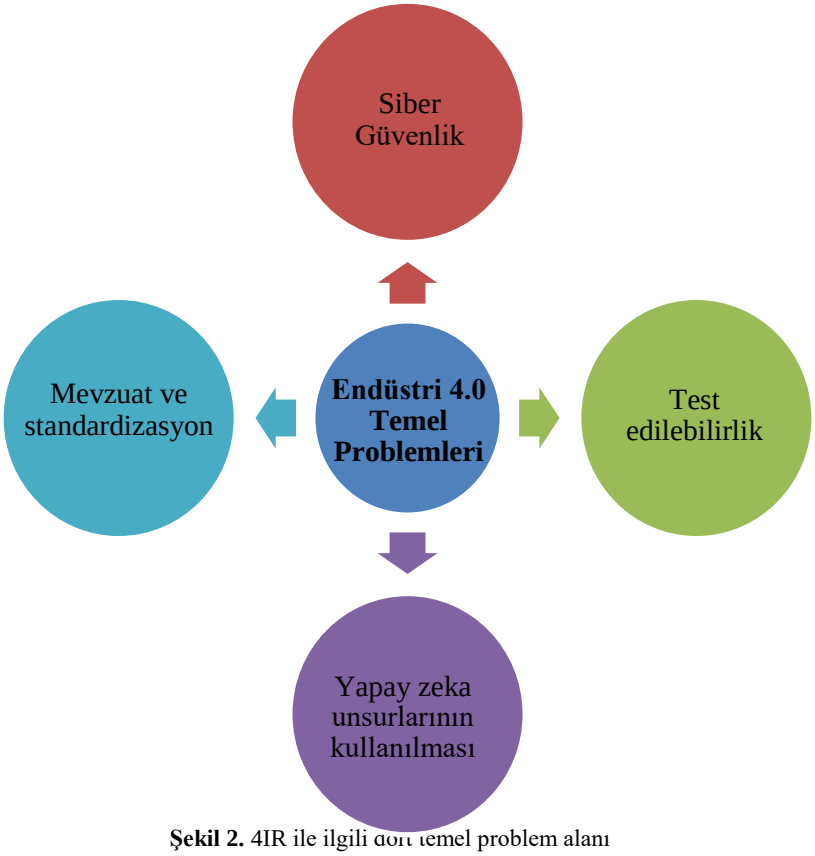
Nesnelerin İnterneti (IoT), makineleri ve sistemleri birbirine bağlayacak ve bir işyerinin tüm departmanlarında kesintisiz veri aktarımına olanak tanıyarak, imalat, bilgi işlem ve diğer birçok sektörde tamamen yeni iş modelleri için fırsatlar oluşturmaktadır. Örneğin başlangıçta basit koruma için kullanılan bir cihaz artık sigorta şirketlerine satılabilen verileri sağlayabilmektedir. Birdenbire, kendi iş modeli tamamen farklı bir hal alabilmektedir. Yarının dünyasında gelişmek ve gerçekten hayatta kalmak için, insanların yukarıdaki zorlukların her birine bakması ve mümkün olan en kısa sürede bunlara göre harekete geçmesi gerekecektir. Ancak, her şeyden önce, 4IR'ın, işletmelerin ve kuruluşların yeni teknolojiler tarafından gerçekleştirilen ara bağlantının gücünü anlayarak yeni bir düşünme zihniyetini benimsemesini gerektirdiğini unutmamak önemlidir. Yeni bir zihniyet benimsemek, şirket kültürünü yenilemek, YZ tabanlı kendi iş modelini uyarlamak, yeni roller oluşturmak ve bu rolleri yerine getirmek için yeteneği beslemek zorluklar ve problem çözme metodolojileri gerektirir. Bu kapsamda en sık sorulan sorular şunlardır:

- *İşletmeniz, 4IR'ın yıkıcı inovasyon etkilerine hazır mı?*
- *Proaktif olarak YZ ile ne tür farklı ölçümler ve önlemler almanız gerekiyor?*

4IR çevremizdeki dünyayla etkileşim şeklimizi değiştirmeye devam ederken yeni zorluklar ortaya çıkmaktadır. İnsanların çok da uzak olmayan bir gelecekte karşılaşabilecekleri başlıca zorluklar şunlardır:

- Yeni iş modelleri ve yeni bir stratejinin tanımı
- Yeni sonuçları en üst düzeye çıkarmak için mevcut organizasyonu ve süreçleri yeniden düşünmek
- Kendi iş durumunu riskler ve fırsatlar çerçevesinde anlamak
- Hazırlık için başarılı pilot çalışmalar yürütmek
- Organizasyonun hangi eylemin gerekli olduğunu anlamasına yardımcı olmak
- Değişiklik ve inovasyon yönetimi ve yönetişimini yapmak,
- YZ gereksinimlerini benimsemek için şirket kültürünün incelenmesi
- Tüm departmanların misyon ve süreçlerinin gerçek bağlantısı
- Yeni yetenekleri işe alma, geliştirme ve tutmak.

Bu bağlamda yukarıda bahsedilen temel sorunları kapsayacak şekil 2'de dört adet problem alanı olduğu söylenebilir. Şekil 2 de temel dört başlıkta asıl problemleri gruplandırabiliriz.



Şekil 2. 4IR ile ilgili dört temel problem alanı

2.1. Siber Güvenlik

2030 lu yıllarda 50 milyar IoT sisteminin anlık olarak haberleşeceği öngörülmektedir. Sistemlerin birbirine bağlanması, endüstriyel dijitalleşmede önemli bir nitelik olabilir. Ancak bu aynı zamanda veri koruma açısından bir güvenlik sorununu temsil etmektedir. Bu veriler, doğrudan, harici bilgisayar korsanlığı saldırılarına karşı ve aynı zamanda, örneğin çalışan hatası veya yetkinlik eksikliğinden kaynaklanan kasıtsız veri sızıntılarına karşı güvence altına alınmalıdır. Siber güvenlik sorunu, işlevsel bir durum (elektrik ve gaz üretimi ve dağıtımı) için kritik olan altyapıların yanı sıra çevresel ve sağlık açısından tehlike riski olan altyapıların (kimya tesisleri, nükleer santraller vb.) yönetilmesi için özellikle önemlidir. (Süzen, 2020)

2.2. Test edilebilirlik

Her yeni sistem veya bir sistemdeki değişiklik, çeşitli durumlarda güvenlik ve güvenilirlik beyanının doğrulanabilmesi için dağıtımdan önce bir endüstri ortamında test edilmelidir. Test, ayrı BT sistemleri çağında bile değişim uygulama sürecinin her zaman kritik bir aşaması olmuştur. IoT sistemlerinin sayı ve fonksiyon olarak akıl almaz bir şekilde artacağı bir gerçeklik iken bunların güvenlik açıkları yönünden test edilebilmesi ve sıfırıncı gün yamalarının yapılabilmesi ayrı bir zorluk olarak karşımıza çıkmaktadır. Bir şirket tamamen entegre edilip dijitalleştiğinde, testler her zamankinden daha karmaşık bir zorluk haline gelmektedir.

2.3. Yapay zekâ unsurlarının kullanılması

4IR ile ilgili olarak en çok tartışılan bir konu, YZ'nin otonom kontrol için yanı sıra akıllı ve öngörücü bakım, kontrol optimizasyonu ve karar alma süreçleri ve son olarak, güvenliği artırmak için örneğin yüz veya konuşma tanıma imkanlarının nitelik ve nicelik olarak ne ölüde kullanabileceğidir. Doğru çalışması için çoğu YZ algoritması, temsili bir veri örneği kullanan bir "öğrenme" veya "eğitim" aşaması gerektirir. Ancak bu tür verileri elde etmek bir başka önemli zorluktur. Bunlar kişisel ve mahrem verilerle temaslı olabilir. Ayrıca doğru öğrenme için yeterli miktarda ilgili veri elde etmek gerekli olmakla kalmaz, aynı zamanda bu verilerin tüm kritik sistem durumlarını yeterince kapsadığı ve böylece tüm sistemin başarılı bir şekilde test edilebileceği kanıtlanmalıdır.

2.4. Mevzuat ve standardizasyon

Endüstriyel otomasyon sektörü, insan sağlığının ve çevrenin korunmasına ilişkin daha katı yasal düzenlemelerle karşı karşıyadır. Dahası, 4IR'ın tek bir standart olmadığını, daha çok hala gelişmekte olan bütün bir standartlar grubunu temsil ettiğinin farkına varmak gerekir.

Bu çalışmamızda ele aldığımız sorunlardan ikisi olan siber güvenlik ve YZ uygulamalarının bir birileriyle yakından ilişkisi olduğu varsayılarak bunlar ile ilgili olarak 4IR bağlamında aşağıda çeşitli inceleme ve değerlendirmeler yapılmaya çalışılmaktadır. Bu bağlamda öncelikle konuyla ilgili literatür taraması yapılmaktadır. Ardından YZ ve 4IR İlişkisi işlenmektedir. Devamında YZ ve Siber Güvenlik İlişkisi üzerinde durulmaktadır. Daha sonra 4IR'da Siber Güvenlik Problemi belirlenmekte ve bunun ne tür çözümlerle giderilmesi gerektiği üzerinde değerlendirmeler yapılmaktadır.

3. Literatür incelemesi

YZ ve 4IR üzerinde pek çok araştırma yapılmış olduğundan literatürde yeterli düzeyde kaynak mevcuttur. "*artificial intelligence*" olarak veri tabanında yapılan aramada 2.220.000 civarında makale çalışması olduğu görülmektedir. "*industry 4.0 artificial intelligence*" kelimeleriyle yapılan aramada ise 128.000 ve "industry 4.0" "artificial intelligence" "*cyber security*" ifadeleri birlikte olarak yapılan aramada ise 3.660 adet ingilizce yayın olduğu tespit edilmiştir. Ancak Türkçe literatürde göreceli olarak çok daha az araştırma olduğu söylenebilir. "*yapay zeka*" olarak yapılan aramada 25.800 civarında, "*endüstri 4.0"* olarak yapılan aramada 2,430, "*endüstri 4.0 yapay zeka*" kelimeleriyle yapılan aramada 1.550 ve "*endüstri 4.0" "yapay zeka" "siber güvenlik"* ifadeleri birlikte olarak yapılan aramada ise sadece 244 adet makale tespit edilmiştir.

YZ ve Endüstri 4.0 (4IR) teknolojilerinin birbirleriyle iç içe oldukları, birbirlerinin ön koşulu gibi kabul edilebilecekleri ve bunların etkili bir şekilde yaygınlaşması için fin-tech denilen dijital finansın da güvenli bir şekilde bütünleşmesi gerektiği literatürde konuşulmaktadır. Çünkü bu teknolojiler dünya nüfusunun ciddi bir oranını ve hatta ülkeleri dışlama potansiyeli göstermektedir. Bu bağlamda Ozili (2018) gibi bazı araştırmacılar dijital finansta, regülasyon ve diğerlerinin yanı sıra hala çözülmesi gereken birçok sorun olduğuna inanmaktadır. Dawei ve ark. (2018), dijital para birimi ve mobil teknoloji aracılığıyla dijital finansal içermenin, sadece 4IR uygulamaları için değil, dünyanın veya ülkenin hizmet verilmeyen bölgelerinde finansal sistemlere girmeye yardımcı olabileceğine inanmaktadırlar. Dijital para birimi ve mobil işlemler de zamanın azaltılmasına ve işlemlerin toplu ve doğru bir şekilde yapılmasına yardımcı olabilir (Dawei ve diğerleri 2018).

Alman hükümeti, dördüncü sanayi devrimi (4IR) olarak adlandırılan imalatın bilgisayarlaştırılmasını teşvik etmeye başladığı zamandan beri bu kavram, üretim sistemlerini önemli ölçüde değiştirmiştir (Schmidt vd., 2015; Pereira vd., 2017). Ancak şirketlerin insan tarafını da hesaba katması gerekir. Operatörler, üretimin çok önemli bir parçası olduğundan tam otomasyonda ihmal edilmemeleri gerekir (Hancock vd., 2013; Roitberg vd., 2014). Cyber-Physical Systems, Internet of Things, IoT, robotik, bulut ve bilişsel bilişim, büyük veri ve artırılmış gerçeklik ile ilişkilendirilen 4IR temel olarak endüstriyel ve bilgi teknolojisine odaklanmaktadır (Munir vd., 2013; Nee ve diğerleri, 2013; Zhou, 2014; Lichtblau vd., 2015; Obitkoet ark., 2015; Gilchrist, 2016; Lanza vd., 2016; Schumacher vd., 2016).

Brezilya, Hindistan, Nijerya ve Kenya ve Zimbabwe gibi diğer Afrika ülkeleri gibi birçok gelişmekte olan ülke, finansal dışlanma sorununun üstesinden gelmek için mobil teknolojiyi benimsemiştir. Sapovadia (2018) çalışmasında, dijital finansal tabana yayılmanın müşterilere tarihsel kayıtlara ihtiyaç duymadan hizmet etmesi açısından geleneksel bankacılıktan farklı olduğunu savunmuştur. YZ ve büyük verinin mevcudiyetinin, alışveriş geçmişi, çevrimiçi davranış modeli, işlem kaydı ve kredi puanlaması için klasik bankacılıkta ortak olmayan diğer birçok potansiyel bilgi kaynağı gibi alternatif bilgilerin kullanımına izin verdiğine inanılmaktadır. Dış ve iç kişilere dolandırıcılıkla mücadele, risk yönetimi, gerçek zamanlı kredi verme ve hedefli pazarlama gibi açık ve her zaman erişilebilir işlevler sağlayan büyük veri örneklerinden biridir. Ek olarak, Levin ve ark. (2018) ayrıca, 1960'lardaki krizin elektronik ticaretin büyümesi, gelişmesi ve finansal hizmetler teknolojisinin geliştirilmesi ihtiyacını doğurduğunu savunmuştur. Araştırmacılar, insanlar yeni döneme hazırlanırken, YZ gibi teknolojinin finans sektöründe önemli olduğuna inanmaktadırlar. Ancak şu anda, Dünya çapında YZ teknolojileri, insan bilişini giderek daha yüksek seviyelerde soyutlama ve adaptasyon yeteneklerinde taklit ediyor. Bu, hala cennet gibi bir dünyada, pazarlama, finans, hukuk, insan kaynakları, operasyonlar ve stratejideki karmaşık görevlerin tam otomasyona geçirilmesi gibi muazzam olasılıkları ortaya koymaktadır (Cox, 2018). ABD'deki işlerin% 47'sinin ve gelişmekte olan ülkelerde daha yüksek bir yüzdesinin YZ gelişmeleriyle risk altında olacağı tahmin edilmektedir (Frey & Osborne, 2016). Bu konuyla ilgili artan endişeler, onu 2016 Dünya Ekonomik Forumu'nun gündemine getirdi. Bununla birlikte, YZ ilerlemesinin etkileri işin doğasındaki değişikliklerin ötesine geçer, aynı zamanda ekonomik mekanizmalar ve iş modelleri ile ilgilidir (Loebbecke & Picot, 2015).

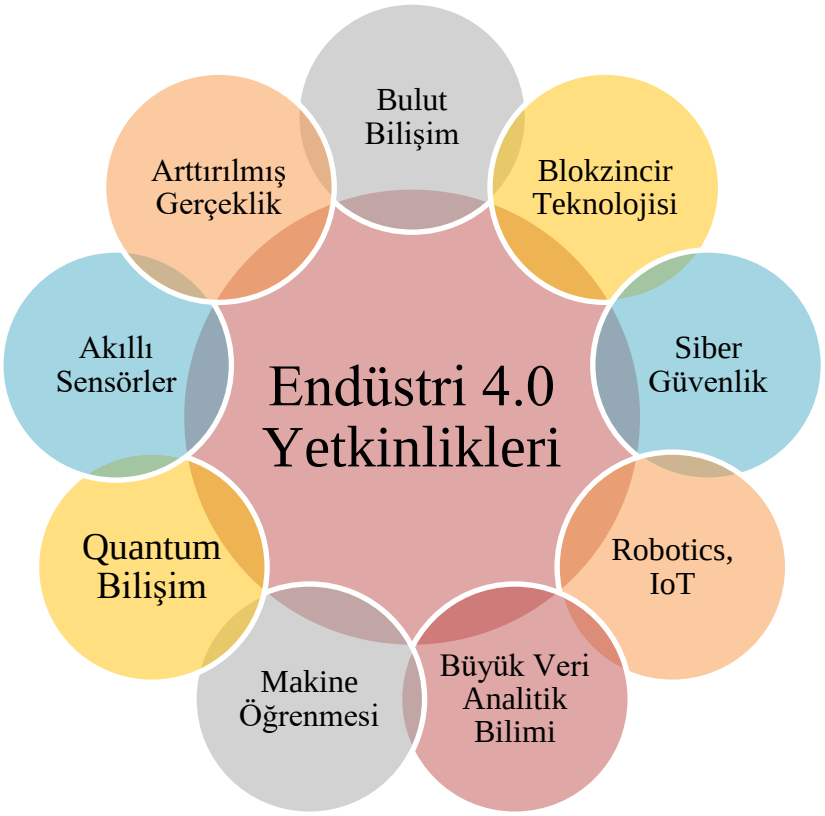
Woodward (1965), üretim teknolojisi, organizasyon yapısı ve örgütsel performansın çoğu zaman ilgi çekici ilişkileri üzerinde durmuştur (Donaldson, 1976). YZ ile ilgili diğer bir tartışma, şirketlerin teknolojik gelişmeleri anlama, benimseme ve bunlardan yararlanma yeteneklerine bağlı olarak nasıl etkileneceklerdir. Bu anlamda, yerleşik şirketler genellikle iş modellerini yeni ekonomik mekanizmalara uyarlamakta zorlanırlar (Loebbecke ve Picot, 2015). Örneğin, çeşitli sektörlerdeki pek çok kullanıcı, aralarında hala kayıplar ve adaptasyon maliyetleriyle karşı karşıya olan geleneksel perakende sektörü de dahil olmak üzere İnternet'e uyum sağlama konusunda sıkıntı çekmektedir. (Townsend, Surane, Orr ve Cannon, 2017). Teknolojinin kullanıcılar tarafından uyarlanması ve beklenmeyen uygulamaların ortaya çıkmasıyla birlikte teknoloji difüzyon etkileri, önemli kazanımlar vaatleriyle sonunda örgütsel alana ulaşan yeni gerçeklikler meydana getirebilmektedir. Örneğin, başlangıçta kişisel bağlantılar dünyasının dijital bir versiyonu olması planlanan ancak kısa süre sonra kuruluşlar tarafından pazarla etkileşim kurmak için bir fırsat (ve kısa süre sonra bir ihtiyaç) olarak görülen sanal sosyal ağın durumu bundan ibarettir.

4IR terimi hem literatürde hem de endüstride yaygın olarak kullanılmaktadır, ancak farklı ülkeler biraz farklı anlamlara sahip farklı ifadeler kullanılabilmektedir. Örneğin, Çin "Çin'de

Üretim 2025" konseptini tanıtırken (Wang ve diğerleri, 2016; Shubin ve diğerleri, 2018), ABD "*yeniden sanayileşme*" terimini kullanıyor ve Japonya farklı bir şekilde "*Yeni Robot Stratejisi*" üzerinden hareket etmektedir. Tüm yaklaşımların amacı aynı olup her strateji, tüm tedarik zincirinin ve üretim sisteminin entegrasyonu yardımıyla tamamen özelleştirilmiş ürünler üretmeyi hedeflemektedir (Huimin vd., 2018; Ford ve diğerleri, 2016). 4IR çok popüler bir araştırma alanı olduğundan literatür incelemeleri çok sık yayınlanmaktadır (Xu ve diğerleri, 2018; Liao ve diğerleri, 2017). 4IR'a odaklanan çok sayıda öğrenme fabrikası, örneğin AutFab veya SEPT kurulmuştur. Her biri farklı bir yöne odaklanırken farklı bir amaçları gözetebilmektedirler (Simons vd., 2017; Elbestawi vd., 2018). Bu alanda öğrenme fabrikalarının mevcut yaklaşımlarını sunan makaleler de yaygındır (Abele vd., 2017; Tisch vd., 2017). Dolayısıyla endüstriyel teknolojideki modern yenilikler, üst düzey bilgi teknolojisi altyapısına ihtiyaç duymaktadır.

4. Yapay zeka ve Endüstri 4.0

Modüler yapılı akıllı fabrikalarda, siber-fiziksel sistemler fiziksel süreçleri izler, fiziksel dünyanın sanal bir kopyasını oluşturur ve merkezi olmayan kararlar alır. Nesnelerin İnterneti üzerinden, siber-fiziksel sistemler birbirleriyle ve insanlarla gerçek zamanlı olarak hem şirket içinde hem de değer zincirinin katılımcıları tarafından sunulan ve kullanılan kurumsal hizmetler genelinde iletişim kurar ve iş birliği yapar. 4IR'da dört tasarım ilkesi vardır. Bu ilkeler, 4IR senaryolarını belirleme ve uygulama konusunda şirketleri destekler (Helmold, 2019). Şekil 3 den de anlaşıldığı üzere, 4IR pek çok farklı alanda yetkinlik gerektirmekte ve bunlardan belki de en önemlisi diğerlerinin de işleyişini etkileyecek olan YZ'dir.



Şekil 3. 4IR ile ilişkili temel alanlar ve tam uygulama için yetkinlik gerektiren konular

Bu yeni teknolojilerin uygulanması, mevcut işgücü arasında beceri eksikliğini getirecektir (Trotta & Garengo, 2018). Bu, endüstriyi mevcut çalışanlarını yeniden vasıflandırmaya yatırım yapmaya veya bu becerileri dışarıdan edinmeye veya iş piyasasından bu teknolojilerde yetenekli yeni bir işgücü işe almaya zorlayacaktır (Aresova ve diğerleri ,2018). Durum, kalifiye bir işgücünde daha yüksek becerilere olan talebi artıracak bu nedenle daha yüksek niteliklere olan talebi artıracaktır (Kagermann, 2014). Dahası, yüksek nitelikli ve düşük nitelikli işgücü arasındaki boşluk önemli ölçüde daha da genişleyecektir. "*İş kutuplaşması*" alanı, Trotta ve Garengo (2018) tarafından da gözlemlenmektedir. İstenilen ve dinamik işgücünün belirlenmesi, işe alınması, eğitilmesi, yeniden eğitilmesi ve elde tutulması, geleceğin akıllı kuruluşlarının insan kaynakları yöneticileri için zorlayıcı olacaktır (Nagy ve diğerleri, 2018; Kumar ve diğerleri, 2020).

Bu nedenle, yeni teknolojilerin sunduğu yeni zorluklar ve fırsatlar, kamu ve iş idaresi için belirli etkilerle birlikte kullanıcılar, araştırmacılar ve uygulayıcılar arasında yansımaları doğurur. YZ söz konusu olduğunda, 4IR veya dördüncü sanayi devrimi olarak bilinen şeyden yararlanmak için akıllı teknolojilerin uygulanmasında organizasyon çalışmaları için umut verici bir yol görülmektedir. Dördüncü devrim ağırlıklı olarak fiziksel, dijital ve biyolojik yapıların, özellikle İnternet ve endüstriyel değer zincirinin (Hermann, Pentek ve Otto, 2016) entegrasyonuna dayanmaktadır ve insanlar, işletmeler ve hükümetler üzerinde önemli etkiler oluşturmaktadır 4IR aynı zamanda YZ'daki gelişmelerle yakından ilişkili olarak görülmektedir (Schwab, 2015; Lee, Davari, Singh ve Pandhare, 2018; China Daily, 2018). Bu da bizi akıllı teknolojilerin birleşmesi üzerine araştırma için büyük fırsatların, insan becerileri ve yeni organizasyonel konfigürasyonlar, rutinler ve beklenen sonuçlar gibi başlıklar altında mevcut olduğunu göstermektedir.

5. Yapay Zeka ve Siber Güvenlik

Siber güvenlik ve YZ arasında çok çeşitli disiplinler arası kesişimler vardır. Bir yandan, derin öğrenme gibi YZ teknolojileri, kötü amaçlı yazılım sınıflandırması ve saldırı tespiti ve tehdit edici istihbarat algısını uygulamak için akıllı modeller oluşturmak için siber güvenliğe dahil edilebilir. Öte yandan, YZ modelleri, örneklerini, öğrenmelerini ve kararlarını rahatsız edecek çeşitli siber tehditlerle karşı karşıya kalacaktır. Bu nedenle, YZ modelleri, rakip makine öğrenimiyle mücadele etmek, makine öğreniminde gizliliği korumak, federe öğrenmeyi güvence altına almak, vb. İçin belirli siber güvenlik savunma ve koruma teknolojilerine ihtiyaç duyar (Trieu & Yang, 2018). Yukarıdaki iki hususa dayanarak, YZ ve siber güvenliğin kesişimini gözden geçirmekte yarar vardır. Son zamanlarda, disiplinlerarası Siber Güvenlik ve YZ alanı bir araya gelmektedir (Nelson vd., 2013; Akusok vd., 2017). Bir yandan araştırmacılar, siber güvenlik suçlarını ve savunmalarını daha akıllı hale getirmek için YZ, özellikle makine öğrenimi ve örüntü tanıma uygularken öte yandan, YZ algoritmalarını korumak için siber güvenlik teknolojileri kullanılmaktadır. Bu arada YZ algoritmalarının kötücül amaçla kullanımı ve saldırı tekniklerini daha sofisitke hale getirebildiği de dikkatlerden kaçmamaktadır (Patel, 2010; Süzen, 2020).

Ağların ve İnternetin büyümesi, kullanıcılar için son derece kolaylık sağlayan birbirine bağlı ve birbirilerini etkileyen bir ortamı sağlamıştır. Bu ara bağlantı sayesinde, bu alanların korunmasına ilişkin zorluklar giderek daha zor hale gelebilmektedir. Endüstriyi ve hükümetleri savunmada başarılı olan geleneksel teknolojiler ve metodolojiler, siber uzayı YZ destekli çok sayıda gelişmiş tehdide karşı başarılı bir şekilde savunmada yetersiz kalıyor. Tüm sektörlerde YZ teknolojiye uygulanmaktadır. Geleneksel siber güvenlik teknolojileri ve metodolojileri, YZ ile geliştirilmiş siber güvenlik sistemleri oluşturmak için YZ teknolojileri veya alt kümeleri Makine Öğrenimi (ML) ve sinir ağları ile de geliştirilmektedir (Masombuka, Grobler ve Watson, 2018).

Siber güvenlik iş gücü açığı büyümeye devam ediyor ve nitelikli siber profesyonellerin mevcudiyetinin önümüzdeki yıllarda azalacağı tahmin ediliyor. Aslında, Uluslararası Bilgi Sistemi Güvenliği Sertifikasyon Konsorsiyumu'ndan bir Siber Güvenlik İş Gücü Çalışması, 2022'ye kadar siber işgücünde 1,8 milyonluk bir eksiklik öngörüyor (ISC2, 2020). Hatta bazı kaynaklar, önümüzdeki iki yıl içinde 3,5 milyondan fazla işçi açığının olduğunu iddia ediyor. Takip edilen sekiz yıllık dönemde, doldurulmamış siber güvenlik işlerinin sayısının 2013'te bir milyondan 2021'de 3,5 milyona çıkarak yüzde 350 artması bekleniyor. Bu pozisyonlara başvuran adayların dörtte birinden daha azı MIT Technology Review'e göre nitelikli sayılıyor (Morgan, 2019). Bu, endüstri için yaklaşan bir sıkıntı ve kasvet gibi görünse de YZ, mevcut siber çalışanları güçlendirirken endişeleri gidermeye yardımcı olabilir. Upwork gibi insan kaynakları sistemleri, kendini kanıtlamış, siber güvenlik ve Doğal Dil İşleme uzmanlarından oluşan büyük havuzlar oluşturmaktadırlar (Upwork, 2021).

Diğer birçok endüstri, insan işçilerin ihtiyacının yerini alan robotik sistemler görse de siber güvenlik için durum böyle görünmüyor. İnsanlar doğru araçlar ile desteklendiklerinde daha fazlasını başarabilirler. Bir ankete göre, İngiltere'deki işlerin %30'u YZ alanındaki gelişmelerden potansiyel olarak tehdit altında. Aynı zamanda, ABD'deki işlerin %38'inin 2030'a kadar modasının geçme riski "yüksek" olarak görülmektedir (Eckerman, 2018). YZ'nin insan davranışını desteklemesine ve tepki vermesine izin vermek, siber profesyonellerin kritik görevlere odaklanmasına, potansiyel tehditleri analiz etmek için uzmanlıklarından yararlanmasına ve bir ihlali giderirken bilinçli kararlar almasına olanak tanır. Otonom siber güvenlik, insanlar olmadan siber güvenlik anlamına gelmez.

YZ, insan karar verme sürecini bilgilendirmeye yardımcı olmak için verileri işleme ve analiz etme ayak işini yapabilir. Bu alanda pek çok eğitim programları da internet üzerinden verilmektedir. Saldırgan, savunma ve adli güvenlik araçlarının sona erdiği yerlerde, insan analistlerinin yarının tehditlerini tahmin etmek, azaltmak ve önlemek için YZ ajanlarından nasıl yararlanabileceği çevrimiçi olarak gösterilmektedir (Hayes, 2021). Güvenlik risklerini yönetmek için tamamen YZ'ya güvenirsek, bu daha fazla güvenlik açığına yol açabilir çünkü bu tür sistemler program önyargıları, istismar ve yanlış veri üretme gibi şeyler için yüksek risklere sahiptir. Siber güvenlik alanındaki hemen hemen herkes, düşmanların bizim kadar zeki olduğu fikrini kabul etmektedirler. En son tehdit algılama ve önleme atılımını incelediğimizde, kötü adamların ondan kaçmak veya bozmak için yollar bulmaya çalıştıklarını görebilmekteyiz. YZ, geleneksel makine öğreniminden (ML) derin öğrenmeye (DL) kadar çeşitli permütasyonlarında bir istisna olmadığından dolayı bu anlamda zafiyetler de vardır (Fralick, 2019). Bununla birlikte, siber ekipler için doğru şekilde kullanılır ve dağıtılırsa, YZ, alaylar için rutin görevleri otomatikleştirme ve iş yükünü hafifletmek için sorumluluklarını artırma yeteneğine sahiptir.

Siber güvenlikte YZ'nin uygulanması, kuruluşların mevcut siber tehditlerden korunmasına ve yeni kötü amaçlı yazılım türlerinin belirlenmesine yardımcı olacaktır. Ayrıca, YZ tabanlı siber güvenlik sistemleri, etkili güvenlik standartları sağlayabilir ve daha iyi önleme ve kurtarma stratejileri geliştirmeye yardımcı olabilir. Kurumsal YZ girişimleri, kötü niyetli yolsuzluk veya eğitim verilerinin manipülasyonu, uygulama ve bileşen yapılandırması dahil olmak üzere çok çeşitli potansiyel güvenlik açıklarına sahiptir. Bu gibi durumlarda, kendi kendine öğrenen, YZ tabanlı bir siber güvenlik yönetim sistemi bu sorunları çözme yeteneğine sahip olmalıdır. Kurumsal bilgi sistemlerinde sürekli ve bağımsız olarak veri toplamak için kendi kendine öğrenen bir sistemi uygun şekilde eğitmek için teknolojiler mevcuttur. Bu veriler daha sonra analiz edilir ve kurumsal saldırı yüzeyiyle ilgili milyonlarca ila milyarlarca sinyal arasında modellerin ilişkilendirilmesi için kullanılır. Ek olarak, siber güvenlikte YZ'dan yararlanmak, konumu veya ağ erişim ayrıcalıklarını değiştiren dinamik,

gerçek zamanlı, küresel bir kimlik doğrulama çerçevesi oluşturmaya yardımcı olur. Sonuç, çeşitli siber güvenlik kategorilerinde insan ekiplerini besleyen YZ seviyeleridir. Bununla birlikte, YZ'nin siber güvenlik alanında insanların yerini alıp almayacağıyla ilgili en büyük endişe ortaya çıkmaktadır. Bu soruyu yanıtlamak için, bir bulut güvenlik şirketi olan Trend Micro'nun yeni raporunda bilgisayar korsanları daha gelişmiş araçlar kullandıkça YZ'nin siber güvenlik alanında 2031 yılına kadar insanların yerini alacağı tahmin edilmektedir (TrendMicro, 2021).

BT liderlerinin yaklaşık %41'inin YZ'nin 2030'a kadar rollerinin yerini alacağına inandığını ortaya koyuyor. Ankete katılanların yalnızca %9'u YZ'nin önümüzdeki on yıl içinde işlerinin yerini almayacağını söyledi. Kabaca %32, YZ'nin sonunda tüm siber güvenliği tamamen otomatikleştirmek için çalışacağını söyledi. %19'u, cephaneliklerini geliştirmek için YZ kullanan saldırganların 2025 yılına kadar sıradan olacağına inanıyor. *'Turning the Tide'* başlıklı rapor, 2020'deki sismik olayların dünya genelinde iş ekosistemlerinde uzun süreli değişiklikler yarattığını ve siber suçluların kötüye kullanabileceği yeni yollar açtığını ortaya koymaktadır. Siber güvenlik, işletmelerin, federal hükümetlerin ve sıradan kullanıcıların 2021'de bu yeni koşullara güvenle uyum sağlamasına yardımcı olacaktır. Yanıt verenlerin beşte biri, hedeflerini iyileştirmek için YZ kullanan saldırganların 2025 yılına kadar sıradan olacağını söyledi. BT liderlerinin dörtte biri, 2030 yılına kadar veri erişiminin biyometrik veya DNA verilerine bağlanarak yetkisiz erişimi imkânsız hale getireceğine inanmaktadır (TrendMicro, 2021).

Telekomünikasyon 2021'de devam edecek ve iş ve kişisel görevlerin tek bir makinede bir araya geldiği karma ortamlar güvenlik açısından zorlayıcı olacak. Raporda, "Kuruluşlar, özellikle de küresel işletmeler, verileri üzerinde daha az kontrole sahip olacak" şeklinde öngörüde bulunulmaktadır. Benzer şekilde verilerin nerede depolandığını ve işlendiğini belirlemek daha zor hale geleceği düşünülmektedir. Kurumsal cihazlara yönelik azalan görünürlük, yalnızca çalışanlar kişisel uygulamalara iş cihazlarından eriştiğinde daha sorunlu hale gelmektedir. Hem kullanıcılar hem de kuruluşlar, evden çalışma kurulumlarını tehditlerden korumak zorunda kalacak ve BT ekipleri tüm uzak iş gücünün güvenliğini sağlamaya ihtiyaç duyacaktır. Öte yandan, bireysel kullanıcı sanal çalışma alanlarını ve uç nokta cihazlarını 2021'de güvence altına almak zorunda kalacaktır (TrendMicro, 2021).

YZ, bilgisayarların veya diğer makinelerin, insanların nasıl öğrendiğine, yorumladığına ve karar verdiklerine benzer şekilde, karmaşık algoritmaların yürütülmesi yoluyla özerk veya neredeyse otonom işlemler, öğrenme ve veri yorumlamasını gerçekleştirmesini sağlayan bir bilgisayar bilimi alanı olarak tanımlanmaktadır. Genel olarak, YZ'nin işlevleri kapsamlıdır ve birden çok teknolojide uygulanmıştır. Bu işlevler şunları içermektedir (Castro ve New, 2016):

- Birincisi, derin öğrenme veya aktarılan öğrenme gibi metodolojileri içeren ve bir bilgisayar veya makinenin daha fazla işlevleri yürütmesine izin veren makine öğrenimi kavramını,
- Ikincisi, siber güvenlik veya ilgili tıbbi alanlar gibi belirli görevleri tamamlamak için gereken kapsamlı bilgiyi temsil eden anlayış kavramını,
- Üçüncü olarak, YZ işlevselliği, diğer işlevleri desteklemek için sorunların tümdengelimli veya nicel bir anlayışından oluşabilen muhakemeyi ve
- Dördüncü olarak, YZ işlevselliği, YZ'nin görevleri gerçekleştirmek veya çevrelerinden öğrenmek için insanlarla veya diğer makinelerle nasıl iş birliği yaptığını ele alan etkileşimi içermektedir.

YZ ve alt kümeleri siber güvenlik sistemlerinde uygulandıkça, araştırmalar özellikle saldırı ve anormallik tespitini, tehdit istihbaratı tüketimini ve diğer kritik ağ savunması alanlarını desteklemede yararlı olduklarını göstermiştir. Bu, genel sistem etkinliğini artırmak için geleneksel teknolojileri geliştirerek veya yeni teknolojilerin uygulanmasıyla elde edilir. Bununla birlikte, YZ ile geliştirilmiş siber güvenlik sistemleri, rakipler tarafından aldatma ve manipülasyondan kaçınmak için iyi geliştirilmiş eğitim uygulamaları ve uygun algoritma geliştirme gerektirir. YZ ile geliştirilmiş siber güvenlik sistemleri, siber savunmada önemli faydalar sağlayarak daha sağlam ve uyarlanabilir bir sistem sağlar; ancak, bu cihazların sınırlamalarını ve bir ağ içinde dağıtımlarının olası etkilerini anlamak için dikkate alınmalıdır.

Yenilikçi BT'nin olumsuz bir yönü olarak, teknolojik gelişmelerin yardımıyla suçlular çok sayıda siber suç işlemek için siber uzayı kullanmaktadır. İnsanlar siber uzaya kendi cihazlarıyla bağlandıkları için, tümü izinsiz girişlere ve diğer çeşitli tehditlere karşı savunmasızdır. İnternet güvenlik araçları gibi temel koruma yöntemleri sadece verileri ve cihazları korumak için yeterli değildir. Etkili ve oldukça gelişmiş siber savunma sistemlerini tanıtmak çok önemli hale gelmiştir. Bugün itibarıyla teknoloji ile birlikte dünya YZ'ye doğru ilerlemektedir (Kaur ve Choudhary, 2017). Akıllı sistemler kullanarak siber savunma sistemleri oluşturmak günümüzde bir trend haline geldi. Temelde akıllı bir aracı, bir ortamda ortaya çıkabilen, kararlar veren, fark etme ve temsil etme yeteneğine sahip bir yazılım bileşenidir.

6. Endüstri 4.0'da Siber Güvenlik Problemi

Nesnelerin interneti (IoT) ve Endüstri 4.0 (4IR) siber güvenlik ile ilgili standartlar ve politika girişimlerinin mevcut görünümü oldukça geniştir ve hem yatay hem de dikey (uygulamaya özgü dağıtımlar, örneğin otomotiv, sağlık ve tüketici) bir şekilde güvenlik yönlerini kapsar. IoT bağlamında, birçok üst düzey referans dokümanın yanı sıra temeller, iyi uygulamalar, kontrol listeleri ve genel rehberlik yayınlanmıştır (Enisa, 2021). Bağlantılı endüstriyel sistemler ve üretim sistemleriyle ilgili olarak, özellikle kılavuz görevi görebilecek faydalı kaynaklar da vardır (Enisa, 2018). Ancak 4IR ve Akıllı Üretim söz konusu olduğunda durum biraz farklıdır. Bu alanların yeni ortaya çıkan doğası göz önüne alındığında, güvenliği bütüncül bir şekilde ele almaya yönelik kapsamlı girişimler geride kalıyor. Bununla birlikte, halihazırda var olan bazı önemli örneklere (IEC 62443 veya IUNO / 4IR kapsamındaki çabalar gibi) atıfta bulunmak önemlidir. Buna göre, ilgili taraflar şu anda 4IR ve Akıllı İmalatın geniş yelpazesi için yalnızca kısmen geçerli olan belgeleri kullanmaktadır (IUNO, 2021).

4IR güvenlik standartları ve bu kapsamdaki girişimleri imalat sektörü için özel bir öneme sahiptir. Büyük imalat şirketlerinin dünya çapında yaygın olarak tesisleri vardır. Buna göre, küresel düzeyde tek tip standardizasyon çabalarının eksikliği, bir kuruluşa ait olan sitelerin iş birliği yapamadığı ve farklı planlara tabi oldukları için güvenlik uzmanlığı ve çözümlerini birbirleriyle paylaşamadığı bir duruma neden olur. Dahası, şirketler arasında güvenli iş birliği de engellenir. Aynı zamanda, çapraz haritalama girişimlerinin gelişmeye başlaması umut vericidir, örn. IoT için ENISA Temel Güvenlik Önerileri, Tüketici IoT Güvenliği için Birleşik Krallık Hükümeti Uygulama Kodu (ETSI, 2020), NIST İç Raporu 8228 (NIST, 2019). Bu tür girişimler IoT güvenliği alanında homojenliğin artmasına katkıda bulunurken, bunları 4IR ekosisteminde genişletmek için daha fazla çalışma yapılması arzu edilmektedir (ENISA, 2018).

4IR cihazlarının, platformlarının ve çerçevelerinin mevcut sistemlere tanıtılması ve entegrasyonu ile birlikte çalışabilirlik konusu gündeme gelmektedir. Endüstriyel ortamlarda,

çeşitli cihazlar arasında ara bağlantının sağlanması, özellikle uzun süredir desteklenmeyen cihazlar düşünüldüğünde genellikle zordur. Bu nedenle, 4IR cihazlarının eski sistemlerle ve birbirleri arasında sorunsuz entegrasyonunu sağlamak için güvenli çözümleri teşvik etmek önemlidir. Örneğin farklı ağlar veya diğer protokoller durumunda şeffaf iletişim sağlamak için ağ geçitleri kullanılabilmektedir. Ayrıca, birlikte çalışabilirlik eksikliği, 4IR cihazları tarafından kullanımda olan özel protokollerle ilgilidir. Farklı satıcılardan cihazların ve platformların kullanılması durumunda, birlikte çalışabilirliği sağlamak her zaman mümkün olmayabilir. Cihazlar/ platformlar arasında birlikte çalışabilirliği sağlamak yalnızca sorunsuz çalışma ile ilgili değil, aynı zamanda güvenlik ile de ilgilidir. Bu nedenle, 4IR çözümlerinin işlevselliğini ve güvenliğini iyileştirmek için her zaman güvenli olmayan ve ortak çerçeveler benimseyen tescilli protokoller sorununu ele almak önemlidir. Son olarak, birlikte çalışabilirlik kavramı yalnızca iletişim protokollerine ve farklı uygulama çerçevelerine atıfta bulunmaz. 4IR'ın karmaşık tedarik zincirlerinde, birlikte çalışabilirlik kavramı ortaya çıkmaktadır; bu, platformlar, cihazlar, protokoller ve çerçeveler arasında ortak, güvenlik temelini sağlamanın çok zor olduğu anlamına gelir. Zincirin en zayıf halkası, tüm zincir üzerinde zararlı etkilere sahip olabilir. Bu nedenle tüm bu unsurlar arasında birleştirici bir ortak siber güvenlik katmanı sağlamak çok zor bir konudur (Süzen, 2020).

4IR'da güvenliğin sağlanmasındaki zorluklar, özellikle eski altyapılarla entegrasyon düşünüldüğünde, bağlı endüstriyel cihazların ve sistemlerin teknik yeteneklerinin eksikliğinden kaynaklanmaktadır. Gösterge olarak aşağıdaki sınırlamalar dikkate alınabilir:

- Sınırlı işlem yetenekleri ve cihazın uygun bir boyut ve rekabetçi fiyatını korurken uzun bir çalışma süresi sağlama ihtiyacı, tasarım aşamasında kapsamlı güvenlik özelliklerinin uygulanmasını önemli ölçüde etkiler.
- 4IR cihazları tasarlarken temel koruma mekanizmalarının dikkate alınmaması, güvenliklerini olumsuz yönde etkiler. Yaygın olarak yapılan yama ve yazılım güncellemeleri, çoğu durumda, söz konusu işlevselliği desteklemedikleri için düşük kaliteli cihazlar söz konusu olduğunda uygun çözümler değildir.
- Örneğin, şifreleme veya kimlik doğrulama gibi daha gelişmiş güvenlik önlemlerinin olmaması, endüstriyel sürece en yakın cihazların koruma düzeyini düşürür. Yalnızca ağın güvenliğini sağlamaya yönelik oldukça yaygın bir yaklaşım yetersizdir, örn. bir saldırgan ağa girerse, cihazlar saldırılara açık hale gelir.

Son olarak, sınırlı teknik yeteneklerle ilgili boşlukları değerlendirirken, 4IR sistemleri için özel siber güvenlik araçlarının genellikle çok az veya çok pahalı olduğu gerçeğinden bahsetmeye değer. Tam otomasyon ortamında ağ izleme, otomatik varlık keşfi ve yapılandırma ve değişiklik yönetimi araçları, bu tür sistemlerin güvenlik düzeyini ve kullanılabilirliğini artırmıştır. Bununla birlikte, bu tür araçlar, yeni 4IR cihazlarını kullanmak için henüz tam olarak hazır değil, bu nedenle güvenlik açısından bir boşluk oluşturmaktadır. 4IR dünyasına uyarlanmış güvenlik çözümleri geliştirerek bu tür zorlu sorunları ele almak gerekmektedir.

4IR'dan önce siber saldırılar, teknoloji tabanlı kurum ve kuruluşlar için önemli sorunlar arasındaydı. Bununla birlikte, 4IR ile birlikte, bu güvenlik sorunları daha spesifik sorunlar haline geldi ve otomasyon kavramı, güvenlik konularına yeni paradigmalar eklemiştir. Sonuç olarak, genel olarak siber tehditlerin mağduriyeti artmıştır. Bu bağlamda 4IR bazında meydana gelmesi beklenen değişikliklerle birlikte şu hususlar ileri sürülebilir (Ateş ve diğerleri, 2020) Nesnelerin İnterneti sayesinde her nesnenin ağ bağlantısına açık olması üretim maksimizasyonu sağlayacak ancak güvenlik kusurlarına da neden olabilir:

- Büyük veri kavramı ile akıllı fabrikalar varlığında talep durumu, Üretim ve pazarlama ile ilgili verilerin analizi artacaktır.
- Nesnelerin İnterneti üzerinden toplanan büyük verilerin, fiziksel veya sanal ortamlarda bulut sistemlerinde saklanması güvenlik açıklarına neden olabilir.
- Veri güvenliğini artırmak için alınan tedbirlerle kriptolojinin önemi artacaktır.
- Güvenlik ekipleri tarafından alt düzeyde gerçekleştirilen veri analizleri büyük veri kavramı ile büyük bir düzeye ulaşacaktır ve güvenlik ekipleri şu anda bu alanda çalışmak için yeterli değildir (büyük veri üzerinde görüntü almak çok zor ve maliyetli olacaktır çünkü Görüntü almadan veriler üzerinde analiz yapmak farklı risk unsurlarına sahiptir, konu belirsiz kalır.)
- Nesnelerin interneti teknolojisine sahip maddeler, suçun çözümü için adli tıp açısından fiziksel izlerden daha fazla potansiyele sahiptir.
- Otomasyon sistemine bağlı üretim hatları ve dijital tedarik ağları için uzaktan komuta ederek imhayı mümkün kılan yeni siber riskler ortaya çıkabilir.
- Gerçek ve sanal dünya arasındaki sınırların kademeli olarak kaldırılmasıyla birlikte siber-fiziksel üretim sistemleri (Cyber Physical Systems) olarak bilinen alanlar daha bulanık hale gelecektir.
- Üretim tesislerinde oluşabilecek bir güvenlik açığı, toplumda kendine yer bulma kaygısı taşıyan bazı terör örgütlerine siber terör eylemleri yapma imkânı sağlayacaktır.
- Bulut depolama hizmetlerinin farklı ülkelerde faaliyet gösteren firmalara verilmesi durumunda, bulut depolama verileri üzerinde yapılacak adli analizler endişe yaratacağı için birden fazla ulus devlet yargı sistemini içerebilen bir yapıya ihtiyaç duyulacaktır.
- Teknolojinin sürekli değişmesine paralel olarak, güvenlik ekiplerinin teknik bilgi ihtiyacı gün geçtikçe artacak, siber suçlar daha karmaşık hale gelecek ve çözümü daha zor hale gelecektir.

7. Sonuç

Geleneksel siber güvenliğin mimarları, doğruluk, erişim kontrolü, gizlilik, inkar edememe ve bütünlük gibi hizmetler sunacak güvenlik mekanizmaları gerektirir. Bu nedenle, bu mekanizmaların mevcut olması, belirli bir ağa veya bilgisayara saldırı ve izinsiz girişleri önlemede kritik öneme sahiptir. Günümüz dünyasında, 4IR, bulut bilişim, YZ, bilişsel bilgi işlem, nesnelerin interneti ve siber-fiziksel sistemler aracılığıyla sistemlerin otomasyonu gibi bugün insanların hoşlandığı hemen her yönüyle belirleyici faktörlerdir (Doinea & Pocatilu, 2014) Bununla birlikte, modern internetin kapsayıcı bir şekilde ele geçirildiği çağdaş endüstrilerde, bu modern endüstrilerin görünümü, sürekli olarak değişen, hacimli, ısrarcı, oldukça sofistike ve süper hızlı olarak nitelendirilebilen saldırılarla ilişkilendirilir. Bu nedenle, bir siber tehditte bu tür özelliklere sahip olmak, çeşitli önleyici tedbirlerin zorluğunu artıracaktır (Zota & Petre, 2014).

Bu çalışmada, YZ ve 4IR hakkındaki siber güvenlik perspektifleri hakkında kapsamlı bir çalışma yapılmış ve özünü en basit ifadelerle yakalamaya çalışılmıştır. 4IR'ın benimsenmesinin ardından yakın gelecekte, herkes düz bir platformda, YZ'ye dayalı siber güvenlik risklerini tehlikeye atarken, ucuz işgücünün avantajı artık gelişmekte olan ülkeler lehine olmayacaktır. Önümüzdeki üretim çağında ayakta kalabilmek için endüstrilerin,

değişen müşteri zevkine ve talebine göre yenilikçi ve kişiselleştirilmiş ürünleri kısa sürede, ekonomik ve verimli bir şekilde tasarlama ve üretme yeteneklerini geliştirmeleri gerekiyordu. Bu, tüm üretim ortamını, beceri setinin gerekliliğini, eğitim uygulamalarını ve hizmetleri, vb. yeniden tanımlayacaktır. 4IR karmaşık ve yıkıcı olmasına rağmen kaçınılmazdır, yine de dünyadaki hiçbir ülke kendisini benimsemekten çekemeyeceğinden her ülke ve her endüstri bunu benimsemek zorundadır.

"Türkiye, her ne kadar bir tarım ülkesi ise de tüm sektörlerde emek-yoğun çalışmalardan teknoloji-yoğun çalışmalara geçişin en kısa sürede tamamlanması gerekmektedir. Çağımızda endüstri 4:0 yapay zekâ konuşulurken bu ilerlemenin gerisinde kalınmamalıdır" (Boz Yılmazer ve Tunalıoğlu, 2020). "*Atı alan Üsküdar'ı geçti*" misali başlıca sanayileşmiş ülkeler, bunun uygulanmasına yönelik büyük adımları atmaya çoktan başlamıştır. Amazon, Boing, Google, Facebook gibi bazı Sektörler, gündelik operasyonlarında YZ ile aşılanmış 4IR konseptini ve araçlarını uygulamaya başladı ve diğerleri de bunları takip etmeye çalışmaktadırlar. Makine öğreniminin endüstriyel uygulaması için beklentiler oldukça yüksektir. Gereksinimleri karşılamak, endüstriyel ortaklar için gerçek bir zorluktur. Bir yandan eğitim algoritmaları çok sayıda temiz, önyargısız veri kümesi gerektirir, aksi takdirde eğitimin ve dolayısıyla YZ tarafından verilen kararların sonucu yanlı olabilmektedir. Öte yandan, siber güvenlik, bağlantılı teknolojilerin kullanımının artmasıyla birlikte dikkate alınması gereken bir başka tehdit olarak değerlendirilmektedir. Bu kapsamda yapılan analiz ve değerlendirmeler sonucunda güvenlik ile ilgili olarak aşağıdaki önlemlerin gerekli olduğu sonucuna varılabilmektedir:

1. Siber güvenliğin birlikte çalışabildiği 4IR temellerini kurmak için öncelikli olarak kurumsal stratejilere girişilmelidir.

Güvenlikle birlikte çalışabilirliğin zorluğu, özellikle eski sistemlerle entegrasyon düşünüldüğünde 4IR ekosistemiyle ilgilidir. Birlikte çalışabilirlik ve güvenlik sorunlarının çoğu, farklı üreticilerden ve farklı iletişim protokollerinden gelen cihazların (hem kritik hem de kritik olmayan üretim bileşenleri) birbirine bağlanmasından kaynaklanmaktadır. Endüstri 4,0 cihazlarının, platformlarının ve çerçevelerinin birlikte çalışabilirliğinin yanı sıra güvenlik uygulamalarının sağlanması ve teşvik edilmesi bu nedenle çok büyük önem arz etmektedir. Güvenlikle birlikte çalışabilirlik için Endüstri 4,0 temellerini oluşturmak için şunlar önerilebilmektedir:

- Ortak bir güvenlik dilini ve Endüstri 4,0 bileşenleri için protokollerin kullanımını teşvik eden birlikte çalışabilirlik çerçevelerinin[2] kullanımını teşvik edilmelidir. Bu kapsamda bölgesel kalkınma planları, yenilik stratejileri ile kurumsal stratejik planları yeniden yapılandırılmalıdır.
- Kişiler, süreçler ve teknolojiler olmak üzere üç siber güvenlik unsurunu da kapsayacak şekilde tedarik zincirindeki iş birliği ortakları ve şirketler arasındaki belirli güvenlik seviyeleri belirlenmelidir.
- Açık ve erişilebilir birlikte çalışabilirlik laboratuvarlarını ve güvenlik için test merkezlerini teşvik etmek gerekir.

2. 4IR Güvenliğini Garanti Etmek İçin Sofistike Teknik Önlemler Uygulanmalıdır.

Ekosistemin karmaşıklığı ve ölçeklenebilirliği göz önüne alındığında, IoT ve 4IR güvenliği için tüm çözümlere uyan tek bir çözüm yoktur. Çözümleri birleştirmek ve bu çözümlerin,

[2] Örneğin bu yöndeki dikkate değer çerçeveler, NIST Siber Güvenlik Çerçevesi ve IEC 62541'i (OPC UA) incelenebilir.

güvenlikten ödün vermeden esneklik ve genişletilebilirlik sağladığından emin olmak ve aynı zamanda kullanılabilirlik faktörünü de hesaba katmak meselesidir. Bu bağlamda esneklik kavramı aynı zamanda siber güvenlik ekonomisine de atıfta bulunulmalıdır. Yani benimsenen çözümlerin sistemik bir maliyet-fayda analizinin bir sonucu olarak gelmesi gerekir ki burada faydası açıkça etkili ve güvenilir ürünler ve hizmetlerdir. Risk analizine dayalı olarak 4IR bileşenleri, hizmetleri ve süreçleri için temel güvenlik önerilerini belirlemek, bu alanın zorlu teknik kısıtlamalarına bir çözüme yaklaşmanın ilk adımını oluşturmaktadır. 4IR güvenliğini sağlamak için teknik önlemlerin uygulanması açısından aşağıdaki önlemeler önerilebilmektedir:

- Metodolojik bir risk değerlendirmesini dikkate alarak 4IR için yerli ve milli bir güvenlik mimarisi tanımlanmalıdır.
- Tüm 4IR bileşenleri, YZ destekli YBS uygulamaları, cihazları, hizmetleri, protokolleri, iletişimleri ve süreçleri için tasarım gereği güvenlik ve tasarım gereği gizlilik ilkelerini ve varsayılan olarak uygulanmalıdır.
- Uygulanan siber güvenlik çözümlerinin olgunluğunu periyodik olarak değerlendirmek ve devam eden ve ortaya çıkan tehdit ortamını izlemek için siber tehdit istihbaratını da göz önünde bulundurmak için iç denetim ve teftiş kurullarının yıllık programlarının yeniden güncellenmesi gerekir.
- 4IR dağıtımlarıyla ilgili endüstrilerin siber güvenlik duruşunu izlemek, ayrıca eski sistemler ve altyapılar için süreç adımlarının geliştirilmesi gerekir.
- Yol gösterici ilke olarak organize sanayi bölgeleri, teknoparklar, üniversiteler, sanayi odaları ile kalkınma ajansları gibi kilit kurumlar arasında verimli ve etkili bir ortak çalışma ile, 4IR bileşenlerinin ve hizmetlerinin yaşam döngüleri boyunca sürekli güncellenebilirliği ve yükseltilebilirliği sağlanabilmelidir.
- Siber güvenlik standartlarındaki gelişmeleri ve 4IR siber güvenlik için en iyi uygulamaları takip etmek ve gereksiz işlevselliği kaldırmayı da göz önünde bulundurarak risk değerlendirmesine tabi ilgili güvenlik önlemlerinin uygun şekilde uygulanmasını sağlamak gerekir.

Kaynakça

ABELE, E., CHRYSSOLOURİS, G., SİHN, W., METTERNİCH, J., ELMARAGHY, H., SELİGER, G., SİVARD, G., ELMARAGHY, W., HUMMEL, V., TİSCH, M., SEİFERMANN, S. (2017). Learning factories for future-oriented research and education in manufacturing, CIRP Annals, 66(2) 803–826.

ANTON A, EİROLA E, BJORK K, MİCHE Y, JOHNSON H, and LENDASSE A (2017) Brute-force Missing Data Extreme Learning Machine for Predicting Huntington's Disease, PETRA'17 (Proceedings of the 10th International Conference on Pervasive Technologies Related to Assistive Environments), Pages 189-192.

ARESOVA P., SOUKAL I., SVOBODOVA L., HEDVİCAKOVA M., JAVANMARDİ E., SELAMAT A., KREJCAR O., (2018) Consequences of Industry 4.0 in business and economics, Economics, 6, 46, 1–4, doi: 10.3390/

ATEŞ E. C., BOSTANCİ E., GUZEL M. S. (2020) Security Evaluation of Industry 4.0: Understanding Industry 4.0 on the Basis of Crime, Big Data, Internet of Thing (IoT) and Cyber Physical Systems, Güvenlik Bilimleri Dergisi 9 (Special Issue): 29-50 https://www.researchgate.net/publication/ 339642922

BOZ YILMAZER, E, TUNALIOĞLU, R. (2020). Teknokentler ve Agroparklar (Türkiye)-Technocents and Agroparks (Turkey). Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 7 (2), 133-150. DOI: 10.30803/adusobed.816595

CHİNA Daily. (2018) *AI seen as driving force in industry 4.0*. Retrieved from http://www.chinadaily.com.cn/a/201804/27/WS5ae29547a3105cdcf651ae80.html

COX, C. (2018) *Autonomous exchanges: Human-machine autonomy in the automated media economy* (Doctoral dissertation). Department of Moving Image Studies, Georgia State University, Atlanta, GA, USA.

DAWEİ, Liu, HU Anzi, and Lİ Gen (2018) Big Data Technology: Application and Cases. In Handbook of Blockchain, Digital Finance, and Inclusion. Amsterdam: Elsevier Inc., pp. 65–82.

DOİNEA M. and POCATİLU P., (2014) Security of Heterogeneous Content in Cloud-Based Library Information Systems Using an Ontology-Based Approach, Informatica Economică, vol. 18, no. 4. 101-110.

DONALDSON, L. (1976). Woodward, technology, organizational structure and performance- A critique of the universal generalization. *Journal of Management Studies, 13*(3), 255-273. https://doi.org/10.1111/j.1467-6486.1976.tb00902.x

ECKERMAN, M., (2018) Robots Replacıng Humans – These 6 Industrıes Started Already, GFL, https://www.globalfemaleleaders.com/blog/robots-replacing-humans/

ELBESTAWİ, M., CENTEA D., SİNGH, I., WANYAMA, T. (2018). SEPT Learning Factory for Industry 4.0 Education and Applied Research, Procedia Manufacturing, 23, 249–254

ENİSA, (2018) Good Practices for Security of Internet of Things in the context of Smart Manufacturing, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/at_download/fullReport

ENİSA, (2021) ENISA Good practices for IoT and Smart Infrastructures Tool, https://www.enisa.europa.eu/iot-tool

ETSI, (2020) Cyber Security for Consumer Internet of Things, ETSI EN 303 645 V2.1.1 (2020-06), https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

FRALİCK, C., (2019) Artificial Intelligence in Cybersecurity Is Vulnerable, SC Media, https://www.scmagazine.com/home/opinion/artifical-intelligence-in-cybersecurity-is-vulnerable/

FREY, C. B., & OSBORNE, M. A. (2016) *Technology at work v2.0: The future is not what it used to be*. City GPS: Global Perspective & Solutions.

GİLCHRİST, A. (2016). Industry 4.0: The Industrial Internet of Things; Apress: Berkeley, CA, USA.

HANCOCK, P.A., Jagacinski, R.J., Parasuraman, R., Wickens, C.D., Wilson, G.F., Kaber, D.B. (2013). Human-automation interaction research: Past, present, and future. Ergon. Des., 21, 9–14.

HAYES, B., (2021) How Gamification, Artificial Intelligence, and Reinforcement Learning Will Revolutionize Cyber Skill Acquisition, Circadence Webinar, https://marketing.circadence.com/acton/media/36273/webinar-how-gamification-ai-will-revolutionize-cyber-skill-acquisition

HELMOLD M. (2019) Industry 4.0 and Artificial Intelligence (AI) in PM. In: Progress in Performance Management. Management for Professionals. Springer, Cham. https://doi.org/10.1007/978-3-030-20534-8_13

HERMANN, M., PENTEK, T., & OTTO, B. (2016). Design principles for industry 4.0 scenarios. *Proceedings of the Hawaii International Conference on System Sciences*, IEEE, Koloa, HI, USA, 49. https://doi.org/10.1109/HICSS.2016.488

HUİMİN, M., WU, X., YAN, L., HUANG, H., WU, H., XİONG, J., ZHANG, J. (2018). Strategic Plan of "Made in China 2025" and Its Implementation. In Analyzing the Impacts of Industry 4.0 in Modern Business Environments; IGI Global: Derry Township, PA, USA, Volume 23, pp. 1–23.

ISC2, (2020), Cybersecurity Professionals Stand Up to a Pandemic, Cybersecurıty Workforce Study, https://t.ly/PFoS

IUNO, (2021) IT security in Industry 4.0, https://iuno-projekt.de/

KAGERMANN H., (2014) Chancen von Industry 4.0 nutzen, [in:] Industry 4.0 in Produktion, Automatisierung und Logistik. Wiesbaden: Springer, pp. 603–14,.

KAUR A., CHOUDHARY D. (2017) Cyber Awareness Improvement Using Artificial Intelligence, International Journal For Technological Research In Engineering Volume 4, Issue 9

KUMAR S., SUHAİB M., ASJAD (2020) Industry 4.0: Complex, Disruptive, But Inevitable Management and Production Engineering Review Volume 11 • Number 1 • March • pp. 43–51 DOI: 10.24425/mper.2020.132942

LANZA, G., NYHUİS, P,; ANSARİ, S.M., KUPRAT, T., LİEBRECHT, C. (2016). Befähigungs-und Einführungsstrategien für Industrie 4.0. ZWF Zeitschrift Wirtschaftlichen Fabrikbetrieb, 111, 76–79.

LEE, J., DAVARİ, H., SİNGH, J., & PANDHARE, V. (2018). Industrial artificial intelligence for industry 4.0-based manufacturing systems. *Manufacturing Letters, 18*, 20-23. https://doi.org/10.1016/j.mfglet.2018.09.002

LEVİN, Richard B., PETER Waltz, and HOLLY LaCount (2018) Betting Blockchain Will Change Everything-SEC and CFTC Regulation of Blockchain Technology. In Handbook of Blockchain, Digital Finance, and Inclusion. Amsterdam: Elsevier Inc., pp. 187–212

LİAO, Y., DESCHAMPS, F., de Freitas Rocha LOURES, E., RAMOS, L.F.P. (2017). Past, present and future of Industry 4.0—A systematic literature review and research agenda proposal. Int. J. Prod. Res., 55, 3609–3629.

LİCHTBLAU, K., STİCH, V., BERTENRATH, R., BLUM, M., BLEİDER, M., MİLLACK, A., SCHMİTT, K., SCHMİTZ, E., SCHROTER, M. (2015). Industrie 4.0 Readiness. Impuls-Stiftung des VDMA Aachen-Köln, 52, 1–77.

LOEBBECKE, C., & PİCOT, A. (2015). Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. *Journal of Strategic Information Systems, 24*(3), 149-157. https://doi.org/10.1016/j.jsis.2015.08.002

LYNCH, S. (2017). *Andrew Ng: Why AI is the new electricity*. Retrieved from https://www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity

MCCORDUCK, P. (2009). *Machines who think: A personal inquiry into the history and prospects of artificial intelligence*. Wellesley, MA, USA: AK Peters/CRC Press.

MOLOİ, David MHLANGAAND Tankiso. (2020) COVID-19 and the Digital Transformation of Education: What we are learning in South Africa. Preprints

MORGAN, S., (2019) Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021, Cybercrime Magazine, https://cybersecurityventures.com/jobs/

MOSUMBUKA M., GROBLER M., WATSON B., (2018) Towards an Artificial Intelligence Framework to Actively Defend Cyberspace, 17th European Conference on Cyber Warfare and Security (ECCWS), Aslo, Norway

MUNİR, S., STANKOVİC, J.A., LİANG, C.J.M., LİN, S. (2013). Cyber Physical System Challenges for Human-in-the-Loop Control. In Proceedings of the Presented as part of the 8th International Workshop on Feedback Computing, USENIX, San Jose, CA, USA, 24–28 June 2013; Volume 4, pp. 1–4.

NAGY J., OL'AH J., ERDEİ E., M'AT'E D., POPP J., (2018) The role and impact of Industry 4.0 and the Internet of Things on the business strategy of the value chain – the case of Hungary, Sustainability, 10, 3491, doi: 10.3390/su10103491.

NEE, A.Y., ONG, S.K. (2013). Virtual and Augmented Reality Applications in Manufacturing. IFAC Proc. Vol. 2013, 46, 15–26.

NELSON Blaine, CHRİSTOS Dimitrakakis, and ELAİNE Shi (2013) Summary/Overview for Artificial Intelligence and Security, AISec '13 (Proceedings of the 2013 ACM SIGSAC conference on computer and communications security), Pages 1483- 1484.

NIST, (2019) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf

OBİTKO, M., Jirkovský, V. (2015) Big Data Semantics in Industry 4.0. In Industrial Applications of Holonic and Multi-Agent Systems; Springer International Publishing: New York, NY, USA, pp. 217–229.

OZİLİ, Peterson K. (2018) Impact of digital finance on financial inclusion and stability. Borsa Istanbul Review 18: 329–40.

PATEL Kayur (2010) Lowering the Barrier to Applying Machine Learning, CHI EA'10 (CHI'10 Extended Abstracts on Human Factors in Computing Systems), Pages 2907-2910.

PEREİRA, A., ROMERO, F. (2017). A review of the meanings and the implications of the Industry 4.0 concept. Procedia Manuf., 13, 1206–1214

ROİTBERG, A., PERZYLO, A., SOMANİ, N., GİULİANİ, M., RİCKERT, M., KNOLL, A. (2014). Human activity recognition in the context of industrial human-robot interaction. In Proceedings of the Signal and Information Processing Association Annual Summit and Conference (APSIPA), Siem Reap, Cambodia, 9–12 December 2014; Volume 10, pp. 1–10.

SAPOVADİA, Vrajlal. (2018) Financial Inclusion, Digital Currency, and Mobile Technology. In Handbook of Blockchain, Digital Finance, and Inclusion. Amsterdam: Elsevier Inc., pp. 361–85.

SCHMİDT, R., MÖHRİNG, M., HÄRTİNG, R.C., REİCHSTEİN, C., NEUMAİER, P., JOZİNOVİ´c, P. (2015). Industry 4.0-potentials for creating smart products: Empirical research results. In International Conference on Business Information Systems; Springer: Cham, Germany, Volume 12, pp. 16–27.

SCHUMACHER, A., EROL, S., SİHN, W. (2016). A maturity model for assessing industry 4.0 readiness and maturity of manufacturing enterprises. Procedia CIRP, 52, 161–166.

SCHWAB, K. (2015). The fourth industrial revolution: What it means and what to respond. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution

SCHWAB, Klaus. (2019). Davos Manifesto 2020: The Universal Purpose of a Company in the Fourth Industrial Revolution, World Economic Forum. Available online: http://www.worldacademy.org/files/global_leadership/papers/Davos_Manifesto_2020.pdf

SHUBİN, T., ZHİ, P. (2018). "Made in China 2025" and "Industrie 4.0"—In Motion Together. In The Internet of Things; Springer: New York, NY, USA, pp. 87–113.

SİMON, H. A. (1995). Artificial intelligence: An empirical science. *Artificial Intelligence, 77*(1), 95-127. https://doi.org/10.1016/0004-3702(95)00039-h

STONE, P., BROOKS, R., BRYNJOLFSSON, E., CALO, R., ETZİONİ, O., HAGER, G., et al. (2016). *Artificial intelligence and life in 2030*. Retrieved from https://ai100.stanford.edu/sites/default/files/ai_100_report_0831fnl.pdf

SÜZEN, A.A. (2020). A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem. International Journal of Computer Network and Information Security, 12, 1-12.

SWEENEY, L. (2003). *That's AI? A history and critique of the field* (Technical Report CMU-CS-03-106). Carnegie Mellon University, School of Computer Science, Pittsburgh, PA, USA. Retrieved from https://dataprivacylab.org/projects/thatsai/paper.pdf

TİSCH, M., METTERNİCH, J. (2017). Potentials and limits of learning factories in research, innovation transfer, education, and training, Procedia Manufacturing, 9, 89–96.

TOWNSEND, M., SURANE, J., ORR, E., & CANNON, C. (2017). *America's "retail apocalypse" is really just beginning*. Retrieved from https://www.bloomberg.com/graphics/2017-retail-debt/

TRENDMİCRO, (2021). Turning The Tide, TrendMicro Security Predictions for 2021, TrendMicro Reports, https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2021

TRİEU, Khoa and YANG, Yi, (2018). Artificial Intelligence-Based Password Brute Force Attacks, MWAIS 2018 Proceedings. 39. http://aisel.aisnet.org/mwais2018/39

TROTTA D., GARENGO P., (2018) Industry 4.0 key research topics: A bibliometric review, 7th International Conference on Industrial Technology and Management, pp. 113–117.

UPWORK, (2021) Hire the best Natural Language Processing specialists, https://www.upwork.com/hire/natural-language-processing-freelancers/

WANG, S., WAN, J., ZHANG, D., Lİ, D., ZHANG, C. (2016). Towards smart factory for industry 4.0: A self-organized multi-agent system with big data based feedback and coordination. Comput. Netw., 101, 158–168.

WOODWARD, J. (1965). *Industrial organization: Theory and practice*. London, UK: Oxford University Press.

XU, L.D., XU, E.L., Lİ, L. (2018). Industry 4.0: State of the art and future trends. Int. J. Prod. Res., 56, 2941–2962.

ZHOU, J., LEPPANEN, T., HARJULA, E., YLİANTTİLA, M., OJALA, T., YU, C., JİN, H., YANG, L.T. (2014). Cloudthings: A common architecture for integrating the internet of things with cloud computing. In Proceedings of the Computer Supported Cooperative Work in Design (CSCWD), Hsinchu, Taiwan, 21–23 May 2014; pp. 651–657.

ZOTA R. D., PETRE I. A., (2014) An Overview of the Most Important Reference Architectures for Cloud Computing, Informatica Economică, vol. 18, no. 4, 26-39.