AÇIK VE UZAKTAN ÖĞRENMEDE SİBER GÜVENLİĞİN TEKNİK DESTEK HİZMETLERİ KAPSAMINDA İNCELENMESİ

Yüksek Lisans Tezi

Sehla ERTAN

Eskişehir 2022

AÇIK VE UZAKTAN ÖĞRENMEDE SİBER GÜVENLİĞİN TEKNİK DESTEK HİZMETLERİ KAPSAMINDA İNCELENMESİ

Sehla ERTAN

YÜKSEK LİSANS TEZİ

Uzaktan Eğitim Anabilim Dalı
Danışman: Prof. Dr. T. Volkan YÜZER
İkinci Danışman: Arş. Gör. Dr. Hakan KILINÇ

Eskişehir
Anadolu Üniversitesi
Sosyal Bilimler Enstitüsü
Mart 2022

JÜRİ VE ENSTİTÜ ONAYI

ÖZET

Yaşam boyu öğrenme felsefesi çatısı altında öğrenmenin herkes için eşitlikçi bir politikayla zaman ve mekân gözetmeksizin sürdürülmesini sağlayan açık ve uzaktan öğrenme faaliyetleri; farklı bireylerin, toplumların ve sistemlerin beklenti ve ihtiyaçlarını karşılamayı hedeflemektedir. Öğrenme ile ilgili tüm faaliyetlerde farklılaşan beklenti ve ihtiyaçların desteklenmesini kapsayan destek hizmetleri, öğrenme süreçlerine ve bu süreçlere dahil olan farklı paydaşlara hizmet vermektedir. Bu bağlamda öğrenme süreçlerinde teknolojinin bir araç, aracı ya da teknik olarak kullanılmasını gerektiren açık ve uzaktan öğrenme faaliyetlerinde, teknik destek hizmetleri de yer almaktadır. Bu çalışmada dijital uzamda yer alan sistemlerden biri olan açık ve uzaktan öğrenme sistemleri, gelişen ve genişleyen dijital uzamın tehditleri ve tehlikeleri doğrultusunda teknik destek hizmetleri kapsamında incelenmiştir. Bu doğrultuda açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanmasında makine öğrenmesinin kullanıldığı bir teknik destek hizmeti önerisi oluşturulmak amaçlanmaktadır. Nitel araştırma yöntemlerinden durum çalışmasının benimsendiği çalışmada ilk olarak alanyazında yer alan dokümanlar incelenmiş; daha sonra bu bilgiler ışığında oluşturulan on görüşme sorusuyla sekiz alan uzmanından durum ile ilgili görüşleri alınmıştır. Yapılan görüşmelerin dökümü alındıktan sonra elde edilen verilen NVivo paket programı aracılığıyla kod ve temalara ayrılmıştır. Açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanması için kurum kültürünün, görev ve sorumluluk dağılımlarının, yönetsel desteğin, kurumsal farkındalığın, siber güvenlik eğitimlerinin ve farklı teknolojilerin kullanılmasının çözüm önerisi olarak sunulduğu bulunmuştur. Bunların yanı sıra siber güvenliğin sağlanması ve sürdürülmesi aşamalarında akıllı sistemlerin kullanılması gerektiğine dair ortak bir görüş elde edilmiştir.

Anahtar Kelimeler: Açık ve uzaktan öğrenme, Destek hizmetleri, Teknik destek hizmetleri, Siber güvenlik.

ABSTRACT

Under the philosophy of lifelong learning, open and distance learning activities that ensure the continuation of learning with an egalitarian policy for everyone, regardless of time and place, aim to meet the expectations and needs of different individuals, societies, and systems. Support services, which cover the support of differing expectations and needs in all learning-related activities, serve learning processes and different stakeholders involved in these processes. In this context, technical support services are also included in open and distance learning activities that require the use of technology as a tool, tool or technique in learning processes. In this study, open and distance learning systems, which are one of the systems in digital space, are examined within the scope of technical support services in line with the threats and dangers of the developing and expanding digital space. In this direction, it is aimed to create a technical support service proposal that uses machine learning to provide cyber security in open and distance learning systems. In the study, in which case study, one of the qualitative research methods, was adopted, firstly, the documents in the literature were examined; then, with ten interview questions created in the light of this information, eight field experts' opinions about the situation were taken. After taking the transcript of the interviews, the data obtained were divided into codes and themes through the NVivo package program. It has been found that the institutional culture, distribution of duties and responsibilities, managerial support, corporate awareness, cybersecurity trainings and the use of different technologies are presented as a solution proposal to ensure cybersecurity in open and distance learning systems. In addition to these, a common view was obtained that smart systems should be used in the stages of providing and maintaining cybersecurity.

Keywords: Open and distance learning, Support services, Technical support services, Cybersecurity.

TEŞEKKÜR

Hayallerime giden yolda desteğini, tecrübesini, anlayışını, sevgisini ve şefkatini hiçbir zaman esirgemeyen kıymetli danışman hocam sayın Prof. Dr. T. Volkan YÜZER ’e hayatıma kattığı neşe ve değerler için minnettarım. Eş danışman hocam Arş. Gör. Dr. Hakan KILINÇ başta olmak üzere tez jürimde yer alan kıymetli patron hocam, elinde büyüdüğüm idolüm Doç. Dr. Mehmet FIRAT ’a ve sayın Doç. Dr. Engin KURŞUN hocama emekleri ve katkıları için çok teşekkür ederim. Yolumu ve ufkumu aydınlatan değerli hocalarım Prof. Dr. Mehmet KESİM, Prof. Dr. Yavuz AKBULUT, Doç. Dr. Hakan ALTINPULLUK ve Doç. Dr. Aras BOZKURT ’a sonsuz saygı ve şükranlarımla...

Gerek akademik gerekse kişisel yaşantımda her daim yanımda olup elimden tutan Aysun GÜNEŞ, Dr. Meral CEYLAN, Mona AYKUL, Hülya DÜZENLİ ve Emin ÖZEN ’e; yol arkadaşlarım, biricik hocalarım Dr. Ezgi DOĞAN ve Dr. Ferhan ŞAHİN ’e; her kararımda arkamda durup beni ben yapan her şeye sabırla ve sevgiyle destek olan sevgili annem Mehtap ERTAN ve babam Hayati ERTAN’ a; en büyük destekçim, oyun arkadaşım, tıbbiyeli küçüğüm Betil ERTAN ’a edeceğim teşekkürlerin ardı arkası gelmez. İyi ki vardınız, iyi ki varsınız.

Yolum uzun; yolculuğum sizlerle güzel. Var olun…

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Anadolu Üniversitesi tarafından kullanılan "bilimsel intihal tespit programı"yla tarandığını ve hiçbir şekilde "intihal içermediğini" beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçları kabul ettiğimi bildiririm.

Sehla ERTAN

İÇİNDEKİLER

TABLOLAR DİZİNİ

Sayfa

ŞEKİLLER DİZİNİ

Sayfa

1. GİRİŞ

1.1.Problem Durum

Açık ve uzaktan öğrenme faaliyetleri, farklı kültürlerden geniş yaş aralığına sahip grupların farklı teknolojiler aracılığıyla esnek öğrenme süreçlerine, ortamlarına ve kaynaklarına zamandan ve mekândan bağımsız bir şekilde kolayca erişmesine olanak sağlamaktadır. Öğrenen, öğreten, yönetici ve personel gibi pek çok paydaşın dahil olduğu açık ve uzaktan öğrenme faaliyetlerini düzenleyen, iyileştiren ve geliştiren kapsamlı yapıyı ise "destek hizmetleri" olarak adlandırmak mümkündür. Destek hizmeti, doğrudan öğrenenlere yönelik olabildiği gibi öğrenme süreçlerinin hazırlanması, sunulması ve iyileştirilmesinde temelinde rol oynayan öğreten, yönetici ya da personel gibi paydaşların çeşitlenen ihtiyaçlarını da kapsayabilmektedir. Akademik, idari, teknik, danışmanlık, sosyal ve kütüphane hizmetleri şeklinde çeşitlenen ihtiyaçların ele alındığını söylemek mümkündür. Bu doğrultuda, destek yapılarında gözetilen en önemli faktörün "öğrenme süreçlerini düzenlemek, iyileştirmek ve geliştirmek" olduğu ifade edilebilir. Bununla birlikte, farklı paydaşların farklı ihtiyaçları doğrultusunda şekillenen destek hizmetleri, çoğunlukla öğrenen ve öğretenlerin öğrenme süreçlerindeki akademik ve sosyal ihtiyaçları çerçevesinde yapılanarak sisteme ve paydaşlara yönelik teknik ihtiyaçlar bağlamında yetersiz kalmaktadır (Durak, 2017; El Turk & Cherney, 2016).

Doğası gereği teknik ve teknolojik bir oluşumu temsil eden açık ve uzaktan öğrenme sistemlerinin işleyişini ve devamlılığını tehdit eden kritik faktörlerin başında teknik sorunlar yer almaktadır (Almaiah, Al-Khasawneh & Althunibat, 2020; Yumurtacı, 2020). "Altyapı bileşenleri", "teknoloji tabanlı süreçler", "iletişim ve etkileşim unsurları", "yazılım, donanım ve ağ yapıları" gibi çeşitli katmanlardan oluşan teknik destek yapısı; verilerin, bireylerin, süreçlerin ve sistemin güvenliğine yönelik endişeleri ve faaliyetleri (tespit, önlem, savunma vb.) barındırmaktadır (Alexei & Alexei, 2021; Dhillon, 2020; Durak, 2017; El Turk & Cherney, 2016). Bu sürecin yönetilmesinde ise sosyal bir canlı olan insanın karar verme sürecindeki kısıtlı rasyonelliği göz önüne alındığında (Bone, 2016), sistem güvenliğinin sağlanmasında makine öğrenmesine başvurulması gerektiği savunulabilir. Bu sayede açık ve uzaktan öğrenme sistemlerinin korunması ve devamlılığının sağlanması mümkün olacaktır.

Her biri öne çıktığı döneminin teknolojik devrimi olan mektup, telefon, radyo ve televizyon gibi kitle iletişim teknolojilerinde yaşanan gelişmelerin izlediği hiyerarşinin

bir sonraki ayağı olan internet teknolojileri, uzaktan eğitim faaliyetlerini hızla yaygınlaştırmıştır (Fırat, 2016). Öğrenmenin teknolojik gelişmeler ışığında zamandan ve mekândan bağımsız bir şekilde "yaşam boyu" sürmesi prensibinden beslenen uzaktan eğitim konsepti, geleneksel sınıfların somut sınırlarını aşarak bireylerin öğrenme ihtiyaçları ve beklentileri doğrultusunda öğrenen özerkliğini ve bağımsız öğrenme becerilerini öne çıkarmaktadır (Fırat, 2021). Bu, uzaktan eğitimin fırsat eşitliği sağlayarak farklılaşan öğrenme ihtiyaçlarını ve beklentilerini hiçbir koşul gözetmeden teknolojik araçlar ve süreçler aracılığıyla gidermeyi amaçladığını işaret etmektedir. Bu amaç doğrultusunda uzaktan eğitim; esneklik, teknolojik altyapı, yenilikçi öğrenme yaklaşımları, program çeşitliliği ve yoğunlaşan öğrenen nüfusu gibi çeşitlenen faktörler doğrultusunda günden güne daha kapsamlı hale gelerek esnek, açık ve disiplinler arası bir alan olan açık ve uzaktan öğrenmeyi meydana getirmiştir (Fırat, 2016).

Yenilikçi öğrenme ortamlarının esnek ve açık politikalar çerçevesinde şekillenmesiyle artan ve farklılaşan öğrenen nüfusu, öğrenme süreçlerini destekleyen ve düzenleyen hizmet yapılarına olan ihtiyacı da arttırmış ve farklılaştırmıştır (Montelongo, 2019). Bu doğrultuda, öğrenen ihtiyaçlarını karşılamak için pek çok farklı paydaşı, uygulamayı ve teknolojiyi öğrenme süreçlerine dahil eden açık ve uzaktan öğrenme sistemlerinin etkili, verimli ve sürdürülebilir bir yapıyı temsil etmesinde destek hizmetlerinin önemli bir role sahip olduğu söylenebilir. Farklı kurumların özerk kültürleri ve politikaları çerçevesinde şekillenen ihtiyaçlara yönelik yapılanan destek yapılarını çeşitlenen yaklaşımlar ve bakış açılarıyla ele almak ilgili önemi beslemektedir (Durak, 2017). Bununla birlikte, literatürde yer alan destek hizmeti çalışmalarının sırasıyla öğrenen ve öğreten desteği üzerinde daha fazla yoğunlaştığı görülmektedir (El Turk & Cherney, 2016; Genç Kumtepe vd., 2019). Bu doğrultuda destek hizmetlerinin öğrenen veya öğreten desteğinin çok daha ötesinde bir yapıyı temsil ettiği ifade edilebilir.

Sistemdeki bireylere ve bu bireylerin öğrenmesinden sorumlu olan tüm paydaşlara destek olurken çeşitlenen destek hizmeti tanımlarını göz önünde bulundurmak, planlanan uygulamaların ve kullanılan teknolojilerin etkililiğini değiştirecek önemli bir unsurdur (Genç Kumtepe vd., 2019). Bu durum, özellikle teknolojik gelişmeler ışığında çağa ayak uydurabilmek ve daha iyi hizmet sağlayabilmek adına analogdan dijitale dönüşen destek hizmeti yapısının, sistemin kendisini de kapsayacak düzeyde yapılanmasının önemini işaret etmektedir. Bu süreçte ise tüm paydaşlara hizmet ve destek sağlayan sistemin

kendisinin de destek hizmetlerince optimize edilmesi gerektiği öngörülebilir. Doğası gereği teknik bir oluşumu ifade eden açık ve uzaktan öğrenme sistemi çatısı altında incelenebilecek bu boyut, destek hizmetlerinin teknik yönüne vurgu yapar niteliktedir.

Açık ve uzaktan öğrenme sistemleri, öğrenme faaliyetlerinin sürdürülebilirliğini sağlayan bir altyapı oluşturmak için teknik donanımlara, yazılımlara ve ağlara sahip tutarlı bir yapı kurmaya ve bu yapının desteklenmesinde görev alacak uzmanlara ihtiyaç duymaktadır (Gümüş, 2020). Sistemin teknik boyutu ile ilgilenen teknik destek hizmetleri genel bir bakış açısıyla "donanım, yazılım ve ağ yapılarının kurulumunu", "bu yapıların bakımı ve sunumunu", "içerik tasarımını ve yönetimini", "teknolojik kullanışlılık testlerinin uygulanmasını", "bireylere ve sisteme ait verilerin kontrolünün ve güvenliğinin sağlanmasını" kapsamaktadır (Durak, 2017; Minh Hoang vd., 2020; Montelongo, 2019). Bu noktada üzerinde durulması gereken önemli noktalardan birinin bireylere ve sistemlere ait varlıkların kontrolünün ve güvenliğinin sağlanması olduğu düşünülmektedir.

Enformasyon ve iletişim teknolojileri ile etkileşime giren varlıkları (veri, birey, teknoloji, sistem, kurum ya da hükümet) her türlü kötü niyetli girişime ve manipülasyona karşı korumayı temsil eden siber güvenlik; güvenlik tehditlerine ya da ihlallerine dair tedbir, öngörü ve savunma faaliyetlerini ifade etmektedir (Fischer, 2016; Jang-Jaccard & Nepal, 2014). Geniş bir teknolojik spektrum kapsamında sunduğu etkileşim ortamlarında büyük miktarda veri üreten, depolayan ve transfer eden açık ve uzaktan öğrenme sistemlerinin günden güne çeşitlenen siber saldırılar için gelecek vadeden potansiyel bir "açık" hedef haline geldiği söylenebilir. Bununla birlikte, yasadışı faaliyetlerin gerçekleştirildiği siber uzamda hızla gelişim gösteren teknolojik yeniliklerin, aynı zamanda açık ve uzaktan öğrenme faaliyetlerini de hızla geliştirmesine ve yaygınlaştırmasına rağmen, açık ve uzaktan öğrenme sistemlerinin güvenliğine gereken ilgi gösterilmemektedir (Bandara, Ioras & Maher, 2014; Fırat, 2021; Minh Hoang vd., 2020). Bu noktada açık ve uzaktan öğrenme kurumları siber saldırılara yönelik faaliyetleri uygulamaya koymadan önce, uygulama sırasında ve sonrasında bir dizi teknik faktörü kurumsal kültür çerçevesinde titizlikle değerlendirmelidir (El Turk & Cherney, 2016).

Siber güvenliğin sağlanabilmesi ve sürdürülebilmesi için alınan teknik tedbirler, bir kurumun prestijini, dayanıklılığını ve devamlılığını sağlamada önemli bir role sahiptir (Türen & Kaya Bensghir, 2019). Bu durum, kurumsal yapılanma çerçevesinde ideal bir

siber güvenlik sisteminin ve kültürünün teknik bir bakış açısıyla oluşturulması gerektiğini işaret etmektedir. Siber güvenlikte yönetilmesi gereken kritik süreçler ve gitgide artan veri miktarı da göz önünde bulundurulduğunda, sistemlerde kayda değer bir otomasyon olmadığı sürece sistemdeki aktif kullanıcıların ve karar vericilerin siber saldırı süreçlerinin üstesinden gelmesi oldukça zordur (Nespoli, Papamartzivanos, Mármol & Kambourakis, 2018). Bu noktada siber güvenlikte akıllı sistemlerin işe koşulmasının gerekli olduğu öngörülebilir.

Simon (1955), "Sınırlı Rasyonellik Kuramı" ile insan beyninin hesaplama yeteneğinin sınırlı olduğunu; tercih ve karar aşamalarında belirsizliklerin ve bilgi eksikliklerinin olabileceğini vurgulamıştır. Bu doğrultuda Simon (1955; 1976), karar mekanizmasında baş rolde olan kişilerin bilişsel doğaları gereği birçok sınırlılıktan dolayı gerçekçi ve mantıklı, bir diğer ifadeyle *rasyonel* kararlar veremediklerini ifade etmiştir. Rasyonelliği sınırlayan faktörleri tanımlamıştır.

Organizasyonel bir yönetim politikasını kapsayan siber güvenlik yönetiminde sınırlı rasyonelliğin önüne Otto Peters'ın Endüstrileşme Kuramı ile geçilebileceği düşünülmektedir. Uzaktan eğitimdeki organizasyonel süreçlerin uzmanlar tarafından birimler halinde rasyonelleştirilmesi, mekanikleştirilmesi, planlanması ve organize edilmesi gibi pek çok endüstriyel üretim bileşenlerini tartışan bu kuram (Peters, 1993; 2010) ile açık ve uzaktan öğrenme kurumlarında siber güvenliğin sağlanmasında endüstriyel bir yaklaşımın benimsenebileceği savunulabilir.

Açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanmasında ve sürdürülmesinde sistemdeki tüm paydaşların; siber saldırıların öngörülmesi, tespit edilmesi, önlenmesi veya savunulması aşamalarında bazı kararlar vermesi gerektiği düşünülebilir. Bu kararlar dijital bir eylemin ya da içeriğin siber saldırı olup olmadığını ayırt etmekteki karar süreçlerini kapsayabileceği gibi saldırı faaliyetlerine karşı aktif tespit, önlem ya da savunma faaliyetleri göstermedeki süreçleri tasarlamak ve yürütmekte verilen kararları da ifade edebilir. Yukarıda verilen bilgiler ışığında açık ve uzaktan öğrenme sistemlerinde teknik destek hizmetlerinde yaşanan sorunlar altında yer alan siber güvenliğin sağlanmasında tam rasyonel kararlar alınması adına akıllı sistemlerin kullanımı incelenmeye değer bir yaklaşım olarak görülmektedir. Yüz yüze sağlanan destek hizmetlerinin zaman ve mekân gerekliliğini aşarak yerini yapay zekâ ve özellikle makine öğrenmesi yazılımlarına ve uygulamalarına bırakacağı öngörülmektedir. Bu

noktadan hareketle, açık ve uzaktan öğrenme sistemlerinde sağlanan teknik destek kapsamında insan gücünün yanı sıra yapay zekâ ve makine öğrenmesi gibi ileri teknolojilerden de destek alınması gerektiği söylenebilir.

1.2.Amaç

Bu çalışmanın amacı, açık ve uzaktan öğrenme sistemlerine yönelik siber saldırıların önlenmesi ve siber güvenliğin sağlanması süreçlerinde makine öğrenmesinin kullanıldığı bir teknik destek hizmeti önerisi oluşturmaktır. Destek hizmeti yapısında siber güvenliğin sağlanması için Otto Peters'ın Endüstrileşme Kuramı doğrultusunda makine öğrenmesinin kullanılması önerilmektedir. Bu öneri, yapay zekanın önde gelen isimlerinden biri olan Herbert Simon'ın "Sınırlı Rasyonellik Kuramı" kapsamında ele alınmaktadır. Belirtilen amaç doğrultusunda aşağıdaki sorulara yanıt aranacaktır:

- Açık ve uzaktan öğrenme sistemlerinde siber güvenlik faaliyetleri sistemin hangi bileşenlerini ve bireylerini kapsamaktadır?
- Açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanmasında sistem paydaşlarının ve teknik destek hizmetlerinin sınırı ve sınırlılıkları nedir?
- Açık ve uzaktan öğrenme sistemlerinin teknik destek hizmetlerinde siber güvenliğin sağlanması için makine öğrenmesinden nasıl yararlanılabilir?

1.3.Önem

Bu çalışmanın, açık ve uzaktan öğrenme sistemlerinde siber güvenliğin yerini ve önemini belirtmek adına alanyazına katkı sağlayabilecek bir çalışma olduğu düşünülmektedir. Araştırmanın problem durumu ve araştırma amacı ışığında bu çalışma;

- Açık ve uzaktan öğrenmede destek hizmetleri altında incelenen teknik destek hizmetlerinin öneminin vurgulanabilmesi,
- Açık ve uzaktan öğrenme sistemlerinin karşılaşabileceği siber saldırılara karşı farkındalık ve öngörü oluşturulabilmesi,
- Açık ve uzaktan öğrenme sistemlerindeki verilerin ve bireylerin siber güvenliğinin sağlanabilmesi,
- Siber güvenlik ışığında makine öğrenmesinin teknik destek hizmetlerindeki yeri ve öneminin vurgulanabilmesi,

- Siber güvenliğin en iyi şekilde sağlanabilmesi ve sistemin dengelenmesi ve sağlamlaştırılması adına makine öğrenmesinin kullanılabilmesi için önem taşımaktadır.

2. ALANYAZIN

2.1. Açık ve Uzaktan Öğrenmede Destek Hizmetleri

Açık ve uzaktan öğrenme paydaşları (öğrenenler, öğretim elemanları, yöneticiler, personel), çeşitli internet teknolojileri ve etkileşim ortamları aracılığıyla zamandan ve mekândan bağımsız öğrenme deneyimleri edinmektedir (Genç Kumtepe vd., 2019; Okur, 2012). Yaklaşık üç asrı aşan kurumsal ve kuramsal bir geçmişi olan açık ve uzaktan öğrenme faaliyetlerinin yetişkin öğrenen nüfusu ile eşzamanlı artışı, çeşitli beklenti ve ihtiyaçların da ortaya çıktını işaret etmektedir. Bu ihtiyaç ve beklentilere cevap vermeyi amaçlayan destek yapıları ilk olarak yüz yüze eğitimin rehberlik hizmetlerini model almıştır (Brindley, 1987; Zawacki-Richter, 2004). Öğretim elemanlarının çeşitli konularda öğrenenlere rehberlik yapmasıyla başlayan bu hizmet (Rekkedal, 1981), sistemin çeşitlenen nüfusuyla şekillenerek "destek hizmetleri" olarak yapılanmıştır (Sewart, 1980).

Kuramsal geçmişinden çok daha eskiye dayanan uygulamalı açık ve uzaktan öğrenme faaliyetleri göz önünde bulundurulduğunda, bu faaliyetlerin bağlamına göre değişen destek yapılarının da olduğu öngörülebilir. Ancak geniş hedef kitlesi ve kapsamı dolayısıyla farklı kurumlarda farklı kurumsal kültür ve politikalar çerçevesinde şekillenen destek faaliyetlerinin farklı tanım ve sınıflandırmalar kapsamında incelendiği görülmektedir (Durak, 2017). Bu doğrultuda, farklı destek hizmeti yaklaşımlarını incelemenin "destek" kavramını somutlaştırmak için faydalı olacağı düşünülmektedir.

2.1.1. Destek hizmetlerinde farklı sınıflandırmalar, yorumlar ve paydaşlar

2.1.1.1. 2000 yılından önce destek hizmetlerinin incelendiği çalışmalar

Yazışmalı eğitim ile başlayan açık ve uzaktan öğrenme serüveninin kurumsal öncülerinden olan İngiliz Açık Üniversitesi, öğrenen motivasyonu ve devamlılığı için 1960'lardan itibaren rehberlik hizmetleri vererek destek oluşumunda da öncü olmuştur (Sewart, 1980). Destek hizmetlerinin zeminini oluşturan öğrenen odaklı rehberlik

hizmetlerinin, zaman içinde artan öğrenen nüfusu ile paralel bir şekilde çeşitlenen ihtiyaçlar ve beklentiler doğrultusunda şekillendiğini söylemek mümkündür. Öğretim elemanlarının gerek akademik gerekse sosyal yardım sunduğu öğrenen odaklı rehberlik hizmetlerinin öğreten eğitimi ile desteklenmesini savunan Sewart (1980), öğrenen ve öğreten desteğine dikkat çekmiştir. Bu, öğrenme süreçlerini iyileştirmek için verilen hizmetlerin odağında yalnızca öğrenenlerin olmadığını işaret etmektedir.

"Yazışmalı eğitimde rehberlik hizmetleri" yerine "uzaktan eğitimde rehberlik hizmetleri" ifadesini kullanan Rekkedal (1981), açık ve uzaktan öğrenmedeki "uzaklık" ögesinin rehberlik hizmetlerinde de göz önünde bulundurulması gerektiğini vurgulamıştır. Buradaki uzaklık vurgusunun zaman ve mekân bağlamında öğretenden, akranlardan ve kurumdan ayrı olan ve bu süreçte yazışmalı eğitimin alternatifleriyle sürece dahil olan öğrenenlerin desteklenmesine yönelik yapıldığı söylenebilir. Rehberlik hizmetlerinde kurumsal kültüre dikkat çeken Brindley (1987), bu hizmetlerin kariyer planlamasını, mali yardımı ve dezavantajlı bireyleri kapsaması gerektiğini savunmuştur. Bu noktada bu sınıflandırma ile kurumsal kültürün yalnızca öğrenen boyutuna yönelik hizmetlerin ele alındığını söylemek mümkündür.

"Rehberlik hizmeti" yerine "öğrenen desteği" ifadesini kullanan Hui (1989) ise bu desteği "bireysel öğrenme materyallerinin sağlanması", "öğrenme sistemlerinin yapılandırılması" ve "ölçme-değerlendirme uygulamaları" olarak incelemiştir. Öğrenen boyutunu kapsayan desteğe değinen bu sınıflandırmada öğretenden ya da kurumdan zamandan ve mekândan bağımsız olarak verilen destek hizmetlerinin, yüz yüze eğitim öğesi olan rehberlik hizmetlerinden ayrıştırıldığı söylenebilir. Bu, öğrenenlere rehber olmanın yanında destek olmayı da ifade eden bir yapılanmanın önemini işaret etmektedir.

Öğrenen desteğini "program öncesi", "program sırası" ve "program sonrası" şeklinde sınıflandıran Rowntree (1992), süreç odaklı bir yapı inşa etmiştir. Bu süreç sınıflandırmasının; "kayıt öncesi tanıtım ve bilgilendirme", "kayıt sırasında işlem ve prosedürler", "kayıt sonrası öğrenme süreçleri ve faaliyetleri" ile "mezuniyet sonrası imkanlar ve planlamalar" gibi aşamaları ifade ettiği söylenebilir. Öğrenen desteğinde kurumsal kültüre dikkat çeken Sewart (1993); "öğrenen özellikleri", "öğretim programları", "öğretim yöntemleri" ve "bireysel farklılıklar" çerçevesinde destek sunulmasını önermiştir. Kurumsal kültürün öğrenen boyutu üzerinden ele alındığı bu

sınıflandırmanın, çeşitlenen öğrenen nüfusunun farklılaşan özellikleri ile ele alınması yönünde öncü çalışmalardan biri olduğu söylenebilir.

Destek hizmetlerini çevrimiçi öğrenenlere ve öğretenlere göre yapılandıran Berge (1995), bu yapıyı "pedagojik", "sosyal", "yönetsel" ve "teknik" boyutlarda ele almıştır. Kapsamlı doğasından ötürü yaygın bir kullanıma sahip olan bu destek hizmeti modelinde öğrenme faaliyetlerinin "çevrimiçi" olduğu vurgulandığı görülmektedir. Bu yaklaşımın, 1992 tarihinden itibaren var olan ve gelişim gösteren internet teknolojilerinin açık ve uzaktan öğrenme faaliyetlerinde hızlı bir şekilde benimsendiğini işaret etmektedir.

Destek hizmetlerinin hızla değişen açık ve uzaktan öğrenme bağlamına göre yapılandırılmasında izlenecek stratejilerde kurumsal kültür ve değerlerin önemini belirten Brindley (1995), öğrenen desteğinin etkili tek bir tanımı olamayacağını savunmuştur. Bu tanım ışığında geliştirilen hizmetlerinin odağında "bağımsız öğrenenlerin gelişimi", "öğrenenin yetkilendirilmesi", "öğrenme sisteminin kişiselleştirilmesi", "sistemin demokratikleşmesi" ve "öğrenenlerin erken katılımı ve bağlantılığın kolaylaştırılması" yer almaktadır (Brindley, 1995). Kurumsal kültürü ele alan diğer çalışmaların aksine bu çalışmada kurumsal kültür çerçevesinde öğrenenlere ve sistemin kendisine yönelik bir destek yapısının kurgulandığını söylemek mümkündür.

Öğrenen desteğinde dengeleyici (*compensatory*) ve tamamlayıcı (*complementary*) olmayı savunan Reid (1995), herkes tarafından her an erişilebilen tamamlayıcı hizmetlerin tüm öğrenme süreçlerini kapsadığını ifade ederken dengeleyici hizmetlerin olası problem durumlarda ek materyal ya da etkinlikler olarak sunulması gerektiğini belirtmiştir. Bu iki destek ögesinin birbirini besleyen bir destek döngüsünü temsil ettiğini göstermektedir.

Bir başka çalışmada Robinson (1995), öğrenen desteğini oluşturan bileşenleri "sistemi meydana getiren unsurlar", "bu unsurların yapılandırılması" ve "bu unsurların öğrenenler ile etkileşimi" olarak ifade etmiştir. Bu sınıflandırmada öğrenen desteğinde akademik boyutunun yanı sıra sosyal ve yönetsel boyutlara da dikkat çektiği söylenebilir. Bu boyutların hangi amaca ve kitleye yönelik nasıl yapılandırılacağı ise açık ve uzaktan öğrenme kurumlarının destek hizmetlerine karşı tutum ve yaklaşımlarına göre çeşitlenebilmektedir (Robinson, 1995). Kurumsal kültüre vurgu yapan bu yaklaşımda da

destek yapısını şekillendiren kültürün öğrenen boyutuna odaklanarak ele alındığı ifade edilebilir.

Öğrenen desteğinde yaygın olarak kabul gören bir diğer kapsamlı destek sınıflandırmasının Keast (1997) tarafından oluşturulduğu söylenebilir. Bu modelde Keast (1997), öğrenen desteğinin "akademik", "idari", "teknik", "kütüphane" ve "danışmanlık" şeklinde 5 boyuttan oluştuğunu ifade etmiştir. Öğrenme süreçlerinin gerek akademik gerek teknik gerekse yönetsel boyutlarına göre şekillenen bu destek yapısında, daha önce bahsi edilen "rehberlik" yapısının destek hizmeti çatısı altında "danışmanlık" hizmeti olarak verildiği görülmektedir. Bu doğrultuda, destek hizmetlerinin rehberlik hizmetlerinden ayrıştığını ve daha kapsamlı bir yapıyı temsil ettiğini söylemek mümkündür.

2.1.1.2. 2000'li yıllarda destek hizmetlerinin incelendiği çalışmalar

2000'li yıllara gelindiğinde Brindley (2000), öğrenen desteğinde sosyal destek kuramı kapsamında bir müdahale stratejisi geliştirerek öğrenme süreçlerinde sosyal desteğin gerekli olduğunu vurgulamıştır. Zamandan ve mekândan bağımsız bir şekilde öğrenme ortamlarından, öğretenlerden ve akranlardan izole olan öğrenenler için tasarlanan bu sosyal destek modelinde öğreten, yönetim, kurum ve akran etkileşimine yönelik bir yaklaşım olduğu söylenebilir. "Fakülte desteği" kapsamında ele aldığı yapıda Padgett ve Conceicao-Runlee (2000), teknolojinin eğitime dahil olduğu faaliyetlerin tümünde fakülte personelinin teknolojik yeterliklerinin ve gelişimlerinin öneminden bahsetmiştir. Öğrenme süreçlerine dahil olan akademik, yönetsel ve diğer personelin teknik ve teknolojik yeteneklerini geliştirmeye yönelik bir program tasarısı sunarak kurumsal bir teknik destek yapısını işaret etmektedir.

Öğrenen desteğinde "sosyal destek", "akran desteği" ve "görev desteği" bileşenlerini temel alan McLoughlin (2002), öğrenen desteğini bir iskelet üzerine inşa ederek yapılandırılmayı önermiştir. Sağlam bir destek iskeleti için "bilgisayar destekli amaçlı öğrenme ortamları" ve "akıllı ders sistemleri" gibi teknolojik yaklaşımlarla "hedef odaklı senaryolar" ve "tasarım destek ortamları" oluşturulmalıdır (McLoughlin, 2002). Bu yaklaşım, yakın zamanlı daha önceki destek hizmeti tanımlarında vurgulanan sosyal

ve teknik desteğin birlikte ele alındığı bir yapılanmayı işaret etmektedir. Bu doğrultuda, destek yapılarının belirli ölçüde birbirinden etkilenerek şekillendiği söylenebilir.

Simpson (2002) tarafından yapılan sınıflandırmada öğrenen desteği "akademik" ve "akademik olmayan" hizmetler olarak genel bir çerçevede incelenmiştir. Öğrenenlerin öğrenme deneyimlerinde akademik süreçler kadar akademik olmayan (teknik, yönetsel, sosyal vb.) süreçler için de desteğe ihtiyaç duyduğunu söylemek mümkündür. Tait (2002) ise, öğrenen desteğini "bilişsel (akademik), duyuşsal (sosyal) ve yönetsel" hizmetler kapsamında modellemiştir. Öğrenen desteğindeki farklı boyutları genel bir çerçeveden ele alan bu modelle öğrenme deneyimlerinin zihinsel yönüne vurgu yapıldığı söylenebilir. Farklı bir bakış açısıyla öğrenen ve öğreten desteğine değinen Turhan (2002), sunulacak hizmetlerin öğrenenleri ve öğretenleri etkili kaynak kullanımına yönlendirecek kapsamda üssel bir amaç benimsemesi gerektiğini savunmuştur.

Hardman ve Dunlap (2003); danışmanlık, değerlendirme ve destek ögelerinin öğrenenlerin öğrenme süreçlerindeki bilişsel, duyuşsal ve yönetsel ihtiyaçlarına yanıt oluşturan tüm faaliyetleri ve ögeleri kapsadığını belirtmiştir. Öğrenen desteği stratejilerini belirlerken özellikle bilişsel süreçler göz önünde bulundurularak yapılandırılan destek yapısının, öğrenenlerin öz-denetimlerini ve etkileşimlerini arttırarak öğrenme süreçlerini olumlu yönde etkileyeceği söylenebilir. Öğrenen desteğini daha mikro yapılarda inceleyen Keegan (2003), "bilgilendirme", "rehberlik", "kayıt", "entegrasyon", "final", "akreditasyon" ve "program sonrası rehberlik" süreçlerini irdelemiştir. Öğrenme faaliyetlerinin öncesi ve sonrası ile de ilgilenen bu destek modelinde, oryantasyon ve rehberlik hizmetleri tüm süreçlerde verilirken akreditasyon ve uygunluk değerlendirmeleri ile kuruma özgü standartların belirlendiği görülmektedir. Bu yönüyle açık ve uzaktan öğrenme sistemlerinin kendi ekolojisini oluşturarak sunduğu açıklık felsefesini saydam bir akademik kalite standardı çerçevesinde tanınır kıldığı ve yapılandırdığı söylenebilir.

Öğrenenlerin teknoloji kabulü ve teknoloji yeterlik gelişimlerindeki önemli faktörlerden birinin memnuniyet olduğunu belirten Lee (2003), bu memnuniyetin sağlanmasında sunulan öğrenen destek hizmetlerinin "yönetsel", "akademik", "teknik", "danışmanlık" ve "kütüphane" ögelerini barındığını savunmuştur. Daha önce Keast (1997) tarafından yapılan sınıflandırmaya yakın olan bu modelde öğrenenlerin

motivasyon ve memnuniyetlerinin sağlanmasında teknoloji odaklı teknik desteğin öneminin daha yoğun bir şekilde pekiştirildiği ve vurgulandığı düşünülebilir.

Süreç odaklı bir tanım yapan Rekkedal ve Qvist-Eriksen (2003), öğrenen desteğini "program öncesi", "öğrenme süreci" ve mezuniyet sonrası" şeklinde ele almıştır. Bu yapının genel anlamıyla öğrenenlere yönelik bilgilendirme, oryantasyon ve danışmanlık faaliyetlerine odaklandığını ve destek yapısını rehberlik hizmeti zeminine oturttuğunu söylemek mümkündür. 2002'de yaptığı tanımı genişleten Tait (2003), akademik destek boyutuna bilişsel desteği eklerken akademik olmayan destek yapısında duyuşsal ve kurumsal boyutlara yer vermiştir. Akademik destek altında incelenen bilişsel destekte "öğrenme, öğretme, ölçme ve beceri geliştirme" gibi bileşenlerden söz edilebilirken duyuşsal ve kurumsal desteklerde sırasıyla sosyal ve idari bileşenlerin yer aldığı söylenebilir. Rekkedal ve Qvist-Eriksen (2003)'ın tanımını daha bütüncül bir yapıda inceleyen Thorpe (2003), öğrenen desteğini tüm süreçleri kapsayan "kurumsal destek" ve daha dar kapsamda öğrenen-öğreten etkileşimini ele alan "konu desteği" şeklinde iki başlıkta ele almıştır.

Öğrenenlere yönelik destek hizmetlerini "öğrenen giriş aşaması", "öğrenen müdahalesi", "öğrenen desteği", "öğrenen geçiş aşaması" ve "ölçme" aşamalarından oluşan bir döngüyle modelleyen Floyd ve Casey-Powell (2004), öğrenen desteğinde "akademik danışmanlık", "öğretim desteği", "kütüphane hizmeti", "engelli hizmetleri" ve "örgütlenme" bileşenlerinden bahsetmiştir. Öğrenme süreçlerinin daha çok akademik yönüne vurgu yapan bu modelin, çeşitlenen öğrenen nüfusu ile farklı bir boyut kazanarak dezavantajlı bireyleri de kapsayan bir yapıda oluşturulduğu işaret etmektedir. Bunun, açık ve uzaktan öğrenme faaliyetlerinde artan nüfusun çeşitlenen doğasını betimler nitelikte olduğu söylenebilir.

Akademik desteğin öğretim elemanı desteğine eşit olmadığını vurgulayan Zawacki-Richter (2004) ise, öğrenen desteğine ek olarak öğreten ve fakülte desteğine de dikkat çekmiştir. Fakülte desteğinin öğrenme süreçlerindeki tüm faaliyetlerde rolü olan öğretim elemanları, yönetim ve personel boyutunu kapsadığı söylenebilir. Bu, öğrenme süreçlerinde öğrenenlerin desteklenmesi kadar öğrenme süreçlerinde rol oynayan paydaşların da desteklenmesinin önemli olduğunu işaret etmektedir.

Muilenburg ve Berge (2005), destek hizmetlerine farklı bir açıdan bakarak açık ve uzaktan öğrenmede bu hizmetleri gerekli kılan sekiz faktörü "yönetsel sorunlar, sosyal etkileşim, akademik yeterlikler, teknik yeterlikler, öğrenen motivasyonu, çalışmalar için gerekli zaman ve destek, internete erişim maliyetleri, teknik sorunlar" olarak sıralamıştır. Öğrenen desteğinin kapsamlı bir şekilde ele alan bu modelin, daha çok yönetsel süreçler ve politikalar çerçevesinde yapılanarak kurumsal kültürün destek yapısı karşısında izlediği yaklaşımı ifade ettiğini söylemek mümkündür. Doğrudan öğrenme süreçlerini kapsamaktan ziyade öğrenme süreçlerinin alt bileşenlerine yönelik bir modeli temsil ettiği söylenebilir.

Öğrenme süreçlerini baz alan bir diğer tanımda Hughes (2007), öğrenen desteğini "ders öncesi" ve "ders sırası" şeklinde geniş bir perspektiften incelemiştir. Bu yapıda sadece öğrenme süreçlerini besleyen bir destek yapısının inşa edildiği söylenebilir. Destek hizmetlerinde hem süreç hem de faaliyet odaklı kapsamlı bir tanım yapan Somayajulu ve Ramakrishna (2008) ise, ilk olarak bu hizmetleri "bölge/ eğitim merkezlerinin kurulması ve bakımı", "enformasyon hizmetleri", "kayıt öncesi hizmetler" ve "kayıt sonrası hizmetler" olarak sınırlandırmıştır. Kayıt sonrası hizmetler ise "materyal gönderimi", "kütüphane hizmetleri", "ölçme-değerlendirme", "finansal destek", "teknolojik hizmetler", "medya hizmetleri" ve "kişisel bilgilerin yönetimini içeren diğer hizmetler" bileşenlerini içermektedir (Somayajulu ve Ramakrishna, 2008).

2.1.1.3. 2010'lu yıllarda destek hizmetlerinin incelendiği çalışmalar

Kapsamlı bir destek modeli çizen Okur (2012), etkili bir destek hizmeti için kimlere hangi ortamda ne tür bir destek verileceğini belirleyebilmek için "destek türleri", "hedef kitle" ve "destek ortamları" ögelerine dikkat çekmiştir. Bu çalışmada genel odak her ne kadar öğreten desteği olsa da destek hizmetlerinin yalnızca bu boyuta dayandırılmadığı; destek yapılarında farklı destek faaliyetleri ile kapsamlı ve çeşitlenen bir paydaş yelpazesinin tanımlandığı söylenebilir. Bununla birlikte gelişen internet teknolojilerinden beslenen açık ve uzaktan öğrenme faaliyetleri kapsamında sunulan destek yapılarının çeşitlenen ortamlarda zaman ve mekân ögeleri gözetilerek çeşitlendirilen bir yapıda verildiğini de belirten çalışma, o tarihe kadar yapılan destek tanımlarının farklı boyutlarını kapsar niteliktedir.

Öğrenme süreçlerinde teknik desteğe vurgu yapan Khanna ve Basak (2013), teknolojinin ön koşul olduğu açık ve uzaktan öğrenme süreçlerinde makro ve mikro düzeydeki her faaliyetin teknik destek hizmetlerinin endişesi olduğunu savunmuştur. Teknik desteğin öğrenene motivasyonu ve devamlılığı için önemli olduğunu işaret eden bu tanım ile açık ve uzaktan öğrenme faaliyetlerinde teknik ve teknolojik yapılanmanın geliştirilmesi, iyileştirilmesi ve sürdürülmesinin kapsamlı bir sistem yaklaşımını belirttiği söylenebilir. Inkelaar ve Simpson (2015) ise, yaptıkları çalışmada açık ve uzaktan öğrenme kurumlarının yüz yüze eğitim veren kurumlara göre çok daha düşük mezuniyet oranlarına sahip olmasını etkileşim ve destek hizmetlerindeki yetersizliğe yorarak destek hizmetlerinin önemini vurgulamıştır.

Berge (1995)'e benzer bir yapı oluşturan Baran ve Correia (2016), destek yapısını "teknik", "pedagojik" ve "finansal" şeklinde ele almıştır. Öğrenen desteğine odaklanan bu yapının genel anlamıyla eğitsel ve idari faaliyetlere odaklandığı söylenebilir. Açık ve uzaktan öğrenme kurumlarında öğrenme süreçlerindeki sorunların giderilmesinde "uygulama öncesi, sırası ve sonrası" aşamalarının olduğunu belirten El Turk ve Cherney (2016), bu faaliyetleri yürütürken göz önünde bulundurulması gereken kültürel ve teknik engellerin dikkatle değerlendirilmesini önermiştir. Gürer, Tekinarslan ve Yavuzalp (2016), destek hizmetlerinde öğrenen desteğinin teknik yönüne değinmiştir. Bu çalışmaya göre teknik desteğin hem öğrenenlere sağlanmasının yanını sıra öğretenler için de ulaşılabilir, etkili, esnek ve hızlı çözümler üretmesi gerektiği söylenebilir.

Öğrenen desteğinin teknik boyunun önemli olduğunu ifade eden Arko-Achemfuor (2017), teknik destekteki yetersizliğin artan öğrenen nüfusuna rağmen destek personeli ve yapılarının güncellenmemesinden kaynaklandığını savunmuştur. Bu doğrultuda teknik destek hizmetlerinin sağlanmasında uzman personel kadrosunun ve teknik donanımın önemli bir yere sahip olduğu söylenebilir. Destek hizmetlerinde yaşanan sorunları genel bir çerçeveden inceleyen Durak (2017) ise, literatürde yer alan benzer çalışmaları derleyerek destek hizmetlerindeki sorunların çözümünde "akıllı destek yapılarının" kullanılmasını önermiştir. Bu, teknolojik gelişmelerin destek hizmeti yapılarını da doğrudan ilgilendirdiği, etkilediği ve şekillendirdiğini işaret etmektedir.

Öğrenen desteğini "akademik destek", "topluluk duygusu", "teknik destek" ve "iyi olma & refah" olarak sınıflandıran Roddy ve arkadaşları (2017), öğrenenlerin katılım ve motivasyonlarını sağlamak adına teknik desteğin kritik bir öneme sahip olduğunu

vurgulamıştır. Açık ve uzaktan öğrenme sisteminde e-öğrenme araçlarını kullanmada yetersiz olan öğretim elemanlarına yönelik bir çalışma gerçekleştiren Mısırlı, İzmirli ve Şahin İzmirli (2018), bu yetersizliklerin teknolojik ve pedagojik destek ile giderilmesini önermiştir. Benzer yaklaşımla Alemdağ, Çevikbaş ve Baran (2019), öğreten desteğinde teknik ve pedagojik hizmetlerin ders süreçlerinde öğretenlere çeşitli fırsatlar sunduğunu belirtmiştir. Dalton vd. (2019), öğreten desteğinde yalnızca pedagojik hizmetlerin önemini vurgulamıştır.

Destek hizmetlerini oldukça geniş bir perspektiften inceleyen Genç Kumtepe vd. (2019) ise, açık üniversitelerdeki destek hizmetlerini ve farklı araştırmacılar tarafından yapılan tanımları inceleyerek kapsamlı bir model oluşturmuştur. Destek hizmetlerini "öğrenen" ve "personel" desteği şeklinde temel iki başlıkta ele alan bu modelde, farklı paydaşlara yönelik (aday öğrenen, kayıtlı öğrenen, idari ve akademik personel) farklı destek hizmetleri (sistem tanıtımı, akademik, yönetsel, teknik ve sosyal destek) tasarlanmıştır (Genç Kumtepe vd., 2019).

2.1.2. Açık ve uzaktan öğrenmede teknik destek hizmetleri

Öğrenme süreçlerine dahil olabilmek için teknolojinin ön koşul olduğu açık ve uzaktan öğrenmede öğrenen ve öğretenlerin etkili bir teknik destek hizmeti alabilmelerinin önemli olduğunu işaret etmektedir. Bu doğrultuda, teknik destek hizmetinin hızlı geribildirim sağlayan; programa kabul şartları, kurs etkinlikleri tanıtımı, materyal/ kaynak kullanımı, kurs prosedürleri veya bileşenleri hakkında çalışma rehberi sunan; teknik hizmetin öğrenilmesinde zaman tanıyan; akran öğrenmesine teşvik eden; uzun talimatlara yönelik konu anlatımı seçeneği sunan; öğrenenin bireysel deneyimlerine fırsat veren yapıda olması gerektiği söylenebilir.

Keast (1997)'e göre teknik destek hizmeti, öğrenme ortamlarının sunulmasını ve bu ortamların verimli çalışması için yapılan faaliyetleri kapsamaktadır. Bu tanımda yer alan teknik destek hizmeti, öğretenler ve rehberlik hizmeti veren öğretim elemanları için teknik desteğin önemini de vurguladığı söylenebilir. Benzer bir kapsamda teknik destek hizmetini öğretim elemanları için teknoloji kullanımına yönelik destek olarak tanımlayan Padgett ve Conceicao-Runlee (2000), öğretim elemanlarının teknoloji kullanım

yeteneklerinin ve yeterliklerinin geliştirilmesi için "fakülte desteği" çatısında teknik eğitim verilmesini önermiştir.

Destek hizmetlerinde yeni teknolojilerin kullanımına dikkat çeken Lee (2003)'ye göre teknik destek hizmeti, planlanmış çalışma saatleri dahilinde öğrenenlerin ücretsiz iletişim kanalları (telefon, e-posta, diğer iletişim araçları) ile teknik personelden yardım alabildiği tesisleşmiş yapılardır. Bu doğrultuda, öğrenme faaliyetlerinde olduğu gibi teknik destek yapısında sürece doğrudan müdahil olmayıp öğrenene rehber olan bir ikinci aktörün olduğu söylenebilir. Başka bir tanıma göre destek hizmetlerine ihtiyaç duyulmasındaki sebepler arasında teknik sorunlar ve yetersizlikler yer almaktadır (Muilenburg ve Berge, 2005). Bu tanımın teknolojinin ön koşul olduğu açık ve uzaktan faaliyetlerinde teknik destek hizmetinin destek hizmetleri çatısını oluşturan ve gerekli kılan temel sorunlarla ilgilendiği sonucu çıkarılabilir.

Öğrenen desteğinin teknik boyutuna dikkat çeken bir diğer çalışmada teknik destek hizmeti "bilgisayar laboratuvarlarının kurulumu ve bakımı", "eğitim programlarının tanıtımı", "web barındırma (hosting), geliştirme ve bakımı", "ağ imkânı ve enformasyon ve iletişim teknolojileri kaynağı sağlamak" şeklindedir (Somayajulu ve Ramakrishna, 2008). Ağırlıklı olarak somut teknolojilerin hazırlanması, sunulması ve kullanılması gibi faaliyetleri kapsayan bu tanımın genel anlamda donanım ve ağ hizmetlerine odaklandığı; soyut teknolojiler ve yazılım hizmetlerini ele almadığı söylenebilir. Bu, zamanın teknolojik yapılanmasının gerekli kıldığı teknik hizmetlerin kapsamını işaret eder niteliktedir.

Açık ve uzaktan öğrenme süreçlerinde öğrenenlerle etkileşim halinde olan öğretenlere yönelik destek yapılarını inceleyen Okur (2012), içerik üretimi ve sunumu gibi teknoloji tabanlı faaliyetlerde başat rol oynayan öğretenler için teknik destek hizmeti ihtiyacına dikkat çekmiştir. Bu kapsamda açık ve uzaktan öğrenme sistemlerinde teknolojik araçlarının kullanımı ile ortaya çıkan yazılımsal ve donanımsal problemlerin çözülmesini ele alan bu destek yapısının yalnızca öğrenen desteğinde değil, sürece dahil olan öğreten desteğinde de öğrenme süreçlerine etkileyen bir önemi olduğu söylenebilir.

Başka bir tanıma göre "yazılım ve donanım kurulumları veya bakım hizmetleri", "altyapı tasarımı", "hizmet iletimi", "sistem değerlendirme ve düzenleme" faaliyetleri teknik destek hizmetine örnek gösterilebilir (Khanna ve Basak, 2013). Yazılım ve

donanım hizmetlerine odaklanan bu teknik destek tanımında ek olarak mevcut sistemin iyileştirilmesinin yanı sıra sistemin oluşturulmasının da ele alındığı söylenebilir. Bu, doğası gereği teknolojik bir yapılanmayı temsil eden açık ve uzaktan öğrenme faaliyetlerinde öğrenme süreçlerinin iyileştirilmesi endişelerini giderebilmek için öncelikle teknik destek hizmetlerinin gerekli bir çatı destek yapısı olduğunu işaret etmektedir.

Teknik destek hizmetini "bilgisayar ve internet erişimi" olarak iki ana başlıkta inceleyen Arko-Achemfuor (2017), teknik destek hizmeti yalnızca öğrenen odaklı sorunları ele almıştır. Açık ve uzaktan öğrenme sistemlerindeki sorunların incelendiği bir diğer çalışmada teknik destek hizmeti, benzer şekilde öğrenenlerin karşılaştığı yazılımsal ve donanımsal sorunlara çözüm üreten yapılardır (Durak, 2017). Bu doğrultuda teknik destek yapısının donanım ve yazılım boyutunu ele alan bu yaklaşımın aynı zamanda ağ problemlerinden kaynaklanan destek ihtiyacını da kapsar nitelikte olduğu söylenebilir.

Roddy vd. (2017)'nin çalışmasında ise teknik destek hizmetini, teknolojik yeterlikleri ve yetenekleri geliştirmeye odaklanan hizmetlerin tümü olarak tanımlanmıştır. Bu doğrultuda, açık ve uzaktan öğrenme kurumlarının, öğrenim öncesinde teknolojik gereksinimleri belirleyerek ve belirterek ders beklentilerinin karşılanmasındaki hızı arttırmak adına iyi yapılandırılmış bir teknik destek hizmetine sahip olması gerektiğini söylemek mümkündür. Destek hizmetlerini öğrenen ve personel desteği olarak iki genel başlıkta inceleyen Genç Kumtepe vd. (2019)'ne göre teknik destek hizmeti, "öğrenenleri gerekli teknik altyapı (donanım gereksinimleri, internet bağlantısı, e-posta ve parola işlemleri, sanal kampüs erişimi) hakkında bilgilendirmek" ve "öğretim elemanlarının enformasyon ve iletişim teknolojileri kullanımını, alan uzmanlık yeterliğini ve öğretim stratejilerini geliştirmektir".

2.1.2.1. Açık ve uzaktan öğrenmede teknik sorunlar

Açık ve uzaktan öğrenme sistemleri doğası gereği teknik sistemlerdir ve açık ve uzaktan öğrenme paydaşlarının sistemi benimsenmesine engel olabilecek kritik faktörlerin başında teknik sorunlar yer almaktadır (Almaiah, Al-Khasawneh ve Althunibat, 2020; Yumurtacı, 2020). Teknik destek, öğrenenlerin öğrenme süreçlerindeki motivasyon ve devamlılığı üzerinde pozitif bir etkiye sahiptir (Alshammari, 2020; Antwi-

Boampong, 2021). Dolayısıyla açık ve uzaktan öğrenme süreçlerini verimli yürütebilmek için teknolojik engellerin ve sorunların giderilmesi gerekmektedir. Bu bağlamda, teknik sorunlara yönelik tanımların incelenmesinin faydalı olacağı düşünülmektedir.

- Teknik sorunlar, teknik destek hizmeti eksikliğinde ortaya çıkan ve öğrenme süreçlerini olumsuz etkileyen tutarsız öğrenme platformları, tarayıcılar veya yazılımlar ile ilgilidir (Muilenberg ve Berge, 2005).
- Teknik sorunlar, hem öğrenme-öğretme süreçlerini hem de teknik yeterliklerin geliştirmesini sekteye uğratabilir (Gutiérrez-Santiuste, Gámiz-Sánchez & Gutiérrez-Pérez, 2015).
- Teknik sorunlar; yetersiz altyapı, teknolojik arızalar, elektrik kesintileri veya internet erişiminde/ hızında aksaklık gibi sebeplerden kaynaklanabilir (El Turk ve Cherney, 2016).
- Teknik sorunlar, açık ve uzaktan öğrenme sistemlerinde karşılaşılan donanımsal ve yazılımsal sorunları kapsamaktadır (Durak, 2017).
- Teknik sorunlar; "çok modlu arayüz tasarlama", "öğrenenleri anlamak ve desteklemek için yeni teknikler oluşturma", "mobil öğrenenleri destekleyecek sistemlerin geliştirilmesi", "kişisel ihtiyaçlara yönelik bireysel hizmetlerin sunma", "etkileşim ortamları sağlama", "yeni öğrenme toplulukları oluşturma" ve "değerlendirme desteği sağlama" gibi endişelere sebep olmaktadır (Dhillon, 2020).

2.1.3. Açık ve uzaktan öğrenmeye yönelik güvenlik endişeleri

"Yazılım ve donanım arızaları", "ağ yapıları", "hizmet kalitesindeki sapmalar", "teknolojik eskime", "bireylerin kullanım hataları" veya "teknoloji kullanımındaki yetersizlikleri" (Alwi ve Fan, 2010; Minh Hoang vd., 2020) gibi teknik sorunlarla yakın temas halinde olan siber endişelerin, daha önceki tanımlar doğrultusunda açık ve uzaktan öğrenme sistemlerini de ilgilendirdiği söylenebilir. Öğrenmenin insana, mekâna, zamana, fikre ve yönteme açık olduğu bu sistemler, doğası gereği çevresi ile etkileşim halindedir (Fırat, 2021).

Açık ve uzaktan öğrenme sistem altyapılarının; öğrenenleri, öğretenleri, idari personeli ve en önemlisi verilerin oluşturulduğu ve işlendiği kritik bir dijital altyapıyı içerdiğini söylemek mümkündür. Dolayısıyla bu sistemlerdeki dijital etkileşimin çok yönlü ve çok kapsamlı bir yayılım gösterdiği öngörülebilir. Bunun sonucunda ise düşük güvenlik önlemlerine sahip açık ve uzaktan öğrenme sistemleri; farklı konumlardaki, rollerdeki veya pozisyonlardaki saldırganlar tarafından gerçekleştirilebilecek çeşitli ataklara açıktır (Minh Hoang vd., 2020; Ulven & Wangen, 2021). Bu nedenle açık ve uzaktan öğrenme sistemlerinin siber uzamın dinamik zorlukları karşısında istikrarlı bir kurumsal yapılanma ile sistem güvenliğini ve devamlılığı sağlayabilmesinin oldukça önemli olduğu düşünülmektedir.

2.2. Siber Güvenlik

Enformasyonun şekillendirdiği 21.yüzyıl dünyasındaki bilgi-işlem ortamları ve bilgisayar uygulamalarının, binlerce aktif kullanıcının katılım gösterdiği dijital ağ ve teknoloji yapılarını geliştirerek hızlı bir değişimin ve dönüşümün temsilcisi olduğu söylenebilir. Dijital teknolojiler paydasında avantaj sağlayan bir değer olarak pek çok sektör tarafından benimsenen bu gelişmelerin, beraberinde saldırı ve suç faaliyetlerini barındıran bir ortamın oluşumuna zemin hazırladığını söylemek mümkündür.

Dijital saldırı ve suç faaliyetlerinin gerçekleştiği ortamı ifade eden *siber uzam*daki önlem ve savunma süreçlerinin terimsel karşılığı olan siber güvenlik; verileri, bireyleri, ağları, cihazları, programları, sistemleri, kurumları ve hükümetleri çeşitli saldırılara karşı korumayı ifade etmektedir (Fischer, 2016; Minh Hoang vd., 2020). Koruma faaliyetleri ile siber uzamda gizliliği, bütünlüğü ve erişilebilirliği korunan varlıkların güvende olduğunu söylenebilir. Bununla birlikte farklı ilkeler ışığında da güvenliği pekiştirmek mümkündür (Bkz. Tablo 2.1).

Tablo 2.1. *Güvenlik ilkeleri (Çalışkan, 2015, s.40)*

Güvenlik İlkeleri	Özellikler
Gizlilik	Sistem ve veriler yetkili kişinin (kullanıcının) kontrolünde mi?
Bütünlük	Sistem ve veriler orijinal haliyle saklanabiliyor mu?
Erişilebilirlik	Sistem ve veriye istenilen anda ulaşılabiliyor mu?
İzlenebilirlik	Sistemde gelişen her olay daha sonra ulaşılıp incelenebiliyor mu?
Kimlik Sınaması	Sistemi kullanan veya veriyi paylaşan taraflar, olması gereken kişiler mi?

Tablo 2.1. (Devam) *Güvenlik ilkeleri (Çalışkan, 2015, s.40)*

Güvenirlik	Sistem, kendisinden beklendiği gibi çalışıyor mu? Tutarlı mı?
İnkâr Edememe	Bilgi ve veriyi paylaşanlar kimliklerini doğrulayabiliyor mu?

Gizlilik ilkesinin sistemde yer alan verilerin, kullanıcıların ya da sistemin kendisinin yetkisiz ve izinsiz erişime ya da kullanıma karşı korunmasını temsil ettiği söylenebilir. Verilerin, kullanıcıların ya da sistemlerin yetkilendirilen kullanıcılar tarafından kullanılmasını ifade eden bu ilkenin, bireysel ve kurumsal düzeyde verilerin ve sistemlerin yetkili kullanıcılar tarafından kontrol edilme düzeyine karşılık geldiğini söylemek mümkündür. Bunun yanı sıra izinsiz erişilen sistemin ya da sistem varlıklarının bozulması, değiştirilmesi, istenmeyen ekler yapılması, bilgilerin bir kısmının veya tamamının silinmesinin engellenmesi gerekir" (Çalışkan, 2015, s.41). Bütünlüğü temsil eden bu ilke ise bireysel ya da kurumsal varlıkların gerektiği özgün halleriyle muhafaza edilerek veri ve sistem bütünlüğünün sağlanmasını ifade etmektedir. Sistem varlıklarının her an ve her koşulda kullanıma ve ulaşıma açık olmasını ifade eden erişilebilirlik ilkesi ise yine bireysel ve kurumsal kapsamda açıklık çerçevesinde eksiksiz ve sürekli faaliyet göstermeyi işaret etmektedir. Bu ilkenin, sistemlerin ve sistem varlıklarının yetkili ve izinli kullanıcılar tarafından eksiksiz ve süreğen bir performans gösterebilmeleri adına açık politikalar benimsemeyi hedeflediği söylenebilir.

Siber uzamda gerçekleşen olayların izlerini takip etmeyi ifade eden izlenebilirlik ilkesi; kullanıcıların sistemdeki hareketlerini, yapılan paylaşımları, servis ve yazılım faaliyetlerini kayıt altında tutarak gerek sistem gerekse ağ yapıları üzerindeki faaliyetleri izleyebilmeyi, inceleyebilmeyi ve değerlendirebilmeyi ifade etmektedir (Çalışkan, 2015). Kimlik sınaması ilkesinin ise, sisteme ya da sistem varlıklarına erişim sağlayan kişilerin yetkilendirilmiş kişiler olduğunu doğrulamakla ilgili olduğu söylenebilir. Bir sistemin ya da sistemde yer alan varlıkların beklenen performansları ile mevcut performansları arasındaki tutarlılık derecesini ifade eden güvenirlik ilkesinin ise, performans sonuçlarının her seferinde istek ve beklentilere cevap veren tutarlı çıktılar üretmesi ile ilgili olduğunu söylemek mümkündür. Bunların yanı sıra, inkâr edememe ilkesi ile varlıkların, varlık paylaşımlarının ve bu paylaşımın taraflarının güvenli bir şekilde doğrulanması hedeflenmektedir.

2.2.1. Siber uzam

Canlıların yeryüzündeki felsefi varoluşunu anlamak ve anlamlandırmak için sorgulanan en temel kavramlardan biri olan "varlık"; bireyleri, ilişkileri, zamanı, hafızayı veya hatırayı soyut ya da somut olarak barındıran "mekân" algısıyla yakından ilişkilidir (Çiftçi & Karakuş, 2019). İnsanı etkileyen ve dolayısıyla insanda iz bırakan mekân algısının, iletişimin oluşturulduğu, dönüştürüldüğü ve taşındığı bir kanalı temsil ettiği söylenebilir. Nesne-düşünce düzeni arasındaki ilişkinin değişmesini ve dönüşmesini ifade eden çağ değişimlerinin, iletişim kanallarındaki ontolojik algının da değişmesini tetiklediğini söylemek mümkündür. Bu; telgraf, telefon, radyo ve televizyon, bilgisayar ve internet gibi teknolojik ve dijital devrimlerin mekân algısını değiştirdiğini ve dönüştürdüğünü işaret etmektedir.

Dijital dinamizmle şekillenen ve dijital dinamizmi şekillendiren küreselleşme, küresel somut düzeni dijital bir forma dönüştürerek yerleşik-somut mekân algısını "*boyutsuz mekân*" veya "*siber-mekân*" (Çiftçi & Karakuş, 2019, s.14) olarak yapılandırmıştır. İlk defa Kanadalı yazar William Gibson (1984)'ın bilim kurgu romanı *Neuromancer*'da internet yapısını ve kapsamını betimlemek için kullandığı "*siber uzam (cyberspace)*" terimi, bahsi edilen yapılanmayı temsil etmektedir. Teknolojik varlıkların sırasıyla dijitalleşmesi, ağ yapısına dahil olması ve veri akışı sağlayan iletişim araçlarına dönüşmesi (ör. enformasyon ve iletişim teknolojileri), sürekli gelişmekte olan siber uzamı meydana getirdiği söylenebilir. Bu süreğen gelişim aynı zamanda siber uzamdaki tehdit ortamlarını ve uygulamalarını da çeşitlendirerek potansiyel saldırıların kapsamını da genişletmektedir (Jang-Jaccard & Nepal, 2014; Ulven & Wangen, 2021).

2.2.2. Siber saldırı türleri

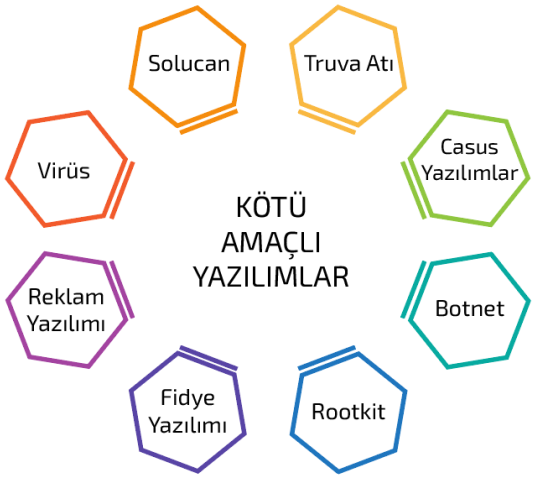
Siber güvenliğin sağlanmasındaki mücadele, teknolojik gelişmeler ışığında gitgide zorlaşmaktadır (Jang-Jaccard & Nepal, 2014; Khan, Brohi & Zaman, 2020). Enformasyon ve iletişim teknolojileriyle etkileşim halinde olan verilerin, bireylerin ve sistemlerin hassas ve savunmasız yönlerinden yararlanan yetkisiz bilgisayar korsanları, saldırganlar, hırsızlar ya da dolandırıcıların, siber uzamda fiziksel ve dijital sonuçları olan yasa dışı eylemler gerçekleştirdiği söylenebilir. Saldırganlar; sistem açıklarını, güvenlik politikası kusurlarını ve hatta fiziksel güvenlik boşluklarını kullanarak, sistemlere ve gizli

bilgilere yetkisiz erişim elde edebilirken hizmetlerin kullanılabilirliğini bozabilmekte ve finansal kayıplara neden olabilmektedir (Nespoli, Papamartzivanos, Mármol & Kambourakis, 2018).

Dijitalleşen küresel düzeninin yaşantısını ve etkileşim ögelerini giderek daha fazla içine alan siber uzamın, yalnızca suç unsurlarının yürütülmesi için kârlı bir pazar oluşturmakla kalmayıp aynı zamanda suçluların yakalanma riskini de en aza indirdiğini söylemek mümkündür. Bu doğrultuda, fiziki sınırları olmayan sonsuz bir coğrafyayı temsil eden siber uzamdaki saldırıların anonim saldırganlarca yürütülmesinin bu saldırıları takip ve tespit etmeyi zorlaştırdığı da düşünülebilir. Ek olarak, bir saldırıyı gerçekleştirmek için en azami ihtiyacın bir bilgisayar ve ağ bağlantısı olması, düşük maliyetinden dolayı siber saldırıları cazip ve kârlı kılmaktadır (Jang-Jaccard & Nepal, 2014). Bununla birlikte siber saldırılar, saldırganın yaklaşımına ve belirlediği amaca göre çeşitlenebilmektedir.

2.2.2.1. Kötü amaçlı yazılım (malware)

Geniş bir saldırı sınıfını oluşturan kötü amaçlı yazılımlar, saldırıların hedefindeki varlıkların ve sistemlerin güvenlik açıklarından faydalanarak faaliyet gösteren en yaygın siber saldırı türüdür (Jang-Jaccard & Nepal, 2014; Ulven & Wangen, 2021). Ticari, askeri veya tamamen kişisel çıkarlar doğrultusunda planlanan tehlikeli girişimleri ifade eden kötü amaçlı yazılımlar; varlıkları, cihazları, sistemleri veya kurumsal faaliyetleri etkilediği gibi, doğrudan bireylerin ve toplumların zarar görmesine yol açabilmektedir. Bu yazılımları kapsamına ve amacına göre farklı başlıklar altında incelemek mümkündür (Bkz. Şekil 2.1).



Şekil 2.1. *Kötü amaçlı yazılım türleri*

2.2.2.1.1. Virüs

Kullanıcı izni ve yetkisi olmadan sisteme erişen ve kendini kopyalayarak çoğaltabilme özelliğine sahip olan virüsler; yürütülebilir dosyalar, Word belgeleri, virüslü web siteleri, eşler arası *(P2P-peer-to-peer)* dosya paylaşımı veya e-posta ekleri aracılığıyla bilgisayar sistemlerine sızabilmektedir (Jang-Jaccard & Nepal, 2014). Bir virüsün çoğalabilmesi ise, virüsü barındıran dosyanın veya programın çalıştırılarak virüsün aktif hale getirilmesine bağlıdır (Kaspersky, 2021). Aksi halde virüsün hareketsiz ve eylemsiz bir şekilde sistemde uykuda beklediği söylenebilir. Bununla birlikte farklı şekilde sınıflandırılabilecek ve tanımlanabilecek pek çok farklı virüs türünün bulunduğu siber uzamda her virüsün aynı şekilde yayıldığını söylemek mümkün olmayacaktır. Bu doğrultuda çeşitlenen virüs türleri aşağıdaki gibi sınıflandırılabilir (Bkz. Tablo 2.2).

Tablo 2.2. *Virüs türleri (Çalışkan, 2015)*

Virüs Türleri	Virüs Özellikleri	Etkileri
Dosya sistem virüsleri	Kendileri birer program olan ve genellikle çalışabilir programlara bulaşıp onlara yerleşen ve oradan diğer dosyalara yayılan virüsler	Çalışan programlar bozulabilir, kullanılmaz hale gelebilir, sabit diskte bulunan veriler silinebilir.
Ön yükleme virüsleri	Sistemin sabit disklerindeki ön yükleme dosyaları arasına sızan ve sistemin açılışıyla çalışıp yayılan virüsler	Bilgisayarların tüm işlemleri ve programların çalışması yavaşlar, sistemden veri kayıplarına neden olabilir.

Tablo 2.2. (Devam) *Virüs türleri (Çalışkan, 2015*

Makro yazılım virüsleri	Kelime işlemci programlar vb. yazılımlar gibi makro yazılımların içinde bulunan virüsler	Sistemdeki belge ve dosyalara zarar verir, belgelerde eksikler oluşur veya belgelere fazladan veriler eklenir, ağlar yoluyla diğer sistemlerdeki belgelere bulaşır ve onları değiştirir.
Web komut dosyası virüsleri	İnternette web sayfalarının kaynak kodu dosyaları içinde bulunan ve web sayfaları yoluyla bulaşan virüsler	Sistem dosyalarına zarar verir, kullanıcıları yanılır ve verilerin izinsiz paylaşılmasına neden olur.
Ağ virüsleri	Yerel ağlar veya geniş ağlarda hızla yayılan ve bulaşan virüsler	Kişisel bilgileri, şifreleri, hesaplarınıza ait bilgileri istenmeyen kişilerle paylaşabilir.
Yazılım bombaları	Belirli şartlar oluşana dek sistem içinde uyuyan ve bir etkiyle aktive olan virüsler	Belirli bir zaman diliminde veya farklı şartlar oluştuğunda etkinleşip sistemdeki dosyaları siler.

2.2.2.1.2. Solucan (worm)

Virüslerden farklı olarak herhangi bir müdahale olmaksızın bağımsız bir şekilde aktifleşen ve çoğalan solucanlar, virüslerin çok daha hızlı yayılan bir alt sınıfıdır (Kaspersky, 2021). Ağ bağlantısı ya da dosya indirme faaliyetleri aracılığıyla sistemlere sızabilen solucanların, kısa sürede oldukça fazla sayıda kopya üreterek bu kopyalarını ağ yapıları üzerinde yer alan savunmasız cihaz ve sunuculara yaydığı söylenebilir. Bu süreçte içinde bulundukları sistemlerin veri kaynaklarını (kayıtlı e-posta adresleri, sosyal medya kullanıcı listeleri, etkileşim kurulan ağ yapıları vb.) kullanarak yayılan solucanlar, bu sistemlerin bant genişliği ve ağ kaynaklarını da kullanarak ilgili sistemlerde dosya ya da veri kayıpları, yavaşlama, kilitlenme ve zayıflamalara sebep olabilmektedir.

2.2.2.1.3. Reklam yazılımı (adware)

Ağ geçmişinin izinsiz bir şekilde izlendiği cihaza otomatik olarak reklam gönderen reklam yazılımları, internet kaynaklı problemlerin başında yer almaktadır (Kaspersky, 2021). Ağ kullanıcılarının internet alışkanlıklarını ve geçmişlerini haritalayarak çeşitli manipülatif stratejilerle bu kullanıcıları kötü amaçlı yazılım barındıran web sayfalarına ya da dosyalara yönlendirme fikrini barındırdığı söylenebilir. Virüslerden farklı olarak bulaşma ve yayılma özelliği göstermeyen bu yazılımların, yalnızca kuruldukları cihazların ya da sistemlerin üzerinde aktif olarak faaliyet gösterdiğini söylemek

mümkündür. Sistem arka planında sürekli faal durumda olduğu için performans kaybına sebep olan bu yazılımlar kimi zaman işletim sistemlerine ve işletim sistemi dosyalarına zarar vererek ilgili sistemlerin zarar görmesine ve sağlıklı çalışmamasına sebep olabilmektedir. Veri toplayarak reklam görüntüleme amacı güden bu yazılımların, veri toplamak ve reklam görüntülemek dışında varlıklarını belli etmeyen ve sistem dosyalarında görüntülemeyen ve tespit edilemeyen yazılımlar olduğu söylenebilir.

2.2.2.1.4. Fidye yazılımı (ransomware)

Fiziksel yapılar ya da ağ yapıları aracılığıyla sistemlere sızdırılan bu yazılım, bulunduğu sistemdeki verileri, dosyaları veya kullanıcı izinlerini şifreleyerek bu varlıkların yasal sahibini erişim haklarını yeniden elde edebilmesi için ödeme yapmaya zorlamaktadır (Grimes, 2020). Kullanıcıların ödeme yapmayı reddetmesi halinde sistem varlıklarını ya da doğrudan sistem yapısı yok eden bu yazılımla saldırganların, kullanıcıların yasa dışı faaliyetler yüzünden verilerinin şifrelendiğini öne sürerek psikolojik bir yaptırım uyguladığı söylenebilir.

Kilitleyici ve şifreli olmak üzere yaygın iki türü bulunan bu yazılım sırasıyla temel bilgisayar işlevlerini engellemekte ya da bu işlevlere müdahale etmeden yalnızca verilerin şifrelemektedir (Kaspersky, 2021). Kilitleyici fidye yazılımlarında sadece kullanıcı hareketlerinin kısıtlanması hedeflendiği için veri kaybı oranının yüksek olmadığı söylenebilir. Fakat daha yıkıcı bir etkiye sahip olan şifreli fidye yazılımlarında veri kaybı olasılığının daha yüksek olduğunu söylemek mümkündür. Bu, bulut ya da harici depolama cihazlarının verilerin yedeklenmesinde kullanımının önemini işaret etmektedir. Bu tür saldırıların yaşanmış örneklerine Locky, WannaCry, Bad Rabbit, Ryuk, Shade/ Troldesh, Jigsaw, CryptoLocker, Petya, GoldenEye, GandCrab gibi saldırılar örnek olarak gösterilebilir.

2.2.2.1.5. Casus yazılımlar (spyware)

Kullanıcı alışkanlıklarını (tuş vuruşları, arama geçmişi, oturum açma bilgileri, dijital eğilim ve alışkanlıklar, banka bilgileri vs.) bir casus gibi izleyerek kayıt altına alan kötü amaçlı yazılım türüdür (Grimes, 2020). Bunun yanı sıra ağ bağlantısı kesintileri ve

güvenlik ayarı manipülasyonları gibi faaliyetlerde de kullanıldığı söylenebilir. Ağ bağlantıları ve internet tarayıcıları açıklarından faydalanarak bulaşabilen bu yazılımların anonim ya da farklı bir amaç kapsamında faaliyet gösteriyormuş gibi görünen sahte bir program aracılığıyla sisteme bulaştığını söylemek mümkündür. Bu programlara web siteleri ya da uygulamalar aracılığıyla indirilen oyunlar, müzikler, paylaşım dosyaları ya da farklı amaçlara hizmet eden internet dosyaları örnek gösterilebilir. Bu yazılımlar, sistemlerin yavaşlamasına sebep olduğu gibi hem sistemin hem de sistem varlıklarının kalıcı zararlar görmesine, manipüle edilmesine, faaliyetlerinin aksamasına ya da tamamen durmasına sebep olabilmektedir.

2.2.2.1.6. Truva atı (trojan)

Yunan mitolojisinin analog Truva atının, küresel bir kültür haline gelen dijital dönüşüm ile dijital bir form aldığı düşünülebilir. Virüs ve solucanlardan daha farklı bir yayılma politikası üzerine inşa edilen Truva atı; sistemlere, ağlara ya da sunuculara sızmak için kullanıcıları kötü amaçlı yazılımı indirmeye yönlendirmek için yasal bir yazılım kılığına bürünmektedir (Simmons vd., 2014). İki farklı dosya ile yapılandırılan Truva atlarının ilk olarak kullanıcının indireceği zararlı dosya ile sisteme konumlanırken ikinci olarak bu dosyanın aktifleştirilmesiyle sisteme erişim sağlanacak bir kapı açma prensibine dayandığı söylenebilir.

Erişim sağlanan sistem ya da sistem varlıklarının manipüle edilmesi, silinmesi ya da daha kritik zararların meydana gelmesi gibi sonuçları olan bu kötü amaçlı yazılım, virüslerden ve solucanlardan farklı olarak kişisel verileri doğrudan hedef aldığından daha tehlikeli bir yapı olarak değerlendirilebilir. Bununla birlikte, sisteme bir kapı üzerinden izinsiz ve yetkisiz erişim sağlanması, sistemin farklı türden siber saldırılara da daha hassas ve açık bir konuma geldiğini işaret etmektedir.

2.2.2.1.7. Botnet

Cihazlara, sistemlere ya da sistem varlıklarına bir e-posta eki, ağ bağlantısı ya da program aracılığıyla kötü amaçlı yazılım yerleştiren siber suçluların yerini uzaktan kontrol edilebilen yazılımlar, uygulamalar ya da komut dosyalarının almasını ifade eden

otomatikleştirilmiş robot yapılarını "bot" olarak adlandırmak mümkündür. "Zombi" olarak da ifade edilen bu yapının genellikle veri hırsızlığı, sunucu manipülasyonu ve çökmesi, kötü amaçlı yazılım üretimi ve dağıtımı gibi geniş kapsamı ve hedef kitlesi olan saldırıların otomatikleştirilmesini temsil ettiği söylenebilir. Bu şekilde kötü amaçlı yazılım bulaşan ağ yapıları ise "botnet" olarak adlandırılabilir.

Robotlaştırılan ağ yapısını ifade etmek için "robot" ve "network (ağ)" kelimelerinden türetilen botnet, otomatikleştirilmiş bir dizi faaliyeti gerçekleştirmektedir. Kötü amaçlı yazılım yaymak amacıyla ağ yapılarına sızan botnet, ağ üzerinden ele geçirilen cihazları uzaktan yöneterek saldırganın amacına göre farklılaşan hasarlar vermektedir (Karpersky, 2021). Kötü amaçlı yazılım bulaşmış makine kümelerinin yönetilmesiyle yapılan bu saldırı türünün bağlı olan cihazlar arasında komutlar aracılığıyla taşındığı ve yayıldığı düşünülebilir.

2.2.2.1.8. Rootkit

Virüs türevi bir kötü amaçlı yazılım olmasına rağmen virüslerden oldukça farklı olan rootkit, işletim sistemlerine sızarak uzaktan erişim ve kontrol yetkilerinin alınmasını sağlayarak uzaktaki kullanıcıların sisteme girebilmesi için bir arka kapı açmaktadır (Kaspersky, 2021). Bir bütün halinde işletim sistemi çekirdeğine gizlendikleri için rootkitlerin tespit edilmesinin oldukça zor olduğunu söylemek mümkündür. Tek bir yazılımın parçası olarak görülebilen Rootkit, çoğunlukla yetkili kullanıcı düzeyinde kontrol yetkilerinin elde edilmesine olanak sağlayan bir dizi araçtan meydana gelebilmektedir. Kelime anlamıyla Rootkit, yetkilendirilmemiş kök (root) veya yönetici düzeyinde erişime izin veren uygulamaların (kit) kullanımını işaret etmektedir.

Yetkisiz ve izinsiz erişim sağlanan sistemlerin bilgilerinin çalınması, bu sistemlerin birer botnet'e dönüştürülmesi ya da kötü amaçlı yazılımların yüklemelerinin yapılması gibi faaliyetleri kapsayabilen Rootkit, kapsamındaki cihazları dağıtılmış hizmet reddi saldırıları için de kullanabilmektedir. Bu doğrultuda farklılaşan amaçları ve eylemleri kapsayan Rootkit'leri aşağıdaki gibi sınıflandırmak ve tanımlaman mümkündür (Bkz. Tablo 2.3).

Tablo 2.3. *Rootkit türleri (Kaspersky, 2021)*

Rootkit Türü	Özellikleri
Donanım veya aygıt yazılımı Rootkit'i	Algılanması zor olan kötü amaçlı yazılımları yüklemek için doğrudan işletim sisteminin yerine cihazın aygıt yazılımını hedef alır. Donanımı etkilediği için korsanların kullanıcı tuş vuruşlarını kaydetmesi ve çevrimiçi etkinlikleri izlemesi mümkün olur. Diğer türlerden daha az yaygın olmakla beraber çevrimiçi güvenlik açısından ciddi bir tehdit oluşturmaktadır.
Ön yükleme Rootkit'i	Önyükleme mekanizması, işletim sisteminin bilgisayara yüklenmesinden sorumludur. Önyükleme rootkit'ler, cihazların gerçek önyükleyicisini korsan bir önyükleyiciyle değiştirerek bu sisteme saldırır. Böylece cihazların işletim sistemi tamamen yüklenmeden önce bile rootkit etkinleştirilmiş olur.
Bellek Rootkit'i	Rastgele erişim belleğinde (RAM) gizlenir ve arka planda kötü amaçlı etkinlikler gerçekleştirmek için cihazların kaynaklarını kullanır. Yalnızca RAM'de bulundukları ve kalıcı kod eklemedikleri için sistemin yeniden başlatılması durumunda bellek rootkit'leri kaybolur.
Uygulama Rootkit'i	Microsoft Office, Notepad veya Paint gibi programlara bulaşır. Saldırganlar, bu programlar her çalıştırıldığında cihaza erişebilir. Rootkit bulaşan programlar hala normal çalıştığından, kullanıcıların bunu algılaması zordur. Ancak antivirüs programları her ikisi de uygulama katmanında çalıştığından bunları algılayabilir.
Çekirdek modu Rootkitleri	İşletim sistemlerinin çekirdeğini (yani çekirdek düzeyini) hedeflediği için bu tehdidin en ciddi türlerinden biridir. Bilgisayar korsanları bu dosyaları yalnızca cihaz dosyalarına erişmek için değil, kendi kodlarını ekleyerek işletim sistemlerinin işleyişini değiştirmek için de kullanır.
Sanal Rootkitler	Kendisini bilgisayarın işletim sisteminin altına yükler. Daha sonra, hedef işletim sistemlerini sanal makine olarak barındırır ve bu, orijinal işletim sistemi tarafından yapılan donanım çağrılarına müdahale edebilmesine olanak tanır. Bu tür bir rootkit, işletim sistemini değiştirmek için çekirdeği değiştirmek zorunda değildir ve tespit edilmesi çok zor olabilir.

2.2.2.2. Oltalama (phishing)

İnternet tarihinin en eski ve en etkili saldırıları türlerinden birine örnek olan ve kimlik avı ya da oltalama olarak adlandırılabilen bu saldırı türü, güvenilir bir varlığın taklidi olan sahte bir kimlik aracılığıyla kişisel ve hassas bilgileri elde etmeye dayanmaktadır (Lallie vd., 2021). Genellikle e-posta yolu ile gönderilen bağlantıların yönlendirdiği paravan web sitelerine gömülmüş kötü amaçlı yazılımın cihazlara indirilmesine sebep olarak kullanıcıların verileri ve cihazları erişilir hale getirdiği söylenebilir.

2.2.2.3. SQL enjeksiyon

SQL (Structured Query Language/ Yapılandırılmış Sorgu Dili), genel hatlarıyla modern ve farklılaşan web geliştirme yazılımları aracılığıyla ilişkisel ve etkileşimli veri tabanları oluşturarak veri ekleme, düzenleme, değiştirme, yönetme ve silme gibi sorgularla içerik yönetim sistemlerini yapılandırmayı temsil etmektedir. Tarihi 1998'e

dayanmasına rağmen hala etkili bir şekilde kullanılan ve doğrudan veri tabanlarını hedef alan bu saldırı türünde güvenlik katmanları hassas veya yetersiz olan sistemlere SQL ifadeleri kullanarak erişilmektedir (Tuan, 2020; Turhost, 2021). Saldırganlar ile sistem arasındaki ara yazılımın güvenlik açıklarının ihlal edilmesiyle sistemdeki verilerin ele geçirilmesinin, manipüle edilmesinin, kontrol altına alınmasının ya da silinmesinin amaçlandığı söylenebilir.

2.2.2.4. Sosyal mühendislik

Genel yapısı oltalamaya benzeyen sosyal mühendisliğin, çok daha organize bir saldırı sürecini ifade ettiği söylenebilir. Bu saldırı türünde doğrudan bir hedef gözetilmektedir (Uslu, 2021). Aynı zamanda hedefin dijital yaşantısı yakın bir mercekten incelenip hedefe yönelik saldırı senaryoları oluşturularak bu kişilerin hassas verilerinin, kimlik veya banka bilgilerinin ele geçirildiğini söylemek mümkündür.

2.2.2.5. Ortadaki adam (man-in-the-middle)

Kablosuz ağ bağlantıları aracılığıyla gerçekleştirilen bu saldırılarda kişisel verilerin çalınması için ağ modemleri hacklenmektedir (Uslu, 2021). Genellikle halka açık alanlardaki ücretsiz ağ sunucuları üzerinden gerçekleştirilen bu saldırılar, modeme bağlanan kullanıcıların ağ geçmişleri aracılığıyla kişisel bilgilerini, paylaşımlarını, ekran görüntülerini ve ağ hareketlerini ele geçirebilmektedir.

İzinsiz bir dinleme sayılan ve gerçek zamanlı konuşmaları, ağ hareketlerini ve veri paylaşımlarını açığa çıkaran ortadaki adam saldırılarının "Sidejacking (yan oyun), Evil Twin (şeytan ikiz), sniffing (koklama)" gibi formlara büründüğü görülebilmektedir. Sniffing'de verilere müdahale etmek için bir yazılım kullanılırken cihazlara enjekte edilen kötü amaçlı yazılımın kendisini otomatik olarak tarayıca yüklemesi sağlanmaktadır (Turhost, 2021). Sidejacking'in oturum açma bilgilerini çalmaya ve bir kullanıcı oturumunu ele geçirmeye odaklandığı söylenebilir. Bunların yanı sıra Evil Twin'de ise saldırgan ortak kullanıma açık ücretsiz bir Wi-Fi ağının ele geçirilerek çoğaltılması ve gerçek ağda oturum açtığına inanan kullanıcıların verilerinin ele geçirilmesi amaçlanmaktadır (Turhost, 2021).

Ortadaki adam saldırılarının müdahale ve şifre çözme olmak üzere iki aşamadan oluştuğu söylenebilir. Müdahale aşamasında, bir Wi-Fi yönlendirici aracılığıyla ya da alan adı sistemi (DNS) sunucularının manipüle edilmesiyle erişim elde edilen ağda güvenlik açıklarının ve olası giriş noktalarının bulunmasını işaret etmektedir. İkinci aşama olan şifre çözmenin, çalınan verilerin şifresinin çözülerek siber suçlular tarafından anlaşılır hale getirilmesini kapsadığını söylemek mümkündür. Şifresi çözülen veriler; kimlik hırsızlığı, yetkisiz satın almalar veya dolandırıcılık amaçlı banka faaliyetlerinde kullanılabilir (Turhost, 2021).

2.2.2.6. Kripto hırsızlığı (cryptojaking)

Sömürülmüş *(exploited)* cihazlarla oluşturulmuş bir ağ üzerinden kripto para madenciliği yapma faaliyetlerini içeren bu saldırı, çok sayıda bilgisayarın botnet gibi kötü amaçlı yazılım aracılığıyla kontrol altına alınmasıyla gerçekleştirilmektedir (Uslu, 2021).

2.2.2.7. Sıfırıncı gün saldırıları (zero-day attacks)

İşletim sistemi araçlarının kurulumu ya da güncellenmesi aşamalarında oluşan güvenlik açıkları aracılığıyla sisteme sızma eylemlerini kapsamaktadır (Kron, 2021). Gerek kişisel gerekse toplumsal düzeyde hasarlar oluşturma potansiyeline sahip olan bu saldırının fark edilmesi en zor saldırı türü olduğu söylenebilir. "Sıfır gün", yakın zamanda keşfedilen ve bilgisayar korsanlarının sistemlere saldırmak için kullanabilecekleri güvenlik açıklarını açıklayan geniş bir terimdir (Kaspersky, 2021). Bu terim, siber sorunun ya da saldırının çok kısa süre önce öğrenildiği ve sorunun düzeltilmesi için "sıfır güne" sahip olduğunu işaret etmektedir.

Yazılımlarda genellikle korsanların tahribata neden olmak için kullanabilecekleri güvenlik açıkları bulunduğu söylenebilir. Bu doğrultuda yazılım geliştiricilerinin güvenlik açıklarını tespit ederek bu açıkları yamaladıklarını söylemek mümkündür. Yazılım geliştiriciler tarafında tespit edilen güvenlik açıkları, çoğu zaman siber saldırganlar, korsanlar ya da kötü amaçlı kişiler tarafından daha önce fark edilerek kodlar aracılığıyla sömürülebilmektedir. Bu doğrultuda bu şekilde faydalanılan sistem

açıklarının sistemi pek çok siber saldırının gerçekleştirilmesine açık hale getirdiği söylenebilir.

2.2.2.8. Dağıtık hizmet reddi (distributed denial of service-DDoS) saldırıları:

Web sitelerinin hizmet vermesini engelleyen siber saldırı türlerinden biri olan dağıtık hizmet reddi, cihaz ya da sistem açıklarının kullanılmasıyla gerçekleştirilmektedir (Uslu, 2021). Bu açıkların web sitesi hizmeti sunan altyapı ya da ağ yapılarındaki kapasiteden faydalanmayı temsil ettiği söylenebilir. Bu saldırı türündeki amaç, web sitesinin sunucu kaynağına çok sayıda istek göndererek bu kaynaktan aynı isteklere yanıt göndermesi için kaynak kapasitesini zorlamaktır. Sunucuların birim zamanda işleyebileceği istek *(request)* sayısının belirli bir kapasiteye sahip olması, sunucunun istek bombardımanı karşısında yanıt *(response)* veremez hale gelmesine sebep olabilmektedir. Sunucuların yavaşlaması, hasar görmesi ya da çökmesi gibi sonuçları olan bu saldırılarla web hizmeti sağlayan sistemlerin sunduğu hizmetleri engellendiğini söylemek mümkündür.

Bir web sitesinin, veri tabanının ya da sistemin hizmet vermesini engellemek amacıyla sistemdeki açıklardan faydalanan bu saldırı türünde, çok sayıda cihaz kötü amaçlı yazılım türlerinden biri olan botnet aracılığıyla ele geçirilmektedir (Tuan, 2020). Botnetlerin kontrol altına almasıyla birer *zombi*ye dönüşen cihazlar, hedef alınan yapıyı aynı anda istek bombardımanına tutarak yanıt vermesi için zorlamaktadır (Uslu, 2021). Aynı anda işlenebilecek istek sayısının sınırlı olması ise sistemleri yoğun istek karşısında yanıt veremez hale getirerek sunucularının çökmesine sebep olduğu söylenebilir.

2.2.3. Siber saldırıların olası fiziksel, psikolojik, sosyal ve zihinsel sonuçları

Hukuk, psikoloji, felsefe ve sosyoloji gibi çeşitli alanlarda derinlemesine araştırılan "zarar" kavramının siber bağlamda önemli ölçüde oldukça az ele alınan karşılığı, dijital altyapıları ve bu altyapıların etkileşim halinde olduğu veri, enformasyon, cihaz ve yazılımlar üzerinde gerçekleştirilen saldırı faaliyetlerinin sonuçlarını ifade etmektedir (Agrafiotis vd., 2018). *Etki (impact)* ve *risk* kavramları ile yakından ilişkili olan siber zarar kavramını, farklı boyutlarla sınırlandırmak mümkündür. Agrafiotis ve arkadaşları

(2018) literatürde yer alan pek çok tanımı sentezleyerek aşağıdaki gibi bir sınıflandırma oluşturmuştur:

- Fiziksel ya da dijital zarar
- Ekonomik zarar
- Psikolojik zarar
- İtibar Zararı
- Sosyal ve Toplumsal Zarar

Sistemlerin hasar görmesi ya da çalışmaması; veri dosyaların silinmesi, değiştirilmesi ya da bozulması; kullanıcı ya da sistem verilerinin sızdırılması ya da sistem varlıklarının fiziksel zarar görmesi gibi örnekleri olan fiziksel ya da dijital zararların, yaygın olarak görüldüğünü söylemek mümkündür. Diğer zarar türleri ile örtüşebilen ekonomik zararlar, siber saldırılar sonucunda finansal ve ekonomik olarak sistem bütçelerinde istenenin ve beklenenin dışında harcamalar ve kayıplar karşılaşılmasını işaret etmektedir. Saldırıya maruz kalan kişi ya da kurum personeli zihinsel ve ruhsal zararlar görebildiği gibi kurumsal kapsamda maruz kalınan saldırılarla kurumun kamu imajı zedelenerek güvensiz ve değersiz olarak damgalanabilmektedir. Bununla birlikte kamu algısındaki olumsuz etkilerin (örneğin bir saldırıdan sonra halk belirli bir teknoloji türünü ya da bunu piyasaya süren kurumu güvenilmez veya güvensiz olarak görmesinin), gündelik sosyal ve toplumsal yaşamının kesintiye uğramasına da neden olduğu söylenebilir.

2.2.4. Siber saldırı önlemleri

Potansiyel bir tehdit unsuru olan yetkisiz saldırganların fiziksel ya da dijital varlıklara, cihazlara ve sistemlere erişmesini önlemek amacıyla tasarlanan süreçler ve teknolojiler, siber saldırı risklerinin tespit edilmesinde ve önlenmesinde çeşitli çözüm önerileri sunmaktadır (Agrafiotis vd., 2018). Bir bilgi işlem cihazları sistemine veya çevrimiçi bir platforma/hizmete yönelik riskleri yönetmek için genel olarak güvenliği artırmak veya belirli riskleri ele almak için ek kontroller (karşı önlemler) uygulanabilir. Chowdhury, Adam ve Teubner (2020) karşı önlemleri 4 ana kategoride incelemiştir (Bkz. Şekil 2.2).

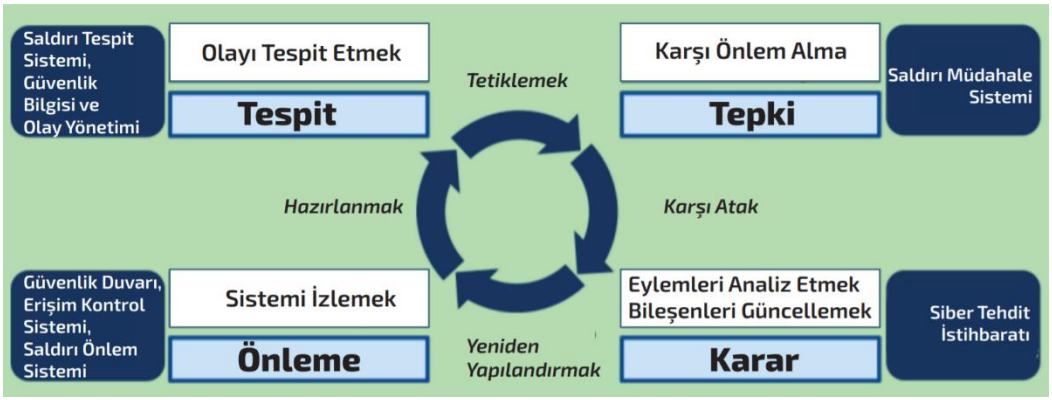
Şekil 2.2. *Siber saldırılara yönelik karşı önlemler (Chowdhurt, Adam & Teubner, 2020)*

Karşı önlemler her ne kadar belirli risklerin zararlarını önlemek ya da azaltmak için iyi niyetlerle ele alınıyor olsa da bu önlemlerin gerek kullanıcı gerekse sistem kaynaklı istenmeyen sonuçlar da doğurabileceğini söylemek mümkündür. Bununla birlikte, siber saldırıların hedefindeki varlıkların korunmasında, saldırıyı tespit etme ve önleme faaliyetleri kapsamında sarf edilen çabanın tek başına yeterli olmayacağı söylenebilir. Dinamik ve üssel bir hızla gelişim gösteren siber endişelerin fiziksel, psikolojik, sosyal ve ekonomik tüm sonuçlarını en aza indirmek için mücadeleci bir politika ile dinamik bir strateji geliştirerek faaliyete geçmek oldukça önemlidir (Nespoli, Papamartzivanos, Mármol & Kambourakis, 2018).

2.2.4.1. Siber savunma stratejileri

Yukarıda bahsi edilen saldırılar ve önlemler ışığında bilimsel topluluklar ve enformasyon ve iletişim teknolojileri endüstrisi, siber savunma çözümlerini sağlamlaştırmanın yollarını araştırmaktadır (Agrafiotis vd., 2018). Nespoli, Papamartzivanos, Mármol ve Kambourakis (2018) tarafından dört aşamalı bir döngü

olarak ele alınan siber savunma stratejisinin, bu arayışa yanıt olabilecek kritik önerilere, tekniklere ve yaklaşımlara değindiği düşünülmektedir (Bkz. Şekil 2.3).



Şekil 2.3. *Siber savunma döngüsü (Nespoli, Papamartzivanos, Mármol & Kambourakis, 2018)*

Önleme aşaması, olası bir güvenlik açığını ya da yanlış yapılanmayı keşfetmeyi amaçlayan girişimleri sürekli olarak izlemekten sorumludur (Nespoli, Papamartzivanos, Mármol & Kambourakis, 2018). Bu aşama için sürece dahil edilebilecek farklı yaklaşımlardan söz etmek mümkündür:

- Anti-Virüs Programları
- Güvenlik Duvarları
- Erişim Kontrol Sistemleri
- Saldırı Önleme Sistemleri
- Risk Değerlendirmeleri

Tespit aşaması, sistemdeki veya olası hassasiyetleri göz önünde bulundurarak güvenlik açıklarından yararlanmayı veya sistemi manipüle etmeyi amaçlayan müdahaleci olayları tanımlamaktan ve raporlamaktan sorumludur (Nespoli, Papamartzivanos, Mármol & Kambourakis, 2018). Bu aşamada kullanılan en yaygın yaklaşımlardan birinin ise *saldırı tespit sistemleri* olduğu söylenebilir. Temel amacı, kötü niyetli kişi ya da saldırıların faaliyetlerini önlemeyi kapsayan bu sistemlerin sistem ve sistem varlıklarını korumak için tehditleri değerlendirerek tanımladığı ve bunlarla ilgili olayların kayıtlarını tuttuğu; bu kayıtlar ışığında saldırıları minimize etmeyi sağladığını söylemek mümkündür.

Reaksiyon aşaması; ilk olarak saldırıyı hızla ortadan kaldırmak için en uygun, etkili ve verimli karşı önlemler kümesini sağlamakla; ikinci olarak ise, sistemi iyileştirmek ve normal durumuna geri getirmek için bir dizi eylem belirtmekle sorumludur (Nespoli, Papamartzivanos, Mármol & Kambourakis, 2018). Bu aşamada ise yoğunlukla *saldırı yanıt sistemi* yaklaşımlarının sürece dahil edildiği söylenebilir.

Son olarak, saldırıların püskürtülmesi ve sistemlerin optimize edilmesi sonucunda sistemin günlük dosyalarına kaydedilen eylemlerin analiz edilmesinden ***adli tıp aşaması*** sorumludur (Nespoli, Papamartzivanos, Mármol & Kambourakis, 2018). Böylelikle bu aşamadaki analizlerle, önleme aşamasını besleyen veriler, öngörüler ve sonuçlar elde edildiğini savunmak mümkündür.

Yukarıda bahsi edilen zorlu görevlerle uğraşmanın yükünü taşıyan güvenlik personeli ve yöneticiler, çeşitlenen saldırı senaryoları karşısında çoğu zaman güvenlik bütçesi kısıtlamaları ve katı bir tepki süresi sınırına sahipken izinsiz girişlere manuel olarak tepki vermek zorunda kalmaktadırlar (Nespoli, Papamartzivanos, Mármol & Kambourakis, 2018). Ayrıca, sorunun diğer temel parametreleri göz önüne alındığında, bir insanın tüm bu gereksinimleri uygun şekilde ele almasının neredeyse *imkânsız* olduğu söylenebilir. Sonuç olarak, insan operatörleri veya güvenlik görevlileri gibi kaynakların yetersizliğini ve bilişsel faktörlerden kaynaklanabilecek olası sınırlılıkları ve riskleri gidermek için verimli bir "tam" veya "yarı otomatik" karar destek sistemlerine ihtiyaç olduğunu söylemek mümkündür.

2.3. Sınırlı Rasyonellik Kuramı

Akıl yürütme ve karar verme süreçlerinin bir davranış bileşeni olarak görülen rasyonellik, başta Yunan filozofları olmak üzere klasik dönemlerden itibaren pek çok düşünürün ve araştırmacının tartışmalarına ve çalışmalarına konu olmuştur (Simon, 2000). Minimum çaba ve maliyet ile maksimum fayda elde edebilmek için var olan bilgilerin eksiksiz ve duygulardan arındırılmış bir şekilde kullanılmasını ifade eden rasyonelliğin; çoğun aza tercih edilmesi, karmaşık problemlerin çözülmesi, farklı alternatifler arasında en iyi seçimin yapılması, tutarlı davranılması ve belirli çıkarlar gözetilerek mantık çerçevesinde eski deneyimlere uygun hareket edilmesi davranışlarını ifade ettiği söylenebilir. Fakat 1947'de *Yönetsel Davranış (Administrative Behavior)* adlı

kitabında Herbert Simon, ilgili karar verme süreçlerinin sınırlı bir bilişsel kapasite dahilinde dışa vurulan davranışlar olduğunu sınırlı rasyonellik kuramıyla öne sürmüştür.

Öngörülen bir değişimin meydana gelmesindeki olasılığın bu değişimin ek bilgilerden ve değerlerden ne derece etkilendiğini inceleyen Bayesyen karar verme teorisinin öncüsü olan Leonard J. Savage (1954), neoklasik ekonomide rasyonelliğin "tutarlılık", "beklenen fayda maksimizasyonu" ve "öğrenme söz konusu olduğunda olasılıkların Bayesçi yolla güncellenmesi" olmak üzere üç ayağı olduğunu savunmuştur (Gigerenzer, 2021). Bu üç ayağın oturduğu zemini oluşturan temel iki şarttan bahsetmek mümkündür: Gelecekteki durumlara ve bu durumların sonuçlarına dair *mükemmel* öngörü. Ancak Simon yaptığı gözlemler ve deneyler sonucunda karar birimlerini temsil eden bireylerin, yöneticilerin ya da organizasyonların mükemmel öngörüler ile beklenen fayda maksimizasyonunu sağlayamayan ve Bayes güncellemesi varsayımlarını karşılamayan durumlarla uğraşmak zorunda olduklarını fark etmiştir (Gigerenzer, 2021).

Tamamıyla rasyonel kararlar verebilen akılcı birey (*homo economicus*) tanımını iktisat çatısında birçok çalışmayla ele alan Simon'a göre, bireylerin hesaplama, akıl etme ve karar verme yeteneklerinde göz ardı edilemeyecek bilişsel sınırlar bulunmaktadır (İskender, 2019; Simon, 2000). Karar verme süreçlerinde karar birimlerinin (bireyler, kurumlar ya da organizasyonlar) bilişsel kapasitelerinde bir doygunluk sınırı olduğunu belirten Simon, karar süreçlerindeki mevcut alternatiflerin bireysel sınır ya da sınırlılıklar çerçevesinde karar süzgecinden geçirildiğini belirmiştir (Tozlu, 2016). Çünkü "*karar birimleri birer bilgisayar değil, pratik varlıklardır: Kaynaklar yani bilgi, zaman, otokontrol ve deneyimler sınırlı; karar birimleri sezgiseldir*" (Kamber & Süslü, 2020, s.328).

Rasyonellik ile irrasyonelliği ayıran çizgide konumlanan sınırlı rasyonelliğin, karar vericilerin rasyonel olmak için hedef odaklı, uyarlanabilir ve kasıtlı davranışlarda bulunduğunu; fakat bu bireylerin bilişsel ve duygusal kapasitelerinin ilgili karar verme süreçlerinde tutarsız, başarısız veya yanlış seçimler yapmasına sebep olduğunu savunduğu söylenebilir. Bu noktada, bireyin karar verirken rasyonellik tanımına uymuyor olması karar vericilerin, karar süreçlerinin ya da sonuçlarının tamamen irrasyonel olduğu anlamına gelmediğine dikkat edilmelidir. Mükemmel bir rasyonellik önermesini geçersiz kılan çevresel ve kalıtsal faktörler; karar vericilerin bilgi, hesaplama ve zaman yönetimi

yeteneklerini kısıtlayan sınırlarla başa çıkılması gerektiğini göstermektedir (Kamber & Süslü, 2020).

Davranışsal iktisadın temelini oluşturan sınırlı rasyonellik kuramı, verilecek kararın ne olduğuyla değil karar verme sürecinin kendisiyle ilgilenmektedir (Kamber & Süslü, 2020; Mintrom, 2015). Karar mekanizmasının en iyi sonuca değil; yeterince iyi bir çözüme ulaşmasının beklendiği söylenebilir. Başka bir ifadeyle, "*burada temel fikir optimizasyon değil, yeterince tatmin olmaktır*" (Kamber & Süslü, 2020, s.328). Çünkü her ne kadar bireylerin davranışlarının altında yatan nedenler olsa da bu nedenlerin nadiren en iyi karar süreçlerini barındırdığı ve nadiren tutarlı olan seçimleri oluşturduğu düşünülebilir. Bu doğrultuda "*optimizasyon, tatmin etmenin düşmanıdır*" (Simon, 2000, s.26) görüşünü savunan Simon (1972), bireysel ve organizasyonel rasyonelliği sınırlayan üç temel faktörden bahsetmiştir:

- Risk ve belirsizlik,
- Alternatifler hakkında eksik enformasyon,
- Karmaşıklık.

İnsanların yalnızca risk değil, aynı zamanda belirsizlik altında da karar verme süreçleri incelendiğinde bu faktörlerin karar birimlerinin seçimlerini etkileyen kritik faktörler olduğu görülmektedir (Gigerenzer, 2021). Bunu açıklamak için oyun teorilerini baz alan Simon (1972: 2000), karar süreçlerindeki risk ve belirsizlik şartlarını satranç ile betimlemiştir (Cristofaro, 2017; İskender, 2019). Rakip oyuncunun önceki hamlelerini akılda tutarak sonraki hamlelerini tahmin etmek bir belirsizlik taşımaktadır ve yapılacak hamleler bu belirsizlik doğrultusunda risk almayı işaret etmektedir. Risk ve belirsizlik çerçevesinde tam rasyonel kararlar vermenin mümkün olmadığını gösteren bu yaklaşımla Simon (1972), bilişsel kapasitenin sınırlı bir hesaplama, öngörü ve karar mekanizmasını temsil ettiğini vurgulamıştır.

Karar verme; bir soruna, duruma ya da kestirime ait alternatifler arasından şartlar dahilinde en uygun olanının seçilmesini ifade etmektedir (Tozlu, 2016). Bu doğrultuda rasyonellik, karar vericinin olası alternatifler arasında kâr olasılıklarının dağılımını bildiğini varsaymaktadır (Simon, 1972). Karar vermeyi "belirli amaçlar doğrultusunda belirli alternatifler arasından bilinçli bir seçim yapmak" olarak ifade eden Simon, karar süreçlerinde "*amaç-bilinçlilik-seçim*" bileşenlerine vurgu yapmaktadır (Tozlu, 2016). Bu,

sürece dahil olan bileşenlerin bireysel bir doygunluk sınırına sahip olduğunu ve alternatiflerin bu sınırlar kapsamında belirlendiğini işaret etmektedir.

1950'lerin sonlarında, nispeten karmaşık psikolojik fenomenleri sembolik süreçler düzeyinde modelleyen bilgisayar programlarının psikolojiye girişinin, bilişsel teori ve deneylerin güçlü bir şekilde yeniden canlanmasına yardımcı olarak sadece düşüncenin ürünlerine değil, süreçlerine de bakılmasını sağladığı düşünülebilir. 1960'lı yıllardan itibaren yapılan deneysel çalışmaları ve Simon'ın çıkarımlarını baz alan Selten (1990), rasyonelliği sınırlayan üç temel bileşeni farklı bir bakış açısıyla ele alarak Simon'ın yaklaşımına genişletilmiş bir bakış açısı getirmiştir.

Temelde "bilişsel, motivasyonel ve bilinçli zihindeki duygular" olmak üzere üç temada incelenen bu yaklaşımla bireylerin hesaplama ve düşünme yeteneklerinin rasyonellik üzerinde bilişsel sınırların oluştuğu öne sürülebilir. Bununla birlikte biliş ve karar mekanizmalarının ayrılmasından kaynaklanan motivasyonel sınırların "irade zayıflığını" tetikleyerek kişinin amaçları doğrultusunda en iyi kararı bilmesine rağmen buna paralel olarak hareket edememesine yol açtığı söylenebilir. Bilinçli zihindeki düşünce ve hayal gücünün yönünü kontrol eden öfke ve açlık gibi duygular veya korkular, dikkati geçici hedefler ya da korkularla ilgili çeşitli faaliyete odaklayarak motivasyon sistemindeki uzun vadeli hedeflerin ve kararların sapmasına yol açmaktadır (Selten, 1990).

Uzun kariyeri boyunca siyaset bilimi, ekonomi, psikoloji, bilgisayar bilimleri ve yapay zekâ gibi pek çok alana önemli katkılarda bulunan Simon, sınırlı rasyonellik kuramı sayesinde bireylerin problem çözme becerilerine dair gerçekçi yaklaşımlar sunmuştur (İskender, 2019; Jones, 1999; Mintrom, 2015). Bireylerin zihinlerinin otomatik süreçleri nedeniyle mantıksız davrandıklarını savunan sınırlı rasyonellik kuramının, karar vericilerin daima mantıklı davranan makineler olmadığını; bağımsız ve uyumsuz kararlar verebilen karmaşık varlıklar olduğunu Freudcu bir yaklaşımla öne sürdüğünü söylemek mümkündür. Bu doğrultuda "*Simon, karmaşıklık ve sınırlı rasyonellik kavramlarından yola çıkarak karmaşık yapıların anlaşılabilmesi için bilgisayar teknolojilerinin önemini vurgulamıştır*" (İskender, 2019, s.22). Bu bilgiler doğrultusunda siber güvenliğin sağlanması için gerçekleştirilen öngörü, tespit, önlem ve savunma faaliyetlerindeki karar süreçlerinin sınırlı bir rasyonellikle değerlendirildiği; bu

süreçlerin veri, birey ya da sistem güvenliğini ve sürdürülebilirliğini sağlamak adına daha rasyonel yapılarla desteklenmesi gerektiği söylenebilir.

2.4. Endüstrileşme Kuramı

İnsanlık tarihinde benzeri olmayan bir döneme karşılık gelen endüstrileşme, pek çok alanda çarpıcı değişiklikler meydan getirerek modern ekonominin ve toplumların yanı sıra post-modern toplumları da şekillendirerek insanlığın gelişiminde ve değişiminde etkili bir rol oynamıştır (Birochi & Pozzbon, 2011; Peters, 1993: 2010). Geniş bir zaman dilimini temsil eden endüstrileşme sürecinin, devam etmekte olan bir gelişim ve etkileşim alanına sahip olduğunu söylemek mümkündür. Pek çok farklı zaman dilimini ya da dönüm noktasını baz alarak incelenebilecek olan endüstrileşme süreci, Peters (2010) tarafından üç kritik dönem şeklinde ele alınmıştır:

I.Dönem (Endüstri Öncesi Dönem): 18. Yüzyılın sonlarına denk gelen sanayi toplumunu kapsayan bu dönemde, üretim süreçlerinde yeni enerji kaynaklarının kullanılması, yeni iş kollarının oluşturulması, işçi sayısındaki artış, demir ve karayolu altyapılarının geliştirilmesi, postanelerin açılması ve fabrikaların yoğunlaşmasıyla şehirleşmenin hızlanması, tarım toplumundan sanayi toplumuna kademeli bir geçişe zemin oluşturarak "işçiler" ve "girişimciler" olmak üzere iki sosyal türü meydana getirdiğini söylemek mümkündür.

II.Dönem (Endüstri Dönemi): Petrol, çelik, motorlu ulaşım araçları ve matbaa gibi yeni teknolojilerin endüstrileşmede meydana getirdiği hızlı yükseliş ile küresel boyuta ulaşan sermayenin, yeni yapısal değişiklikleri meydana getirdiği söylenebilir. El emeğinin azalıp profesyonel çalışmanın giderek baskın hale geldiği bu dönemde "rasyonellik ve verimlilik en önemli değerler haline gelmiştir" (Peters, 2010, s.12).

III.Dönem (Endüstri Sonrası Dönem): Hizmet, enformasyon ya da bilgi toplumunu olarak adlandırılabilecek toplumu oluşturan bu dönemde, giderek çeşitlenen endüstriyel yenilikler hızla yaygınlaşmış ve günlük yaşamın bir parçası haline gelmiştir (Birochi & Pozzbon, 2011). Gelişmiş ağ ve mobil teknolojileri, dijitalleşen toplum, küreselleşme, "bilgi işçisi" teriminin kullanımı, sanal çalışma ortamları ve bilginin artan değeri gibi kriterler, dönemin dönüm noktalarından yalnızca birkaçına örnek olarak gösterilebilir.

Endüstri paradigması, endüstri devrimine dayanan bürokratik modelin (Max Weber), bilimsel yönetim teorisinin (Taylor) ve idari teorinin (Fayol) ortaya çıkmasıyla ivme kazanan imalat süreçlerinden oluşan belirli bir üretim tarzıyla ilişkilidir (Birochi & Pozzbon, 2011). Endüstrileşmenin sadece teknik ve ekonomik özellikleri değil, aynı zamanda uzaktan eğitimin yaratılmasına, gelişmesine ve nihai yükselişine neden olan ve kolaylaştıran kültürel, sosyal ve toplumsal yönlerinin de olduğu söylenebilir. Bu, endüstrileşmenin dört bir koldan etkilediği alanlardan biri olan uzaktan eğitimin, uzun soluklu bir gelişim ve etkileşim birikiminden beslenerek varlık bulduğunu işaret etmektedir.

Eğitimin endüstrileşmiş yönünü ele alan endüstrileşme kuramına dair tartışmalar ve çalışmalar ilk olarak 1967 yılında Otto Peters tarafından başlatılmıştır (Peters, 2010; Zawacki Richter, 2019). O dönemde Charles Wedemeyer'in "bağımsız öğrenme" yaklaşımıyla şekillenen uzaktan eğitim konsepti ışığında Peters, uzaktan eğitimin organizasyonel yapılanmasını endüstriyel üretim süreçlerine benzetmiştir (Dikmen, Duman & Horzum, 2016; Garrison, 2000). Wedemeyer ve Peters'ın çalışmalarıyla teorik ve pratik olarak temelleri atılan İngiliz Açık Üniversitesinin, uzaktan eğitimin endüstrileşmiş somut ilk formu ve örneklerinden biri olarak tarihteki yerini aldığı söylenebilir.

Yazışmalı eğitimle uygulamaya konan ve kademeli olarak enformasyon ve iletişim teknolojileri ile şekillenen uzaktan eğitim faaliyetlerinin büyük ölçüde tekrar üretilerek kullanılmasının, eğitim materyallerinin üretiminde ve dağıtımında kitlesel ölçekte endüstrileşmiş bir modelin ortaya çıkmasını sağladığı söylenebilir. Eğitimin kendisinin değil, eğitsel faaliyet ve ürünlerin planlanması, tasarlanması, üretilmesi ve dağıtılması gibi süreçlerin endüstrileşmesini ele alan endüstrileşme kuramına göre endüstrileşen eğitim faaliyetleri en fazla uzaktan eğitim yapılanmalarında görülmektedir (Garrison, 2000; Peters, 1993: 2010). Bu doğrultuda uzaktan eğitimin endüstrileşmesini genel hatlarıyla ifade eden bazı belirleyici faktörler olduğu söylenebilir.

Planlama: Uzaktan eğitimin, öğretenlerin bütün bir yılı günü gününe kişisel yorum ve bakış açılarıyla planlamasından ziyade daha sistematik ve uzun vadeli bir planlama organizasyonuyla ilgilendiğini söylemek mümkündür. Çünkü doğası gereği çok fazla öğrenenin dahil olduğu uzaktan eğitimdeki öğrenme süreçlerinin etkililiği ve verimliliği;

titiz, dikkatli, yeterli ve kapsamlı bir organizasyon çerçevesinde yapılan planlamaya bağlıdır (Peters, 1993: 2010).

Organizasyon: Kurumsal amaçlar doğrultusundaki planlamalar ve faaliyetlerle genel ve kalıcı düzenlemeleri mümkün kılan organizasyon, uzaktan eğitim faaliyetlerinde belirlenen, oluşturulan ya da tasarlanan öğrenme-öğretme birimlerinin hedef kitleye ulaştırılmasını mümkün kılmak için izlenen yoldur (Simonson, Scholosser & Hanson, 1999).

Hazırlık çalışması: Uzaktan eğitim faaliyetlerinin başarılı olmasında belirleyici bir rolü olan hazırlık çalışmalarının, üretim süreçlerine dahil olan tüm paydaşların, faaliyetlerin, cihazların veya malzemelerin ortak bir paydada sağlayacağı faydanın etkisini arttırmak için oldukça önemli olduğunu söylemek mümkündür.

Uzmanlık: Uzaktan eğitim faaliyetlerinin düzenlenmesi, denetlenmesi, değerlendirilmesi ve geliştirilmesinde görev alan kişiler, belirli iş ve faaliyet birimlerine dair süreçlere ilişkin eğitim almış uzman kişilerdir (Peters, 2010).

İş bölümü: Öğretimin faaliyetlerinin öğreten, öğretmen veya öğretim görevlisinden planlanmış oranda arınmasıyla *öğrenme* faaliyetlerine dönüşmesi, uzaktan eğitim faaliyetlerinin basit bileşenlere ayrılarak veya alt görevlere bölünerek gerçekleştirilmesini gerektirmektedir (Peters, 2010; Simonson, Schlosser & Hanson, 1999). Bu durum, farklı uzmanlık alanlarını temsil eden farklı birimlerin etkili bir bütünü oluşturmasında iş bölümünün önemini işaret etmektedir.

Fonksiyon değişimi: Bünyesinde organize ve teknolojik süreçlerin gerçekleştiği uzaktan eğitim uygulamalarında, iş bölümüyle birimlere ayrılan faaliyet ve roller, uzaktan eğitimin dinamik doğası dolayısıyla süreğen bir değişime maruz kalmaktadır (Peters, 2010).

Rasyonelleştirme: Uzaktan eğitim faaliyetlerinin devamlılığının sağlanmasında az maliyet ile teorik olarak sınırsız sayıda öğrenene sabit kalitede ve yüksek verimle ulaşması için metodolojik önlemlerin alındığı rasyonelleştirme, tek bir bireyin (öğreten, öğretim görevlisi vb.) aktif rolünden koparılan ve iş bölümüne, otomasyona, mekanikleşmeye ve teknik yapılanmaya dayanan süreçleri ifade etmektedir (Simonson, Schlosser & Hanson, 1999; Zawacki Richter, 2019)

Makineleşme/ Mekanikleşme: Uzaktan eğitimde öğrenme ve öğretme süreçlerinin gerçekleştirilebilmesindeki koşullardan biri olan teknik ve teknolojik yapılanma, sürekli insan kontrolü gerektirmeyen çok sayıda cihazı ve faaliyeti kapsamaktadır (Peters, 1993:2010). Bu yapılanmanın ifade ettiği makineleşme/ mekanikleşmenin, öğrenme-öğretme faaliyetlerinin özgün ve yaygın değerlerini oluşturmada oldukça önemli olduğu söylenebilir.

Biçimlendirme/ resmileştirme (formalization): Uzaktan eğitimde üretim, denetim, değerlendirme ve dağıtım süreçlerinin hesaplanmış kurallar doğrultusunda belirlenmesini ifade eden resmileştirme, öğrenme faaliyetlerinin ve materyallerinin tekrarlanabilir olması amacıyla tasarlanan süreçlerin iyi ve kapsamlı bir şekilde tanımlanmış bir formata göre yapılanmasını gerçekleştirmeyi amaçlamaktadır (Peters, 2010).

Standartlaştırma: Uzaktan eğitim, oldukça geniş ve çeşitli öğrenen topluluklarına hitap edebilmek için eğitimin diğer formlarına kıyasla standartlaşmayı daha fazla benimsemeye eğilimlidir (Peters 2010; Zawacki Richter, 2019). Bu durum, amaca en doğru yoldan hizmet eden, düşük maliyetli ve düzenlenmesi kolay olan materyallerin türlerinin sınırlı sayıda ve çeşitlilikte üretilmesini işaret etmektedir.

Nesneleştirme: Uzaktan eğitim faaliyetlerinin programlanması, standartlaştırılması, biçimlendirilmesi, rasyonelleştirilmesi ve otomatikleştirilmesiyle bu süreçlerin büyük ölçüde nesneleştirildiğini söylemek mümkündür. Süreçte yer alan insan faktörünün duyarsızlaşmasına yol açan nesneleşme ile uzaktan eğitim "*sürekli ve deneysel olarak geliştirilebilen, makinelerle çoğaltılabilen, seri üretilebilen ve herhangi bir sayıda öğrenciye uyarlanabilen, satılabilen bir ürün haline gelmektedir*" (Peters, 2010, s.18).

Seri/ Toplu Üretim ve Dağıtım: Planlı ve organize bir seri üretim ile standartlaşmış birer nesneye karşılık gelen uzaktan eğitim içerik ve materyalleri, farklı ülkelerden çok sayıda öğrenenin farklılaşan beklenti ve ihtiyaçlarına hitap etmektedir (Peters, 2010). Standartlaşan nesnel materyallerin ise birim başına düşen maliyeti azalttığı söylenebilir. Bununla birlikte artan gelir, alanlarında uzman öğretenlerin sürece dahil edilmesini ve kaliteli bir destek yapısının sunulmasını ve yaygınlaşmasını mümkün

kılmaktadır (Peters, 2010). Çünkü "kitlesel eğitim, kitlesel üretime tekabül etmektedir" (Peters, 1993, s39).

Konsantrasyon ve merkezileştirme: İş bölümü ve seri üretim faaliyetleri için gerekli olan sermaye, beraberinde çeşitli endüstriyel endişeleri getirerek merkezi bir yönetim ve tekelleştirilmiş bir organizasyon yapısını gerekli kılmıştır (Simonson, Schlosser & Hanson, 1999). Bunun, genellikle tek bir kurumun ulusal ve uluslararası kapsamda uzaktan eğitim faaliyetlerini ve organizasyonunu üstlenerek merkez yapılı bir çalışma ağı şeklinde yapılanmasını beraberinde getirdiği söylenebilir.

Kontrol: Ampirik yöntemler kullanarak çalışma materyallerinin ve faaliyetlerinin etkililiğini, kalitesini ve geçerliğini sistematik olarak değerlendirerek öğrenme öğretme süreçlerinin düzenlenmesini, değiştirilmesini veya yürürlükten kaldırılmasını sağlayan kararları kapsamaktadır (Peters, 2010; Zawacki Richter, 2019).

Zaman-mekân ayrımı: Endüstri öncesi dönemde zanaatkar ile müşterinin zaman ve mekân mesafesinin endüstri dönemiyle birlikte giderek açılması, uzaktan eğitim paradigmasının endüstrileşme ile doğrudan benzerlik gösteren önemli bir yönüdür (Peters, 2010).

Montaj hattı: Peters (2010), uzaktan eğitim materyallerinin üretiminde parçaların oluşturuldukları andan bir araya getirilmesi sürecine kadar kademeli olarak gerçekleşen sevkiyat sürecinin Fordist üretim hattını andırdığını ifade etmiştir. Bu, uzaktan eğitim faaliyetlerinde montaj hattı uygulamalarının süreçlerin şekillendirildiğini ve sürdürüldüğünü işaret etmektedir.

2.5. Kuramsal Matris

Açık ve uzaktan öğrenmede siber güvenliğin teknik destek hizmetleri kapsamında ele alındığı bu çalışmada, Herbert Simon'ın sınırlı rasyonellik kuramı ile Otto Peters'ın endüstrileşme kuramı temel alınmıştır. Tablo 2.4'te yer alan kuramsal matris yapısını sınırlı rasyonellik kuramının "sınırlı bilgi, sınırlı yetenek, sınırlı değerlendirme, sınırsız belirsizlik ve sınırlı değerlendirme" şeklindeki beş prensibi ile endüstrileşme kuramının "rasyonelleştirme ve mekanikleştirme" prensipleri meydana getirmektedir. Endüstrileşme kuramı altında incelenen 16 prensipten yalnızca ikisinin (bkz.

rasyonelleştirme ve mekanikleştirme) açık ve uzaktan öğrenmede siber güvenliğin teknik destek hizmetleri kapsamında inceleneceği teknik yönlere vurgu yapacağı düşünülmektedir. Organizasyonel süreçlerin rasyonelliğinden bahsedebilmek için yine organizasyonel bir yönetim politikasını kapsayan siber güvenliğin yönetiminde sınırlı rasyonelliğin önüne endüstrileşme kuramı ile geçileceği öngörülmektedir. Bu araştırmada açık ve uzaktan öğrenmede organizasyonel bir endüstrileşmeyi ifade eden endüstrileşme kuramının (Peters, 2010) rasyonelleştirme ve mekanikleştirme prensiplerinin bu öngörüyü destekleyeceği savunulabilir.

Tablo 2.4. *Kuramsal Matris*

Açık ve Uzaktan Öğrenmede Siber Güvenlik		**Endüstrileşme Kuramı**	
		Rasyonelleştirme	Mekanikleştirme
Sınırlı Rasyonellik Kuramı	Sınırlı Bilgi	Sınırlı bilgiye sahip olan güvenlik uzmanları ve sistem paydaşlarının güvenliğini sağlamak için teknik destek hizmetinin otomasyon ve akıllı sistemler ile rasyonelleştirilmesi	Siber güvenliğin sağlanmasında sınırlı bilgi çerçevesinde yapılanan teknik destek hizmetinin güncel teknik ve teknolojik altyapılarla mekanikleştirilmesi
	Sınırlı Yetenek	Saldırı önlem ve savunma faaliyetlerinde sınırlı yeteneğe sahip olan teknik destek hizmeti uzmanlarının akıllı sistemlerle desteklenmesi	Teknik destek hizmeti uzmanlarının sınırlı yeteneği kapsamında sunulan güvenlik faaliyetlerinin teknik ve teknolojik mekanizmalarla zenginleştirilmesi
	Sınırlı Değerlendirme	Sınırlı değerlendirme yetisine sahip olan güvenlik uzmanları ve sistem paydaşları için teknik destek hizmeti kapsamında saldırı analitiklerinin yapılması	Siber saldırıların tespitinde sınırlı değerlendirme yetisine sahip teknik destek hizmeti uzmanlarının teknik, teknolojik ve analitik mekanizmalarla desteklenmesi
	Sınırsız Belirsizlik	Siber uzamdaki sayısız belirsizliğin riske attığı sistemlerin teknik destek hizmeti kapsamında akıllı öngörü sistemleri ile analiz edilmesi	Siber uzamdaki sayısız belirsizliğin tespitinde ve değerlendirilmesinde teknik destek hizmeti kapsamında otonom tekniklerin geliştirilmesi

3. YÖNTEM

Çalışmanın yöntem başlığı altında araştırma sürecinde benimsenen araştırma modeli, araştırma deseni, örnekleme yaklaşımı, katılım grubu, veri toplama aracı, veri toplama ve veri analiz süreçleri detaylı olarak ifade edilmektedir.

3.1. Araştırma Modeli

Açık ve uzaktan öğrenmede siber güvenliğin teknik destek hizmetleri kapsamında incelenmesi amaçlanan bu çalışmada nitel araştırma yaklaşımlarından durum çalışması benimsenmiştir. Nitel araştırmalar; görüşme, gözlem, doküman veya görsel-işitsel veriler aracılığıyla incelenen bir konunun ya da problemin bütüncül bir resmini kategoriler ve temalar yardımıyla çizmeye yaramaktadır (Yıldırım & Şimşek, 2013). Araştırmacılara dinamik ve esnek bir araştırma süreci ve alanı tanıyan nitel araştırma yaklaşımlarının, araştırmaların tasarlanması ve yürütülmesi süreçlerinde keşfedici bir yaklaşıma olanak sağladığını söylemek mümkündür.

Durumların ve olayların tanınması ve tanımlanması aşamalarında ayrıntıların niteliksel olarak detaylı bir şekilde incelendiği nitel araştırmaların bir bütünü oluşturan karmaşık sosyal etkileşimlerin ve ilişkilerin tümevarımsal bir yaklaşımla daha anlaşılır parçalar halinde incelenmesine olanak sağlandığı söylenebilir. Farklı bakış açılarının farklı veriler tarafından desteklenerek rapor edilmesine olanak sağlayan nitel araştırma yaklaşımlarının, farklı faktörleri kendi bağlamlarında gerçekçi, yakınsak, geniş ve bütüncül bir perspektiften incelemeye olanak tanıdığını da ifade etmek mümkündür. Baltacı (2019)'ya göre *"(...) bilginin derinliği ve özgünlüğünün önemli olduğu iddiasını savunan nitel araştırma, büyük örneklemler yerine daha küçük çalışma gruplarından elde edilen derin ve özellikli verilere*" (Baltacı, 2019, s.369) odaklanmaktadır.

3.1.1. Durum çalışması

Nitel araştırma yaklaşımlarından biri olan durum çalışması, sosyal bilimlerde sorgulayıcı araştırmaların yürütülebildiği önde gelen araçlardan biridir (Thomas, 2011). Durum çalışmaları, araştırmacı kontrolü dışında değişim gösteren olguların ve durumların meydana gelme sebeplerini, değişim süreçlerini ve sonuçlarını doğal ortamlarında

keşfetmek, anlamak, yorumlamak, tanımlamak, betimlemek ve değerlendirmek için sınırlandırılmış bir çerçevede "nasıl" ve "niçin" soruları kapsamında gerçekleştirilen sistematik araştırmalardır (Yıldırım & Şimşek, 2013). Kendi bağlamında incelenen bir olgunun ya da durumun ampirik ve analitik yollarla araştırılmasında başvurulan bir yaklaşım olan durum çalışması, birden fazla farklı kaynağın kullanımını mümkün kılmaktadır (Yin, 2017; Thomas, 2011).

Durum çalışması, ilgilenilen konunun veya sorunun bir bütün olarak ele alınmasını sağlayarak bu durumun ayrıntılı olarak incelenmesine ve durumun genellenmesine olanak sağlamaktadır (Thomas, 2021). Bu incelemelerin yapılacağı analitik süreçler ise dikkatle tasarlanmış sistematik adımlardan oluşmaktadır (Yıldırım & Şimşek, 2013). Bu doğrultuda yapılan genellemelerin istatistiksel değil analitik yollarla yapıldığına dikkat edilmesinin önemli olduğu söylenebilir.

3.1.2. Durum çalışması tasarımı ve planlama aşamaları

Bir durum çalışmasının tasarlanmasında Yin (2017) 'e göre üç temel adım vardır:

Durumun tanımlanması: Bir durum çalışmasının temel analiz birimi olarak işlev gören "durum", belirli sınırlar çerçevesinde incelenen bir yapıyı temsil etmektedir (Yin, 2017). Bu aşamanın alanyazın taraması yapılarak araştırma sorularının belirlendiği süreçleri kapsadığı söylenebilir.

Durum çalışması desenini belirlenmesi: Yürütülecek durum çalışmasında bir ya da daha fazla durumu kapsayan senaryoların "bütüncül" ya da "iç içe" olma durumları göz önünde bulundurarak tasarlanması gerekmektedir (Yin, 2017). Bu desen tasarımı taslağını bir matris üzerinde göstermek mümkündür (Bkz. Tablo 3.1).

Tablo 3.1. *Durum çalışmaları için dört temel tasarım (Yin, 2017)*

	Tek Durum Desenleri	Çoklu Durum Desenleri
Bütüncül (Tek Birim Analizi)	TİP I	TİP II
İç İçe Geçmiş (Çoklu Birim Analizi)	TİP III	TİP IV

Bu araştırmada, durum çalışması deseni olan bütüncül tek durum deseni (tip I) benimsenmiştir. Tek bir analiz biriminin olduğu bütüncül durum çalışmalarında üç farklı durumdan en az birinin varlığı bu desenin kullanımını gerekli kılmaktadır (Yıldırım & Şimşek, 2013). İlki, iyi formüle edilmiş bir kuramın teyit edilmesi veya çürütülmesi amacıyla bu desenin kullanımını gerekli kılan durumlar olarak ifade edilebilir. Özgün, aykırı veya aşırı durumların çalışılması da bu desenin kullanılması gerektiğine işarettir (Yıldırım ve Şimşek, 2013). Sonuncusunu ise, daha önce çalışılmamış veya ulaşılmamış bir durumun incelenmesinde bu desenin kullanımına ihtiyaç duyulduğunu işaret etmektedir. Bu doğrultuda ek bir durumu araştırmayı hedefleyen bu çalışmada bütüncül tek durum deseninin kullanılmasındaki neden, açık ve uzaktan öğrenme alanında siber güvenliğe yönelik çalışmalara erişilememiş olmasıdır.

Desen çalışmasını bir kuram çerçevesinde gerçekleştirilmesi: Bir durum çalışmasını şekillendirirken yöntem odaklı temel adımların belirlenmesinde izlenecek yolun derinliğini ve genişliğini ilgili çalışmada herhangi bir kuramın kullanılıp kullanılmadığı belirlemektedir (Yin, 2017). Bu bağlamda çeşitli önermelerle ve kuramlarla şekillendirilerek başlatılan bir durum çalışmasının, herhangi bir önerme ya da kuram çerçevesinde tasarlanmamış bir durum çalışmasından daha kolay ve etkili yürütülebileceğini söylemek mümkündür.

3.1.3. Durum çalışmasında verilerin toplanması ve analizi

Yin (2017), durum çalışmalarında yaygın olarak kullanılan 6 farklı veri toplama aracını "doğrudan gözlem, katılımcı gözlem, görüşme, doküman, arşiv kayıtları ve fiziksel yapılar" olarak tanımlamıştır. Bununla birlikte, durum çalışmalarında kaynağa bakılmaksızın hem nitel hem de nicel verilerden faydalanılabilir (Subaşı & Okumuş, 2016; Yin, 2017). Bu çalışma kapsamında veriler doküman inceleme ve görüşmeler aracılığıyla elde edilmiştir. Çalışmayı şekillendiren kuramsal iskeletin alanyazındaki çalışmalarla desteklenmesi için yapılan doküman incelemesi sonucunda yine kuramsal iskeleti yansıtan ve besleyen görüşme soruları oluşturulmuştur.

Farklı durumlar bağlamında farklı şekillerde incelenebilecek olarak durum çalışması araştırmalarının yürütülmesinde kalıplaşmış bir analiz sürecinden bahsetmek mümkün olmayacaktır (Yin, 2017). Bu doğrultuda, elde edilen bulguların analiz

edilmesinde yeteri kadar yazılı kaynak olmamasından kaynaklanan boşluğu, sürekli gelişmekte olan bilgisayar paket programlarının kısmen doldurduğu söylenebilir. Nicel verilerin analizinde kullanılan algoritmik yaklaşımlardan farklı olarak öyküsel veri analizlerine olarak sağlayan bu programlar elde edilen bulguların kodlanmasına, bu bağlamda çeşitli kategorilerin oluşturulmasına veya metinsel bulguların kelimesi kelimesine dökümünün alınmasına büyük oranda destek olmaktadır (Yin, 2017). Bununla birlikte verilerin analiz edilmesinde bazı teknikler de sürece dahil olarak öyküsel veri analizlerini kolaylaştırmaktadır (Subaşı & Okumuş, 2016; Yin, 2017).

3.2. Araştırma Deseni

Bu araştırmada, açık ve uzaktan öğrenmede siber güvenliği teknik destek hizmetleri kapsamındaki yerinin ve öneminin ne olduğu sorularına sınırlı rasyonellik ve endüstrileşme kuramları bağlamında yanıt aranmıştır. Açık ve uzaktan öğrenme, açık ve uzaktan öğrenmede destek hizmetleri, eğitim teknolojileri ve siber güvenlik alanlarında deneyimi olan uzmanların görüşleri doğrultusunda yeni ve bütüncül bir bakış açısı ortaya koymak amaçlanmıştır. Bu doğrultuda durum çalışması desenlerinden *bütüncül tek durum deseni* benimsenmiştir.

3.2.1. Amaçlı örnekleme

Nitel araştırma yaklaşımları, araştırma bulgularını belirli bir popülasyona genellemek yerine merkezi bir fenomeni, durumu ya da kavramı derinlemesine incelemeyi amaçlamaktadır (Creswell, 2013). Bu amaç doğrultusunda yürütülen araştırmalarda merkezi fenomeni anlamada, anlamlandırmada, yorumlamada, tanımlamada ve değerlendirmede farklı katılımcıların farklı bağlamlarda araştırma süreçlerine dahil olması gerekebilmektedir. Belirlenen çerçeve kapsamında araştırma sürecine dahil olacak katılımcıları ilgili sürece olasılıklı ve olasılıksız yaklaşımlarla dahil etmek mümkündür.

Evreni temsil etme koşulu aranmayan nitel araştırma yaklaşımlarında sürece dahil edilecek katılımcıların olasılıksız örnekleme yöntemi doğrultusunda araştırmaya dahil edildiği görülmektedir (Creswell, 2013). Bu araştırma kapsamında olasılıksız örnekleme

yöntemlerinde “amaçlı örnekleme” yaklaşımı benimsenmiştir. Bu yaklaşım, araştırma kapsamı ve amacı göz önünde bulundurularak görüş ve öngörülerine başvurulacak kişilerin kasıtlı ve bilinçli bir seçim ile sürece dahil edilmesini ifade etmektedir.

3.2.2. Katılımcılar

Nitel araştırmalarda katılımcılar, az sayıda kişiden oluşan fakat etkisi ve katkısı geniş hacimli bilgi kaynağı olarak görülen bir grup kişiyi temsil etmektedir (Fraenkel, Wallen & Hyun, 2012). Nitel araştırma yaklaşımlarından durum çalışmasının benimsendiği bu çalışmada amaçlı örneklemeyle seçilen katılımcılar, araştırmanın amacı çerçevesinde incelenen duruma yönelik görüşlerin araştırmanın doğal akışında ele alınabilmesi gözetilerek sürece dahil edilmiştir. Bu noktada araştırılan konuya yönelik tanımlamaların yapılabilmesi, durumların betimlenebilmesi ve problem durumların iyileştirilip geliştirilebilmesi için sürece dahil olacak veri kaynaklarının (katılımcı, ortam, olay ya da veriler) araştırma konusunu en çok besleyen ve destekleyen nitelikte seçilmesinin önemli olduğu söylenebilir. Bu doğrultuda araştırma dahil edilen uzmanlar amaçlı örnekleme yöntemlerinden ölçüt yaklaşımı ile sürece dahil edilmiştir. Ölçüt yaklaşımı ile sürece dahil edilen katılımcıların, aşağıda belirtilen kriterler göz önünde bulundurularak seçilmiştir. Bu kriterler araştırmanın amacına, kapsamına ve araştırmacının yaklaşımına göre şekillenebilir (Yıldırım ve Şimşek, 2013).

Araştırma amacı ve kapsamı doğrultusunda uzman görüşleri ile şekillendirilen bu çalışmada, sürece dahil edilen uzmanlar; “açık ve uzaktan öğrenme”, “açık ve uzaktan öğrenmede destek hizmetleri”, “eğitim teknolojileri” ya da “siber güvenlik” alanlarında en az 10 yıllık deneyime sahip olan ulusal ve uluslararası araştırmacılardır. Bu uzmanlar aynı zamanda açık ve uzaktan öğrenme kurumlarında ya da birimlerinde görev yapan araştırmacılar arasından seçilmiştir. Teknik konulara ilişkin eğilimleri ve geçmişleri de göz önünde bulundurularak araştırmaya dahil edilen uzmanların, teknoloji kullanımı ileri düzey olan ve teknolojiyle öğrenme alanlarında çalışmaları bulunan araştırmacılar olması gözetilmiştir. Ayrıca uzmanların açık ve uzaktan öğrenmede destek hizmetleri ya da yönetsel faaliyetler hakkında deneyimlerinin olması da dikkate alınmıştır. Durum çalışmalarında sürece en az 4-5 katılımcının dahil edilmesi gerektiği (Creswell, 2013) göz

önünde bulundurularak 8 uzman ile araştırma süreci şekillendirilmiştir. Katılımcıların demografik bilgileri Tablo 3.2'de yer almaktadır.

Tablo 3.2. *Katılımcı listesi*

Katılımcıların Takma İsimleri	Kurum	Tecrübe
Emir	Atatürk Üniversitesi	19 yıl
Ayça	Eskişehir Teknik Üniversitesi	18 yıl
Burak	Anadolu Üniversitesi	12 yıl
Cem	Anadolu Üniversitesi	15 yıl
Ferhan	İngiliz Açık Üniversitesi	40 yıl
Ufuk	Anadolu Üniversitesi	20 yıl
Efe	Balıkesir Üniversitesi	13 yıl
Taylan	Anadolu Üniversitesi	11 yıl

3.2.3. Veri toplama araçları

Belirli durumlar ve olaylar hakkında esnek ve dinamik bir araştırma süreciyle ilgili koşulların parçalar halinde hem bütünlemesine hem de derinlemesine inceleme imkânı sağlayan nitel araştırmalarda farklı veri kaynaklarının kullanımından söz etmek mümkündür. Araştırma konusu olan olay ve durumların kendi bağlamlarında yorumlanarak incelenmesine olanak sağlayan nitel araştırmalar, ilgili olay ve durumlara atfedilen anlamların yorumlanmasıyla şekillenmektedir (Baltacı, 2019). Bu süreçlerde ise gözlem, görüşme, doküman ya da görsel-işitsel şeklindeki farklı araçlardan yararlanmak mümkündür (Creswell, 2013).

Bu araştırmada, verilerin doküman analizi ve görüşmeler aracılığıyla ile toplanması planlanmıştır. Yapılandırılmış, yarı-yapılandırılmış ve yapılandırılmamış (Fraenkel, Wallen & Hyun, 2012) şeklinde çeşitlenen görüşme yöntemlerinden yarı-yapılandırılmış görüşme yapısı benimsenmiştir. Araştırmanın kapsamını ve amacını yansıtan açık uçlu soruların belirli bir çerçevede katılımcı görüşlerini ve deneyimlerini yansıtmasına olanak sağlayan yarı-yapılandırılmış görüşmeler ile veri toplama sürecinin daha esnek bir ortam sağlayarak araştırmacının kontrolünde ilerlemesine yardımcı olduğu söylenebilir. Ayrıca bu teknik ile verilerin rahatlıkla elde edilmesinin yanı sıra düzenlenmesinin ve çözümlenmesinin de daha esnek ve kolay bir yapı sağladığını ifade etmek mümkündür. Bu doğrultuda araştırmanın kapsamı ve amacı göz önünde bulundurularak oluşturulan görüşme soruları, Sınırlı Rasyonellik ve Endüstrileşme Kuramlarının temel alındığı kuramsal matrisi (Tablo 2.4) temsil edecek biçimde yapılandırılmıştır.

3.2.3.1. Görüşme soruları

Sınırlı Rasyonellik ve Endüstrileşme Kuramlarının düzeyleri baz alarak oluşturulan kuramsal matris (Tablo 2.4) göz önünde bulundurularak hazırlanan görüşme sorularının oluşturulma sürecinde görünüş ve kapsam geçerliğinin değerlendirilmesi açısından iki alan uzmanının görüşleri alınmıştır. Daha sonra katılımcılardan yazılı izinlerin alınmasıyla birlikte veri toplama sürecine geçilmiştir. Araştırma kapsamında hazırlanan görüşme soruları aşağıda yer almaktadır.

Soru-1: Sınırlı bilgiye sahip olan güvenlik uzmanları ve sistem paydaşlarının güvenliğini sağlamak için teknik destek hizmetleri nasıl rasyonelleştirilebilir?

Soru-2: Saldırı önlem ve savunma faaliyetlerinde sınırlı yeteneğe sahip olan teknik destek hizmeti uzmanları nasıl desteklenebilir?

Soru-3: Sınırlı değerlendirme yetisine sahip olan güvenlik uzmanları ve sistem paydaşları için teknik destek hizmetleri kapsamında ne tür değerlendirmeler yapılabilir?

Soru-4: Siber uzamdaki sayısız belirsizliğin riske attığı sistemlerin teknik destek hizmetleri kapsamında nasıl analiz edilebilir?

Soru-5: Sınırlı karar verme yetisine sahip olan güvenlik uzmanları ve sistem paydaşlarının teknik destek hizmetleri kapsamında nasıl desteklenebilir?

Soru-6: Siber güvenliğin sağlanmasında sınırlı bilgi çerçevesinde yapılanan teknik destek hizmetleri nasıl mekanikleştirilebilir?

Soru-7: Teknik destek hizmeti uzmanlarının sınırlı yeteneği kapsamında sunulan güvenlik faaliyetlerinin hangi mekanizmalarla nasıl zenginleştirilebilir?

Soru-8: Siber saldırıların tespitinde sınırlı değerlendirme yetisine sahip teknik destek hizmeti uzmanlarının değerlendirme süreçleri nasıl desteklenebilir?

Soru-9: Siber uzamdaki sayısız belirsizliğin tespitinde ve değerlendirilmesinde teknik destek hizmetleri kapsamında nasıl teknikler geliştirilebilir?

Soru-10: Sınırlı karar verme yetisine sahip bireyler tarafından kontrol edilen savunma ve tespit karar sistemlerini güçlendirilmek için hangi mekanizmalar nasıl kullanılabilir?

3.2.4. Verilerin elde edilmesi

Açık ve uzaktan öğrenmede siber güvenliğin sağlanmasının teknik destek hizmetleri perspektifinden incelenmesini amaçlayan bu çalışma kapsamında uzman görüşleri yarı-yapılandırılmış görüşmeler aracılığıyla elde edilmiştir. İlgili görüşme soruları doküman analizi sonucunda elde edilen veriler baz alınarak oluşturulmuştur. Bu süreçte ilk olarak uzmanlardan katılımları ve görüşmelerin kayıt altına alınması konularında e-posta yolu ile yazılı izinler alınmış; bu doğrultuda görüşme tarihleri ve saatleri belirlenmiştir. Coğrafi uzaklık ve Covid-19 pandemisiyle birlikte yaşanan sağlık kısıtlamalarından dolayı görüşmeler 4 farklı şekilde gerçekleştirilmiştir. Araştırma kapsamında 3'ü yüz yüze, 2'si çevrimiçi, 2'si yazılı ve 1'i telefonla olmak üzere 8 farklı uzmanın katılımıyla veriler toplanmıştır. Sonrasında görüntü, ses ve yazılı olmak üzere 3 farklı formda kayıt altına alınan verilerin analizine geçilmiştir.

3.2.5. Verilerin analizi

Elde edilen görüşme verilerinin analizi aşamasında geçildiğinde ilk olarak sesli ve hem görüntülü hem sesli formlarda kayıt altına alınan verilerin dökümü araştırmacı tarafından alınmıştır. Dökümü alınan veriler ile veri toplama sürecinde doğrudan yazılı olarak elde edilmiş veriler, nitel araştırmalarda farklı türlerden verilerin (ses, görüntü, görsel materyal ve doküman vs.) analiz edilmesine olanak sağlayan NVivo paket programına aktarılarak kod ve temaların oluşturulacağı sürece geçilmiştir. Belirli bir durum kapsamında elde edilen verilerin yorumlanmak üzere farklı tema ve kodlara ayrılması, bu sınıflandırma yapısıyla birlikte kavramlar ile durumlar arasındaki ilişkilerin amaç çerçevesince tespit edilip değerlendirilmesi ve tüm bunların betimlenmesi süreçlerinde NVivo paket programının oldukça etkili ve kullanışlı olduğu söylenebilir.

Yarı-yapılandırılmış görüşmeler aracılığıyla toplanan veriler, içerik analizi yöntemiyle analiz edilmiştir. Duruma yönelik farklı kaynak türlerinden elde edilen

verilerin tümevarımsal bir yaklaşımla incelenmesine olanak sağlayan içerik analizi, durumların farklı boyutlarının derinlemesine incelenmesi, sınıflandırılması, değerlendirilmesi, ilişkilendirilmesi, betimlenmesi ve yorumlanması mümkün kılmaktadır (Fraenkel, Wallen & Hyun, 2012). Bu doğrultuda şekillenen bu araştırmada elde edilip dökümleri alınan veriler ilk olarak baştan sona okunmuş, daha sonra bu verilerin genel yapısı göz önünde bulundurularak veri metinlerinden görüşme sorularıyla ilişkili kodlar ve temalar çıkartılmıştır. Bu doğrultuda elde edilen bulgular betimlenerek araştırmanın temel soru ve sorunlarına yanıt verecek şekilde yorumlanmıştır. İlgili çıktılar araştırmanın "bulgular ve yorumlar" başlığı altında yer almaktadır.

3.2.6. Araştırma güvenirliği

Görüşme verilerinin analiz edilmesiyle kod ve temalar oluşturulmuştur. İçerik analizi ile oluşturulan kod ve temalar üç bağımsız araştırmacı tarafından gerçekleştirilmiştir. Bu analizleri sağlaması yapılarak araştırma güvenirliğini sağlamak adına ilgili sonuçların uyumu karşılaştırılmıştır. Bu karşılaştırma Miles ve Huberman (1994)'ın "Görüş Birliği / (Görüş Birliği + Görüş Ayrılığı) x 100" formülü baz alınarak yapılmıştır. Bu formül doğrultusunda elde edilen sonuç, araştırmacılar arasındaki güvenirliğin %90 olduğunu göstermiştir.

4. BULGULAR VE YORUMLAR

Açık ve uzaktan öğrenmede siber güvenliğin teknik destek hizmetleri kapsamında incelendiği araştırmanın bu bölümünde, toplanan verilere ait bulgular ve bulgulara yönelik yorumlar yer almaktadır. Bulgular, araştırma amacı ve doküman analizi çerçevesinde şekillenen görüşme sorular aracılığıyla yapılan yarı-yapılandırılmış görüşmeler sonucunda elde edilen verilerin NVivo paket programıyla analiz edilmesiyle aktarılan alıntıları kapsamaktadır.

4.1. Bulgular

4.1.1. Siber güvenliğin rasyonel bir şekilde sağlanmasında sınırlı bilginin olması

Sınırlı Rasyonellik ve Endüstrileşme Kuramlarının oluşturduğu matrisin ilk düzeyini kapsayan "sınırlı bilgiye sahip olan güvenlik uzmanları ve sistem paydaşlarının

güvenliğini sağlamak için teknik destek hizmetleri nasıl rasyonelleştirilebilir?" sorusuyla elde edilen yanıtlar "Sınırlı Bilgi Kapsamında Sistemin Rasyonelleştirilmesi" teması altında incelenmiştir. Analizler; "sistemin siber güvenlik çerçevesinde yapılandırılması", "sistem çatısı altında ayrı güvenlik birimlerinin kurulması", "süreç tasarımlarının yapılması", "akıllı sistemlerden yararlanılması", "sistem açıklarının ya da eksiklerinin belirlenmesi" ve "kayıt tutulması" olmak üzere 6 tane alt tema olduğunu göstermiştir. Bunların yanı sıra "sistemin siber güvenlik çerçevesinde yapılandırılması" alt temasının ise kendi içinde "öğrenen-öğreten" ve "teknik destek ekibi" boyutlarında farklı görüşleri barındırdığı görülmüştür. Şekil 4.1'de ilgili temalar yer almaktadır.

Şekil 4.1. *Sınırlı bilgi kapsamında sistemin rasyonelleştirilmesi*

"Sistemin Siber Güvenlik Çerçevesinde Yapılanması" alt temasının altında "öğrenen-öğreten boyutunu" temsil eden doğrudan alıntılar aşağıda verilmiştir. Bu alt tema altında "sistemin isteğe bağlı olması", "sistemin bilgilendirici olması", "sistemin anlaşılır olması" ve "senkron ve asenkron eğitimlerin verilmesi" görüşlerinin desteklendiği görülmektedir:

"…Bu tür sistemleri on-demand şekilde, ihtiyaçları olduğu zaman ulaşabilecekleri bir portal diyebilirsin, bir arayüz diyebilirsin, oradan bunları bilgilendirebilecek bir yapılanma kurmak lazım ve burayı güncel tutmak lazım. Yani, işte burada neler olabilir? İşte bu yapılabilecek siber saldırıların özellikle kullanıcı diliyle açıklanması… Yani öğrenen ve öğretenlerin bu anlamda çok bir teknik becerisini beklemiyoruz. Dolayısıyla bunların türlerinin açıklandığı, bunların sorular sorduğunda işte cevap alabileceği bir mekanizma kurgulamak lazım..." Emir

"…oryantasyon eğitimleri yapabiliriz mesela, öğrencilerimize ve hocalarımıza. İşte bu oryantasyon eğitimleri farklı türlerde yapılabiliyor, senkron asenkron şeklinde. Biz iki yolu da izleyebiliriz. Mesela senkron ve asenkron eğitimler içerisine de entegre edilebilir bu tür eğitimler, böyle bir şey olabilir, yapılanma olabilir..." Emir

Alıntılardan yola çıkarak açık ve uzaktan öğrenmede siber güvenliğin sağlanması için sınırlı bilginin söz konusu olduğu durumlarda sistemin rasyonelleştirilebilmesi için kullanıcı dostu bir yapının tüm paydaşlar göz önünde bulundurularak anlık bilgilendirme sağlayacak şekilde oluşturulması gerektiği söylenebilir. Farklı eğitimlerle desteklenebilecek olan bu sınırlılığın senkron ve asenkron öğrenme ortamlarıyla da rasyonelleştirilebileceğini ifade etmek mümkündür.

Bunların yanı sıra yine "Sistemin Siber Güvenlik Çerçevesinde Yapılanması" alt temasının altında incelenen "teknik ekip boyutunda" aşağıdaki gibi bulgular elde edilmiştir. Bu bulgularda "kalifiye elemanların işe alınması", "görev ve sorumluluk dağılımlarının yapılması", "farklı kanallar aracılığıyla anlık bilgilendirme yapılması", "uzman eğitimlerinin verilmesi/ sağlanması", "üst yönetim destek sistemlerinin kurulması", ve "sistemin ve sistem parçalarının uyumlu ve koordine olması" görüşlerinin olduğu belirlenmiştir:

"…teknik destek hizmetlerinde rol alan paydaşların liyakate dayalı olarak görevlendirilmeleri ve sürekli güncel gelişmelere paralel olarak yetiştirilmeleri beklenebilir…" Ufuk

"…güvenlik uzmanları her şeyi bilemez; sınırlı bilgiye sahipler. Mesela kimisi sızma testlerini yapabilir. Kimisi önlem bölümüne gelir. Ya o üç bölüm varsa mesela, önlem işte tespit ve savunma, bu üç bölümünde apayrı birimler olarak kurulması ve gerçekten yetişmiş kalifiye elemanların buralarda çalışması çok önemli…" Burak

"…Bir görev paylaşımı yapılmalı. Ve biliyorsun siber olaylarda bir şey olduğunda anlık bilgilendirme çok önemli. Yani dolayısıyla bu anlık bilgilendirme mekanizmasının kurulması lazım. Yani hızlı bir şekilde farklı kanallardan (…) Yani olay gerçekleşmeden, diyelim ki bir

> *siber atak var, saldırı var; o gerçekleşmeden bir şekilde sesi geliyor aslında çeşitli şeylerle. O bilgilendirme mekanizmasının iyi kurgulanması gerekiyor. Ona göre de zaten gerekli yapılanma, gerekli işte tedbirler ya da gerekli taarruz neyse alınması gerekiyor (…). Tabii bunlarla birlikte kişilerin eğitimleri de iyi sağlanmalı…"* Emir

> *"…Sistemi kurduktan sonra da özellikle bu destek hizmetlerini yani sadece kişileri eğitmekle de değil; belki onların da üstünde bir üst yönetim destek sistemi oluşturulabilir. İnsan faktörünü bu şekilde çözeriz…"* Burak

> *"…siber uzam çok geniş yani birçok sebebi olabiliyor ve nereden kaynaklandığını anlayamıyorsunuz. O yüzden o sistemin parçalarının birbiriyle uyumlu olması, yani network birimi ile sistem biriminin, sistem birimiyle işte sunucu yönetim biriminin, o yapılanmanın ve bu aradaki koordinasyonun çok iyi olması lazım…"* Emir

"Sistemin Siber Güvenlik Çerçevesinde Yapılanması" alt temasının teknik ekip boyutunu temsil eden bu bulgulardan, işe alınan teknik elemanların seçilmesinde belirli kriterlerin göz önünde bulundurulması gerektiğine yönelik bir çıkarım yapılabilir. Bu doğrultuda kurulacak ekiplerin belirli rol ve görev tanımları çerçevesinde yapılandırılmasıyla ise güvenlik faaliyetlerinde birimler, bireyler ve ekipler arası daha uyumlu ve koordine bir sürecin olacağı savunulabilir. Bu süreçlerdeki iletişimin; tüm paydaşları kapsayan, etkileşimli ve çeşitlendirilmiş bir yapıda sunulmasının da önemli olduğu görülmektedir.

Öğrenen ve öğreten boyutunda önemli bir yere sahip olan eğitim ve anlık bilgilendirme yapılanmalarının teknik destek ekibi bağlamında da önemli olduğu söylenebilir. Bunun yanı sıra bu süreçlerde yönetsel destek ve yapılanmaların da kritik bir rolü olduğunu söylemek mümkündür. Bu noktada sistem yaklaşımının ve yapılanmasının siber güvenlik faaliyetlerine de uyarlanabileceği ifade edilebilir. Bu, siber güvenliğin ayrı bir sistem birimi olarak yapılandırılması gerektiğini işaret etmektedir. "Sistem çatısı altında ayrı güvenlik birimlerinin kurulması" alt teması altında bulgulanan doğrudan alıntı aşağıdaki gibidir:

> "*…bu süreçte güvenlik uzmanları çok önemli. Yani, insan faktörü burada çok önemli. Yani güvenlik birimlerinin apayrı birimler olarak kurulması, özellikle siber güvenlikte bizim tüm alanlarda en az önemsenen alan olduğunu hissediyorum ben Türkiye'de…"* Burak

İncelenen bir başka alt temada "Süreç Tasarımlarının Yapılması" konusuna yönelik görüşler olduğu görülmüştür. İlgili görüş doğrudan alıntı olarak aşağıda verilmiştir:

> *"…bu işi rasyonelleştirebilmek için bir kere süreçleri iyi tasarlamak lazım. Eğer süreçleri iyi tasarlayamıyorsak ortada bir süreçlerde, tamam çok kompleks olabilir ama bunu mümkün olduğu kadar şeye indirgemek lazım, anlaşılabilir seviyeye indirgemek lazım. Yani bir siber saldırı geldi, muhtemel sebeplerini çıkarabilmek lazım ve muhtemel arasındaki, muhtemel sebepler sonrasında yapılabilecek şeyleri üzerinde birimler arasında bir mutabakatın olması lazım. Bu olmadığı müddetçe, hani o bir kriz anı oluyor, bir panik havası oluyor…"* Emir

Yukarıdaki görüş doğrultusunda sınırlı bilgi çerçevesinde yapılanan ve doğası gereği karmaşık olan siber güvenlik faaliyetlerinin rasyonelleşebilmesi için süreç tasarımlarının basit ve anlaşılır bir şekilde hazırlanması gerektiği söylenebilir. Bu görüş, olası saldırılara yönelik öngörü ve tedbir faaliyetlerinin önemli olduğunu işaret etmektedir. Bu faaliyetlerin yürütülmesinde ise birimler arası uyumun da önemli olduğu savunulabilir. Elde edilen bulgular doğrultusunda çıkarılan bir diğer alt tema ise "Akıllı Sistemlerden Yararlanılması" ile ilgili olup bu alt temaya yönelik görüşler aşağıda yer almaktadır.

> *"…Aslında bireyin sınırlılığı, özellikle büyük verinin ortaya çıkışı, dijital teknolojilerin çok yaygın olması, açık ve uzaktan öğrenmede ya da büyük eğitim sistemlerinde bu tür verilerin çok olması bireyin sınırlılığını daha da arttırıyor. Yani, bir kişinin ya da bir ekibin bütün veriye sahip olması oldukça zor hale geliyor. O da bizi nereye götürüyor? Makine öğrenmesine götürüyor. Büyük verilerin tutulacağı veri tabanlarına götürüyor. Bu veri tabanlarının doğal dil işlemeyle, işte algoritmalarla ortaya çıkıp bir öneri sistemi oluşturup ekibe ne yapacakları ile ilgili bilgi vermesini gerektiriyor. Hatta daha da ötesi, eğer yapılabilirse, yapay zekânın ortaya çıkan riskleri büyük verilerden elde edip doğrudan kendinin sisteme uyguladığı, aktardığı bir yapıya da dönüşebilir…"* Cem

Bireyin sınırlı biliş kapasitesinin gerekçelendirildiği bu görüşte, dijital teknolojilerin bu sınırlılığı genişleten ama aynı zamanda çözüme kavuşturan bir faktör olduğu belirtilmiştir. Bu doğrultuda özellikle akıllı sistemlerin sistem güvenliğini sağlayacak faaliyetlerde kullanılmasının, sınırlı bilgi çerçevesinde yapılanan sistemlerin rasyonelleşmesini sağlayacağı ve aynı doğrultuda hem sınırlı bilgiyi hem de güvenliği veriye dayalı olarak çözüme kavuşturacağı savunulabilir. Verilerin sistem güvenliğini ve sınırlı bilgiyi rasyonelleştirmesinin yanı sıra farklı açık ve eksiklerin de öngörülmesi, tespit edilmesi ve önlenmesi aşamalarında önemli bir rol oynayacağını da söylemek mümkündür. "Sistem Açıklarının ya da Eksiklerinin Belirlenmesi" alt temasında bu sava yönelik aşağıdaki gibi bir açıklama yapılmıştır:

> *Sistemin tüm dijital platformlarına, tüm teknik sistemlerine erişebilen, erişim izni olan kütüphaneler oluşturabilen, kendi kütüphanelerini oluşturabilen bir yapay zekâ sistemine ihtiyaç var. Ama şu aşamada, ilk aşamada, öncelikle eksiklerin belirlenmesi, nelerin taranacağının belirlenmesi önemli…"* Cem

Yukarıda söz edilen öneri ve görüşleri destekleyen bir diğer alt tema ise "Kayıt Tutulması" ile ilgili olan bulgudur. Bu bulgu, sistemdeki dijital verilerin ve veri kayıtlarının geçmiş, mevcut ve olası saldırı faaliyetleri için arşiv niteliğinde bir rehber olduğunu işaret etmektedir.

> *"…bilgi yönetim sistemlerinin doğası gereği yaşanan lokal ya da atipik tecrübelerin hızlı bir biçimde ortak bir elektronik performans destek sistemi havuzunda toplanması önerilebilir. Böylece sürekli bir belirsizliğin hâkim olduğu farklı bağlamlarda yaşanan yeni durumların profesyonellerce erkenden tespiti, alınan aksiyonların ve sonuçlarının hızlı bir biçimde diğer paydaşlara da ulaştırılması sağlanabilir…"* Ufuk

4.1.2. Siber güvenliği sağlama faaliyetlerinde sınırlı yeteneğe sahip olunması

Açık ve uzaktan öğrenmede siber güvenliğin teknik destek hizmetleri kapsamında incelendiği bu araştırmada hazırlanan 10 görüşme sorusundan biri olan "saldırı önlem ve savunma faaliyetlerinde sınırlı yeteneğe sahip olan teknik destek hizmeti uzmanları nasıl desteklenebilir?" sorusu, çalışma kapsamında oluşturulan kuramsal matrisin ikinci düzeyini temsil etmektedir. Bu düzey "Sınırlı Yeteneğin Desteklemesi" temasını besleyen bulguları temsil etmektedir. Bu doğrultuda "rollerin tanımlanması", bilgi tabanlı bir sistem tasarlanması", "akıllı sistemlerin kullanılması", "öngörü ve tahmin çalışmalarının yapılması", "farkındalık oluşturulması" ve "bireylerin ve süreçlerin yönetim tarafından desteklenmesi" alt temalarına ulaşılmıştır. "Rollerin tanımlanması" alt teması altında ise "ön bilgilerin tespit edilmesi" ve "eğitim verilmesi/ sağlanması" yönünde bulgular elde edilmiştir. Tablo 4.2'de ilgili alt tema şeması yer almaktadır.

Şekil 4.2. *Sınırlı yeteneğin desteklenmesi*

Siber saldırıların önlenmesinde ve saldırılara karşı savunma faaliyetlerinin gerçekleştirilmesinde teknik destek ekibinin sınırlı yeteneği olduğu düşünülerek yapılandırılan görüşme sorusu aracılığıyla elde edilen alt temalardan biri rollerin tanımlanması üzerinedir. Bu doğrultuda alınan görüşler, doğrudan alıntı olarak aşağıda verilmiştir:

> *"...Lokal bir ortamda yeterli sayı ve nitelikte teknik destek hizmeti personeli bulundurmak ekonomik olmayabilir. Merkezi bir yapının ya da altyapı / ihtiyaç / tercihlere göre bölgelere ayrılmış yapıların oluşturulması ile alınan sağlıklı ve etkili kararların daha çok paydaşa hızlı bir biçimde ulaştırılması sağlanabilir..."* Ufuk

> *"...birimlerde böyle siber güvenlik uzmanları gibi böyle tamamen ona adanmış insanlar yok, benim gördüğüm kadarıyla. Genellikle sistem birimine bakan, networke bakan arkadaşlara böyle ek bir görevmiş gibi geliyor. Tabi böyle münferit bir siber saldırı şeyi kurmak ya da işte önlem birimi gibi bir şey kurmak, ki biz kurmaya çalıştık, o da şundan yaptık yani var olan farklı görevleri olan arkadaşları bir araya getirip kurduk. Bir kere bu böyle bir personel, insan kaynağı istihdamı önemli..."* Emir

Burada ilk olarak bütün paydaşları göz önünde bulundurularak hem bireylerin hem birimlerin hem de sistemin rollerine yönelik bir ayrıma gidilmesi gerektiğine dair bulgular elde edilmiştir. Bununla birlikte mevcut teknik ekip yapılanmalarında sınırları belli görev tanımlarının olmadığı; bu tanımlar arasında siber güvenliğe ait rollerin ise neredeyse göz ardı edildiği söylenebilir. Bu doğrultuda ayrı bir siber güvenlik biriminin kurulmasının, bu birim altında farklı faaliyetler için özelleşmiş rol tanımlarının yapılmasının önemli olduğu savunulabilir. Tanımlanan rollerin doğru kişilerle

eşleştirilebilmesi için ise "ön bilgilerin tespit edilmesi" ya da "eğitimlerin sağlanması" yönünde bir yapılanmaya gidilebileceğine yönelik görüşler olduğu belirlenmiştir.

> *"…öncelikle tabi ki bu personelin bir önbilgisini bir şey yapmak lazım, tespit etmek lazım…"* Emir

> *"…Teknik destek ekibinizin aynı zamanda birer öğrenci olduğunu göz önünde bulundurmak gerektiğini düşünüyorum. Güvenlik konusunda tamamına öğrencilik yönünden yaklaşmak gerekiyor. Durmadan öğreniyorlar. Yani öğrenmeleri gerekiyor..."* Ferhan

> *"…neyin bir saldırı olduğunu, tehdit olduğunu anlamak üzere hani ciddi orada efor sarf edilmesi gerekiyor. Hani kimse yapay zekâ bilmek zorunda değil teknik ekipteki; kullanıcılar da öyle. Ama öyle bir sistem olmalı ki, bir uyarı sistemi belki işte geliştirilip hani o karar destek sistemi dediğim kısım bu yani benim. Hem öncesinde belki analizler yapılabilir hani ne tarz önlemler alırsak ne olur onu hani daha bir saldırı olmadan onların analizleri, simülasyonları yapılabilir. Bir şekilde de teknik destek de böyle böyle eğitilebilir diye düşünüyorum…"* Ayça

> *"…saldırı önleme ve savunma faaliyetlerinde uzmanlaşmak için CEH (Certified Ethical Hacker) sertifikası gibi güvenlik sertifikaları alınabilir. Çünkü siber güvenlikte en zayıf halka kadar güçlüyüz. Siber güvenlikteki en zayıf halkalardan bir tanesi insan faktörüdür..."* Taylan

Açık ve uzaktan öğrenme sistemlerinin tüm paydaşlarını kapsayan siber güvenlik faaliyetlerinde rol oynayan kişilerin siber uzamın dinamizmi doğrultusunda kendini ve bilgisini sürekli güncellemesi gereken öğrenciler olduğunu göz önünde bulundurarak bu kişilere ve bu kişilerin faaliyetleri çerçevesinde korunan diğer paydaşlara sistem kültürü çerçevesinde gerek farkındalık gerek uygulama gerekse simülasyon eğitimleri verilebilir. Açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanmasında akıllı sistemler kullanılabileceği gibi teknik ekibin eğitiminde de bu teknolojilerden yararlanılabileceği düşünülebilir. Bunların yanı sıra "Bilgi Tabanlı Bir Sistem Tasarlanması" alt teması kapsamında yukarıda bahsedilen faaliyetleri besleyeceği düşünülen faaliyetler aşağıdaki gibi bulgulanmıştır:

> *"…Benzer rol ve sorumlulukları üstlenen personelin sürekli kendini güncelleyen, dinamik bir elektronik performans ve paylaşım sisteminde buluşturulmaları önerilebilir. Böylece yeni risklere karşı erken önlem ve yetiştirme adımlarının atılması mümkün olabilir…"* Ufuk

> *"…ihtiyaç anında karşılaşılan durumla ilgili işte anahtar kelimeleri yazdığında bunun sebepleri ve önlemleriyle ilgili bilgi verilecek bir yapılanma kurulabilir mesela. (…). Yani*

soruyorsunuz ve size oradan bununla ilgili bilgiler geliyor ve bu portal güncellenen ve sürekli içerisine bilgi girilecek; hatta kullanıcı deneyimleriyle şekillenen yani…" Emir

"… Yani böyle bir knowledge-based bir, knowledge-collective bir şey oluşturulması lazım, bir yapılanma oluşturulması lazım ve ben onun içerisinde az önce bahsettiğin siber önlem ve savunma tarafında çalışan personeller de buradaki caseleri okuyup o caseler sonucunda neler yapıldığını, nasıl çözüme kavuştuğunu… Yani bir community of practice oluşturulması lazım. Yani insanlar deneyimliyor ve bunları bir community yapmak lazım; bunu da böyle formal bir ortamda yapmak lazım…" Emir

Siber güvenlik faaliyetlerinde anlık bilgilendirme ve güncel kalmanın önemini vurgulayan yukarıdaki bulgularda, olası saldırılara yönelik önlem alma faaliyetlerinde de bu dinamik yapılanmanın önemli olduğu belirtilmiştir. Bireyler, birimler ve sistemler arasındaki etkileşim ve iletişime de dikkat çekilen yorumlarda siber güvenlik faaliyetlerindeki dijital geçmişin "öğrenme geçmişi" olarak yapılandırılabileceği faydalı bir sisteme dönüştürülmesinin sınırlı yeteneğin giderilmesinde faydalı olacağı söylenebilir. Dijital izlerden çıkarılan öğrenme geçmişine yönelik verilerin kullanılmasında ise aşağıda yer alan "Akıllı Sistemlerin Kullanılması" alt temasındaki bulguların incelenmesi faydalı olacaktır.

"Temelinde yapay zekâ, makine öğrenmesi ve derin öğrenme gibi günümüzün popüler teknolojilerinden yararlanılarak mümkün olduğunda insan faktöründen kaynaklanan hataların önüne geçilebilir. Teknik destek hizmetlerinde bu tür teknolojilerin kullanılması aynı zamanda teknik personel eksikliği bulunan kurumlar içinde işgücü değerlendirmesi açısından önemli olacaktır." Efe

"…teknik destek ekibine destek olacak yapay zekâ sistemlerinin geliştirilip sadece bu ekip tarafından değil uluslararası düzeyde, düzlemde geçerliği olan güvenilir sistemlerin geliştirilip bu ekibin hizmetine sunulması gerekiyor…" Cem

"…Burada ben özellikle makine öğrenmesi, yapay zekadan makine öğrenmesinin siber güvenlikte çığır açabileceğini düşünüyorum. Çünkü makine öğrenmesinin olayı zaten bu. Makine öğrenecek, öğrenecek, en sonunda mükemmelliğe ulaşacak ve tüm saldırıları daha ilk anda, teknik personel olabilir, olmayabilir, yeterli bilgiye sahip olmayabilir… Ama makine öyle değildir. Makineye ne verirsen onu aynen alırsın…" Burak

"…savunma faaliyetlerde insan faktörünün yanında mutlaka otomatikleştirilmiş sistemlerin mutlaka devreye girmesi gerekiyor. Yani özellikle akıllı ajanların, mesela hangi sistemler var? Sınırlı yeteneğe sahipse mesela akıllı ajanlar devreye girebilir, grup karar destek sistemleri devreye girebilir, üst yönetim destek sistemleri devreye girebilir, biraz belki uçacağız ama genetik algoritmalar devreye girebilir…" Burak

> *"…Burada saldırı ve önlem eşleştirmesi yapılmalı. Alarm sistemi gibi düşün. Önden sizi, bu hani deprem nasıl deprem önceden çok bilinemez ama otuz saniye öncesinde falan anlayabiliyorsunuz ya, ilk saldırı gelir gelmez hemen devreye girmeli teknik personel. Yani orada değilse farklı personellerin de çalışması gerekir. Bunu sadece teknik destek uzmanlarıyla da çözemeyiz de yani bunların otomatikleştirilmiş sistemlerle de o ilk saldırı anında mesela o güvenlik, firewall dediğimiz o güvenlik duvarının hemen devreye girip kesmesi gerekiyor. Hatta sistemi kapatması gerekiyorsa sistemi kapatmalı…"* Burak

Siber güvenlik kapsamındaki önlem ve savunma faaliyetlerinin yapılandırılmasında akıllı sistemlerin kullanılmasını savunan bu bulgularda özellikle makine öğrenmesinin ön plana çıktığı görülmektedir. Bu sistemlerin saldırı önlem ve savunma faaliyetlerinin yanı sıra bu faaliyetlerde kullanılan yöntemlerin ve stratejilerin süreç bazlı olarak değerlendirilmesinde de kullanılarak sınırlı yeteneği güçlendiren bir yapı kurulmasına ve güvenliğin çok boyutlu olarak pekiştirilmesine fırsat sağlayacağı savunulabilir. Bu noktada var olan saldırıların önlenmesinin ve savunulmasının yanı sıra ayrı bir yapılanmayla saldırı öncesindeki süreçlerin ve tehditlerin de incelenmesinin önemli olduğu düşünülebilir. Bu doğrultuda "Öngörü ve Tahmin Çalışmalarının Yapılması" alt teması altında aşağıdaki gibi görüşlerin olduğu belirlenmiştir:

> *"…saldırıları ya da işte o tehditleri tespit edecek robust bir sistem geliştirmek lazım. Hani her türlü tehdide karşı sistemin dayanıklı olabileceğini sağlamamız gerekiyor..."* Ayça

> *"…bir açık ve uzaktan öğrenmede bir öğrenme yönetim sisteminde ne gibi saldırılar gerçekleşebilir? Öncelikle bunu tespit etmek lazım. Yani bunun iş akışını çıkarmak, bunun listesini çıkarmak… (…). Bu saldırılarda hangi önlemler devreye girebilir bunların hepsinin bir ön çalışmasını yapmak gerekiyor ki en büyük sıkıntı hazırlıksız yakalanıyorlar…"* Burak

Yukarıdaki bulgular doğrultusunda açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanması aşamalarına rehber olacak bir öngörü ve tahmin yapılanmasının olması gerektiği önerilmektedir. Bunun, açık ve uzaktan öğrenme sistemindeki farklı birimlerin ve farklı paydaşların çeşitlenen ihtiyaç ve beklentilerine göre sistemi ve sistemin yeteneklerini güçlendirmeye yarayacağı söylenebilir. Sisteme kayıt sırasındaki ödeme güvenliği ile ödev yükleme sırasında ders sorumlusunun dosya indirme işlemlerindeki güvenliği arasındaki fark bu duruma örnek olarak gösterilebilir. Bu doğrultuda, farklı paydaşlara göre farklı güvenlik protokollerinin izlenmesi için olası senaryoların farklı durumları kapsayacak şekilde yapılandırılmasının önemli olduğu düşünülebilir.

Savunma ve önlem faaliyetlerindeki sınırlı yeteneğin çözülmesine odaklanabilmek için farkındalık çalışmalarının öncelikli olarak yapılandırılmasının gerektiği söylenebilir. Aşağıda "Farkındalık Oluşturma" alt temasına ait bulgulara yer verilmiştir.

> *"Teknik destek hizmet uzmanlarına bilgi güvenliği farkındalığı eğitimleri verilebilir…"* Taylan

> *"… siber güvenlik uzmanı kendisi sadece sistemin geliştirilmesine katkıda bulunan ve aslında kütüphaneyi zenginleştiren, varsa yapay zekânın eksiklerini giderebilecek yeni kütüphaneler, algoritmalar geliştirmeye odaklanmalı yeni dönemde. Dolayısıyla bu yeni bir konsept. Bu yeni konsepti ekibe iyi anlatmak lazım ve ekibin de bunu içselleştirmesi lazım…"* Cem

Tüm bu bulgular doğrultusunda siber güvenliğin sağlanması için yürütülmesi gereken faaliyetlerde sınırlı yeteneğin olması; rollerin tanımlanması, sistemin bilgi tabanlı yapılandırılması, sistemdeki dijital verilerden beslenen ve öğrenen akıllı teknik ve yaklaşımların benimsenmesi, bu bağlamda saldırı öncesi süreçlerin ön çalışmalarının yapılması ve tüm bunların kurum kültürü çerçevesindeki bir farkındalıkla eğitilmiş kişilerce yapılması gibi bileşenlerin uyumlu ve sistematik olarak tanımlanmasıyla giderilebilir.

4.1.3. Sınırlı kapasitedeki değerlendirme süreçlerinin desteklenmesi

Bir teknik destek hizmeti türü olarak açık ve uzaktan öğrenme sistemleri kapsamında incelenen siber güvenliğin sağlanmasında sistem paydaşlarının sınırlı bir değerlendirme yetisi olduğunun varsayıldığı bu araştırmada, "sınırlı değerlendirme yetisine sahip olan güvenlik uzmanları ve sistem paydaşları için teknik destek hizmetleri kapsamında ne tür değerlendirmeler yapılabilir?" görüşme sorusu ile "Değerlendirme Süreçlerinin Desteklenmesi" başlıklı tema altında ilgili varsayımı destekleyen bulgular elde edilmiştir. Elde edilen bulgulardan "bilgilendirme panellerinin kurulması" "görev ve sorumluluk dağılımlarının yapılması", akıllı sistemlerden yararlanılması", sistemin ve sistem parçalarının uyumlu ve koordine olması", "yönetsel desteğin sağlanması" ve "farklı kurumlar ile işbirliği yapılması" yönünde alt temalar çıkarılmıştır. Ayrıca "yönetsel desteğin sağlanması" alt teması, "farkındalık oluşturma" ve "eğitim verilmesi/ sağlanması"; "akıllı sistemlerden yararlanılması alt teması ise "olası saldırı senaryolarının oluşturulması" şeklinde alt başlıklarda incelenmiştir. Bu bulgulara ait alt temalar Şekil 4.3'te şematize edilmiştir.

Şekil 4.3. *Değerlendirme süreçlerinin desteklenmesi*

Siber güvenliğin sağlanmasın gerek sistem paydaşlarının gerekse teknik destek ekibinin saldırılara yönelik süreçleri değerlendirmesinde sınırlı bilişsel doğalarından ötürü sınırlı bir değerlendirme yetisine sahip oldukları söylenebilir. Bu doğrultuda sistemdeki ilgili tüm paydaşların bilgilendirilmesinde ve bu doğrultuda bu paydaşların değerlendirme sınırlarının desteklenmesinde "Bilgilendirme Yapılarının Kurulması" yönünde bir görüşün belirtildiği alt temada, ilgili sürecin yapılandırılmasına yönelik elde edilen bulgu aşağıdaki gibidir.

> *"…dashboardlar oluşturulmalı ve oluşturulan o dashboardlarda o sistemin bütününü, gerektiğinde de ayrıntısını, ilgili bileşenin ayrıntısını görebilecek bir yapılanma lazım. Yani, sistemi canlı izleyebilmemiz lazım, önceki verilerle karşılaştırarak. Yani sorun ne, o büyük pencereyi, o büyük resmi görürsek ve istediğimizde de sorun olduğunu düşündüğümüz component üzerinde detaylı bir bilgi alabilecek bir gösterge yapıları kurgulanabilirse o zaman sanki daha sağlıklı karar alınabilir diye düşünüyorum…"* Emir

Yukarıda bahsi edilen yapının, sistemin farklı birimlerini, yapılarını ve bileşenlerini bir bütün olarak görmeye yarayan bir sistem önerisi olduğu söylenebilir. Bu yapılanma, anlık karar ve bilgilendirme süreçlerinin tasarlanabileceği çevik bir yapılanmayı işaret etmektedir. Dolayısıyla siber saldırıların agresif ve dinamik yapısının desteklenmesinde sınırlı değerlendirme yetisine sahip olan sistem paydaşlarının ve teknik ekibin böyle bir

yapıyla desteklenmesinin faydalı olacağını söylemek mümkündür. Bunun yanı sıra değerlendirme süreçlerinin etkinliği ve etkililiğinden bahsedebilmek için paydaşlarla eşleştirilecek rol tanımlarının da en verimli senaryoyu işaret eden bir tanımlama olması gerektiği savunulabilir. Bu doğrultuda "Görev ve Sorumluluk Dağılımlarının Yapılması" başlıklı alt tema, bu savı destekleyen bulguları içermektedir. İlgili temanın bulguları aşağıda yer almaktadır:

> *"…sorumlulukların da bilindiği ve o ekibin hızlı bir şekilde bir araya gelebileceği bir yapılanma kurgulanmalı ve olay o anda müdahale için gerekli karar alınıp hani şey olur da valiliklerde hemen kriz koordinasyon ekibi toplanır ya, onun gibi bir şey ama orada verinin akışı çok önemli…"* Emir

> *"…benzer rol ve sorumluluklara sahip paydaşların aynı ortamda buluşabilmelerini sağlama, merkezi ya da bölgesel ayrımlara göre rolleri belirlenmiş yetkin paydaşların daha acemi paydaşlara mentörlük yapabilmeleri gibi adımlar atılabilir…"* Ufuk

Değerlenme süreçlerinin desteklenebilmesi için süreçte rol oynayan tüm paydaşların görevlerinin uyumlu ve tanımlı olmasının; ilgili süreçlerin koordinasyonunda, yönetiminde, güncellenmesinde ve yeri geldiğinde değiştirilmesinde kolaylık sağlayacağı söylenebilir. Bunun yanı sıra rol dağılımlarının kendi içinde de kademeli bir yapıyı temsil etmesi önerilebilir. Bu noktada usta-çırak yaklaşımının örnek alınabilir. Fakat yalnızca bu yapılanmalarla değerlendirme süreçlerinin kuvvetlenemeyeceği düşünülmektedir. Bu doğrultuda ilgili süreçleri desteklemek için farklı yaklaşımların ele alındığı bir başka alt temayı oluşturan "Akıllı Sistemlerden Yararlanılması" başlığı altında incelenen bulgular aşağıda yer almaktadır:

> *"Sürekli öğrenen ve kendini geliştiren, basit görevlerin mekanikleştirildiği bir yapı yaratılmadığı sürece lokal olarak sürekli bir altyapı güncellemesi, personel takviyesi, en iyi personeli istihdam etme, sürekli teknik destek sağlama ve biçimlendirici değerlendirme gibi adımlar oldukça yorucu ve kullanışsız olabilecektir…"* Ufuk

> *"…İnsan beyninin sınırlı hesaplama yetisi düşünüldüğünde bu durumda da çeşitli yapay zekâ uygulamaları ile makine öğrenmesi kavramından yararlanılabilir. Gelişen teknolojiyle birlikte bu tür sistemlerin artacağı ve nitelik açısından da gelişeceği düşünülebilir…"* Efe

> *"…Teknik ekip bir, kendi bilişsel sınırlılığı var ve bu bilişsel sınırlılığını egale edecek olan dijital teknoloji otonom sistemlerinden yararlanacak, yani yapay zekâdan, doğal dil işleme modellerinden örneğin GPT-3 gibi mesela…"* Cem

Yukarıdaki bulgularda değerlendirme süreçlerinde de destek yapısında yer alması üzere yapay zekâ modellerinden makine öğrenmesine spesifik olarak bir vurgu yapıldığı görülmektedir. Siber faaliyetlerin değerlendirilmesinde öğrenen otonom yapıların olması gerektiğine dair görüşlerin elde edildiği bu bulgular, sistem verilerinin öğrenme geçmişi için önemli olduğunu işaret eder niteliktedir. Dolayısıyla değerlendirme süreçleri için de akıllı sistemler tarafından oluşturulan, kontrol edilen, güncellenen ve yeri geldiğinde değiştirilen bir değerlendirme paneli oluşturulması gerektiği söylenebilir. Bu süreçlerin yapılandırılmasında ise verinin geçmiş, mevcut ve gelecek saldırılara yönelik veriye dayalı olasılıkları değerlendirmesi de gerekebilir. Bu noktada "Olası Saldırı Senaryolarının Oluşturulması" başlıklı alt tema, bu doğrultudaki bulguları kapsamaktadır.

> *"…burada karar destek sistemleri de kullanılabilir aslında. Yani yönetim bilişim sistemleri belki işletmeler için yine kullanılabilir ama karar destek sistemlerinde özellikle senaryolar üzerinden kararların verilmesi… Burada bakın senaryo çok önemli. Senaryo, biraz önce bahsettiğim "hangi saldırıda hangi senaryo gerçekleşebilir?" ve "bu senaryoya göre hangi önlemler alınabilir?". Yani siz bu yazılımlara bu senaryoları bir defa verdiğinizde zaten sistem kendini tanımlayabilir hale geliyor…"* Burak

Doğrudan alıntıda da belirtildiği üzere değerlendirme süreçlerindeki öngörü yapıları ve senaryolarının da akıllı sistemler tarafından öğrenilerek tasarlanması mümkündür. Dolayısıyla sistemin kendi kendini eğitmesinden bahsedilebilir. Bu eğitim verilerinin ise değerlendirme süreçlerindeki insan sınırlılıklarını giderecek bir yapılanmayı meydana getireceği savunulabilir. Rasyonel değerlendirmelerin yapıldığı bir yapılanmadan bahsetmek için ise sistemdeki bileşenlerin uyum içinde olmasına dikkat edilmesi gerektiği düşünülmektedir. Bu doğrultuda edilen bulgular, "Sistemin ve Sistem Parçalarının Uyumlu ve Koordine Olması" alt teması altında aşağıdaki gibi incelenmiştir:

> *"…Yani aslında sınırlılık insan doğasının sınırlılığından da gelen bir şey, özellik. İnsanın sınırlı bilişsel kapasitesi vardır, insanın sınırlı karar mekanizmaları vardır. Bir sistemin içinde human factor varsa, ki biz buna insan faktörü deriz hatta öğretim tasarımında çok geçer. Human factor her zaman değişkenliği, desteği, eksikliği ya da sınırlılığı göz önünde bulundurmak demek ve farklılığı aynı zamanda. Bu sınırlılığı destekleyebilmek için ekiplerin koordinasyonu ve sistemin bütün bu ekiplerden aldığı verilerle koordinasyonu desteklemesi beklenir…"* Cem

Görüldüğü üzere, insan faktörünün doğası gereği beraberinde getirdiği sınırlılıkların siber faaliyetlerin değerlendirilmesi süreçlerini etkileyeceği varsayımı

desteklenmektedir. Bununla birlikte bu sınırlılığın rasyonel bir bakış açısıyla giderilmesi için sistemin ve verilerin sistem planlamasının uygun ve etkili bir "birimler bütününü" temsil etmesi gerektiği söylenebilir. Burada yine sistem yaklaşımından bahsetmek mümkündür. Dolayısıyla sistemdeki birimlerin, sistemi temsil eden uyumlu parçalardan meydana gelmesi gerektiği savunulabilir. Bu doğrultuda sistem çatısı altında sistemin parçadan bütüne kadar bütün bileşenlerinde yönetsel değerlendirmelerin de önemli olduğu söylenebilir. Bu, "Yönetsel Desteğin Sağlanması" alt teması altında yer alan "Farkındalık Oluşturma" ve "Eğitim Verilmesi/ Sağlanması" görüşleriyle ile ifade edilmiştir.

> *"…teknik destek ekibi yalnız olmamalı. Teknik destek ekibi sadece işin teknik kısmıyla ilgileniyor olabilir ama siber güvenlik sadece teknik destekle ilgili değildir. İnsanların eğitimidir, paydaşların iletişimidir, paydaşların karşılıklı farkındalıklarıdır… Yönetim organizasyonun da bu teknik destek ekibini dışlamayacak bir yapıda organize edilmesi lazım…"* Cem

> *"… Bir, ekibin vereceği geri bildirimlerle sınırlılığın giderilmesi; ikincisi ise, sistemin verdiği raporlarla, işte sense-making, decision-making sürecinde farkındalık oluşturma ve öneri sunma sürecinde teknik destek ekibinin o eksikliğini, o doğal eksikliğini gidermesi sağlanabilir…"* Cem

Siber güvenliğin teknik desteğin ötesinde bir yapısı olduğunu belirten yukarıdaki bulgular; siber uzamda bireyler, birimler, yönetim ve sistem arasındaki etkileşim ve iletişimin siber faaliyetlerin değerlendirilme ve yürütülme süreçlerinde önemli olduğunu işaret etmektedir. Dolayısıyla siber güvenliği teknik destek hizmetlerinin yalnızca bir parçası olarak görmektense apayrı bir birim olan fakat teknik destek hizmetleriyle de büyük bir ortak paydaya sahip olan bir yapılanma olarak görmek gerektiği söylenebilir. Bu noktada ise yönetsel kararların, bu birim yapısının şekillenmesinde kritik bir öneme sahip olduğu söylenebilir. Bunun yanı sıra yönetsel faaliyetlerin kurum sınırlarında kalmayıp farklı kurum kültürlerinden de beslenebileceği söylenebilir. "Farklı Kurumlar ile İşbirliği Yapılması" alt teması ile bu durum aşağıdaki bulgularla ifade edilmiştir:

> *"…Sanırım diğer üniversitelerle birbirlerinden öğrenme konusunda işbirliği yapmaları gerektiğini söylemekten başka, sadece bilmiyorum demeliyim. Güvenlik konularında üniversiteler arasında zaten çok sayıda uygulama alışverişi olduğunu düşünüyorum ve aslında bundan eminim. Ancak bunun güçlendirilmesi gerekiyor. Böylece üniversiteler sadece bireysel kurumlarda değil, bir grupta da yanıt verebilir…"* Ferhan

Yukarıda yer alan doğrudan alıntı uygulama ve bilgi topluluklarının yanı sıra *güvenlik toplulukları*nın oluşturulabileceğini işaret etmektedir. Farklı kurumların kültürleri ve verileri ise beslenecek değerlendirme süreçlerinin gerek saldırı öncesi gerek saldırı sırası gerekse saldırı sonrası süreçler için rasyonelleşebilmesi bu şekilde mümkün olabilir.

4.1.4. Sınırsız belirsizliğin olduğu siber uzamdaki olası risklerin analiz edilmesi

Açık ve uzaktan öğrenme sistemlerinin de içinde yer aldığı siber uzamdaki sınırsız belirsizliğin tespit edilmesinde teknik destek hizmetleri kapsamında saldırı analizlerinin nasıl yapılması gerektiğine cevap arayan araştırma sorusu Tablo 1'de yer alan kuramsal matris çerçevesinde "siber uzamdaki sayısız belirsizliğin riske attığı sistemlerin teknik destek hizmetleri kapsamında nasıl analiz edilebilir?" şeklinde yapılandırılmıştır. Bu doğrultuda elde edilen bulgular "Sınırsız Belirsizliğin Olduğu Siber Uzamda Risk Analizi" teması altında incelenmiştir. Bu temada yer alan alt temalar ise "kurum hafızasının oluşturulması", "akıllı sistemlerden yararlanılması", "avantaj ve dezavantajlara göre hareket edilmesi" ve "saldırı tespit sistemlerinin kullanılması" başlıklarıyla kodlanmıştır. Akıllı sistemlerin kullanımını kapsayan alt temada "insan-bilgisayar etkileşiminden yararlanılması" yönünde görüşler olduğu belirlenmiştir. İlgili alt temalar, Şekil 4.4'te gösterilmektedir.

Şekil 4.4. *Sınırsız belirsizliğin olduğu siber uzamda risk analizi*

Sınırsız belirsizliğin farklı gereksinim ve beklentiler meydana getirdiği siber uzamda, açık ve uzaktan öğrenme sistemlerinin de bu dinamizmden etkilendiği söylenebilir. Bu doğrultuda belirsizlikler kapsamında saldırıların, güvenlik gereksinimlerinin ve beklentilerinin analiz edilmesinde aşağıdaki bulgular farklı bakış açıları sunmaktadır. "Kurum Hafızasının Oluşturulması" yönündeki bulguları içeren alt tema aşağıda yer almaktadır.

> *"…Burada bir kere o kurum hafızası çok önemli. Kurum hafızası bence yeterli değil, onu daha da genişletmek lazım. (…). Yani hani şimdi bir, tamam gelmeden önce şey yapıyorsun bir de gelmesi ihtimaline karşı neler yapılabileceğinin yol haritası da oradan, hani az önce bahsettiğim o karar ağaç şeyleri, akış diyagramları oradan da çıkarılabilir. (…) Siber saldırıya uğramadan önce neler yapılabilir herhalde o caselerin analiziyle olur gibi geliyor bana, aklıma gelen şey bu…"* Emir

Yukarıdaki bulgular, durum incelemelerinin önemini işaret etmektedir. Geçmiş verilerin mevcut ve gelecekteki güvenlik faaliyetleri için rehber olması adına bir bilgilendirme panelinin yapılandırılmasının; bu panelin saldırı öncesi, sırası ve sonrası faaliyetleri kapsayacak bir şekilde beslenmesinin ve tüm bunların analizinde gerek kurumsal gerekse kurumlar arası etkileşim ve iletişimin sağlanmasının önemli olduğu söylenebilir. Bunun yanı sıra "Akıllı Sistemlerden Yararlanılması" alt temasında bu analiz süreçlerinin yeni ve akıllı sistemler ile desteklenebileceği bulgulanmıştır. İlgili bulgular aşağıdaki gibidir:

> *"…Bu tür analizleri ancak derin analizler yapabilen algoritmalarla gerçekleştirmek mümkün olabilecektir. İnsan beynini sınırlı yapısı bu konuda tam bir sorumluluk almasına engel olacağından destek hizmetlerine eklenecek güvenlik sistemlerinin giderek gelişeceği ve artan verilere yönelik olarak daha hızlı ve kararlı hareket edeceği düşünülebilir…"* Efe

> *"…Teknik ekibin yapacağı şey bilgisayarın başına oturup riskleri görüp risklere müdahale etmek değil; riskleri görüp müdahale edebilecek, insan sınırlılıklarından muaf olan bilgisayarların program ve protokollerini geliştirmek aslında. Yapabileceğimiz en mantıklı şey şu an bu…"* Cem

Elde edilen bulgular, siber güvenlikte akıllı sistemlerin kullanımını önermekle birlikte bu sistemlerin tasarlanmasında teknik destek ekibinden de söz etmektedir. Dolayısıyla bu süreçlerin tasarımında ve analizinde ilgili akıllı sistemlerin oluşturulmasında teknik ekibin rol oynayacağı söylenebilir. Fakat sonrasındaki güvenlik analizi faaliyetlerinde ise öğrenen mekanizmalar, veriye dayalı olarak sistemin

otonomonlaşmasını sağlayacaktır. Bu alt tema kapsamında insan ve makine öğrenmesi etkileşimi "İnsan-Bilgisayar Etkileşiminden Yararlanılması" başlığı ile aşağıdaki bulgu ile desteklenmiştir.

> *"…aslında sistemi insandan biraz uzaklaştırmamız gerekiyor. Ha, karar destek sistemi de hacklenebilir mi? Hacklenebilir. Veya biraz önce bahsettiğim o makine öğrenmesiyle geliştirilmiş bir sistem yaptık. Makine öğrendi ama hacklenme ihtimali yine var. Şimdi bu bağlamda aslında bir üst katmana çıkmak gerekebiliyor. Yani tabi yine insan çok önemli bir faktör ama burada ben insan ve makine, insan-bilgisayar etkileşimi deniyor da, insan ve makinenin birlikte çalışması gerektiğini, çünkü biraz önce söylediğim makinenin de hacklenme ihtimali var. Makine hacklenirse o zaman insanlar da tabi çok bunun üzerine düşmeyeceği için, hani makine nasıl olsa tespit edecektir, erken uyarı sistemleri çalışacaktır diye düşünürken tabi bunun da hacklenme ihtimalini de göz önüne alarak belki burada farklı alternatiflerde, farklı durumlarda neler olabilir sorusunu da cevaplamaları gerekir…"* Burak

Farklı bir görüş, sistemin yapılanmasında siber uzamdaki belirsizliklerin sağladığı avantaj ve dezavantajlar göz önünde bulundurulması gerektiğine yöneliktir. "Avantaj ve Dezavantajlar Gözetilerek Hareket Edilmesi" alt temasını oluşturan bulgu aşağıdaki gibidir:

> *"…insan davranışlarıyla, insan bilinciyle, insan hesaplamalarıyla, insan tıklamalarıyla, insan loginleriyle oluşmuş bir evrenden bahsediyoruz, bir siber uzaydan bahsediyoruz. Dolayısıyla belirsiz olacaktır. Çünkü doğal yaşam da belirsizdir. Ve aslında yaratıcılık da burada ortaya çıkar. Yani, insanın gelişimi de burada ortaya çıkar. Eğer analitik olsaydı, doldurulacak bir boşluk olmasaydı, bir belirsizlik olmasaydı bir ilerleme de söz konusu olmazdı. Tıpkı bunun gibi siber uzayda da belirsizliklerin olması aslında siber güvenliğin zararına, dezavantajına gibi görünse de aslında avantajına olan da bir bilgidir, bir durumdur, bir realitedir. Dolayısıyla siber güvenlikte bunu bilerek hareket ettiğinizde, yani belirsizliğin bir avantaj olabileceğini düşünerek hareket ettiğinizde, her şeyi kontrol etmek zorunda olmadığınızın farkına varırsınız…"* Cem

Yukarıdaki bulgu, siber faaliyetlerin analiz edilmesinde gerçekçi, ölçülebilir ve analiz edilebilir bir rasyonalitenin önemini işaret etmektedir. Bu doğrultuda siber güvenlik analizlerinin yapılacağı bir açık ve uzaktan öğrenme sisteminde, öncelikle sistemin gerçeklerinin rasyonel bir şekilde analiz edilmesi gerektiği; daha sonra güvenlik faaliyetlerinin geri ve ileri yönelik analizlerinin yapılması gerektiği söylenebilir. "Amaç ve Kapsamın Netleştirilmesi" başlığı, bu görüşü destekleyen bulguları içermektedir.

"…Bütün bu belirsizlikler içinde siz kendi sisteminizin önceliklerini ortaya koyacaksınız. Diğer belirsizlikleri de yine kendi doğal yapısında nasıl çözümlenebileceğini kendisine bırakacaksınız. Eğer ben bir eğitim sisteminin siber güvenlik ekibindeysem, ben öğrencilerin LMS girişlerinin güvenlik problemlerine odaklanırım. Ödeme süreçlerinde sadece kayıt süreçlerine odaklanırım ve bunun için de standart, işte ikili doğrulama sistemlerine gerek kalmadan zaten tek seferde yapılacağı için banka üzerinden hızlıca yapılabilecek bir süreç olarak değerlendiririm. Yani fark ettiyseniz önceliklerimiz yaptığımız işe göre değişir. Neden? Çünkü önümüzde bir siber uzay var ve sınırsız belirsizlikler var. Ben bu bütün bu belirsizlikleri çözmeye çalışırsam siber güvenlik yapamam. Bu belirsizliklerin içinde kendime uygun olan kısımları netleştirmeye çalışacağım…" Cem

"Sınırsız Belirsizliğin Olduğu Siber Uzamda Risk Analizi" teması kapsamında incelenen bulgular ışığında sistemdeki belirsizliklerin analiz edilmesinde işe koşulabilecek ek sistemlerin olduğunu söylemek mümkündür. "Saldırı Tespit Sistemlerinin Kurulması" alt temasında, bu sistemlerin kullanımına yönelik görüşler aktarılmıştır.

"…dinamik elektronik performans destek sistemleri ve ortak paylaşım alanlarının beslediği erken uyarı sistemleri yardımıyla belirsizliklerle daha etkin mücadele edilebilir…" Ufuk

"…Burada bilişim sistemlerinin izlenmesini sağlayan ve anomali bir durum olduğunda bunun tespit edilmesini sağlayan saldırı tespit sistemlerinin kullanılması önemlidir. Saldırı tespit sistemleri saldırıyı tespit etme açısından imza tabanlı saldırı ve anomali tabanlı olmak üzere iki çeşittir. İmza tabanlı saldırı tespit sistemleri bilinen saldırıları tespit ederken anomali tabanlı saldırı tespit sistemleri bilinmeyen saldırıları da tespit edebilir…" Taylan

4.1.5. Siber güvelik faaliyetlerindeki sınırlı karar verme yetisinin desteklenmesi

Sınırlı Rasyonellik Kuramının temel savlarında biri olan "sınırlı karar verme yetisinin" açık ve uzaktan öğrenme sistemlerindeki paydaşların ve teknik destek ekiplerinin karar süreçleri ile ilişkilendirildiği bu çalışmada, ilgili sınırlılığın giderilmesine yönelik görüşler "sınırlı karar verme yetisine sahip olan güvenlik uzmanları ve sistem paydaşlarının teknik destek hizmetleri kapsamında nasıl desteklenebilir?" sorusuyla toplanmıştır. Elde edilen bulgular "sınırlı karar verme yetisinin desteklenmesi" teması altında incelenmiştir. Şekil 8'de de görüldüğü üzere bu temanın alt temaları "eğitim verilmesi/ sağlanması", "akıllı sistemlerden yararlanılması" ve "yönetsel süreçlerin tasarlanması" şeklindedir. Eğitim verilmesinin irdelendiği alt temada "mentör

desteğinin sürece dahil edilmesi" ile ilgili görüşe yer verilirken yönetsel süreçlerin tasarlanmasının irdelendiği alt temada "anlaşılır bilgilendirmeler ile etkileşim sağlanması" incelenmiştir. İlgili alt temalara ilişkin Şekil 4.5'te yer almaktadır.

Şekil 4.5. *Sınırlı karar verme yetisinin desteklenmesi*

Bireylerin karar verme süreçlerindeki sınırlılıkları göz önünde bulundurularak sınırlı bilgi ve sınırlı değerlendirme yetilerinin ilgili karar süreçlerini etkilediği düşünülebilir. Açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanması ve sürdürülmesi için sistemdeki tüm paydaşların siber faaliyetler karşısında farklı kararlar vermesi gerekebilmektedir. Bu doğrultuda ilgili karar süreçlerindeki sınırlılığın desteklenmesinde uzman görüşleri doğrultusunda farklı yaklaşımlardan yararlanılabileceği belirlenmiştir. İlk olarak "Eğitim Verilmesi/ Sağlanması" alt teması incelenmiştir.

> *"…Gelişen teknolojik sistemlere yönelik olarak bu tür uzmanlara eğitimler verilebilir. Sistemlerin çalışma yapısı ve belki de üst analizlerde bulunma konularında eğitimler aldıktan sonra karar verme süreçlerinin yalnızca belli bir boyutlarında görev alabilirler…"* Efe

Yukarıdaki alıntıda görüldüğü üzere karar verme süreçlerindeki sınırlı bilişsel doğa, eğitimlerle desteklenebileceği gibi farklı yapılar ya da yaklaşımlar tarafından da pekiştirilebilir. "Mentör Desteğinin Sürece Dahil Edilmesi" görüşü, bu tarz bir yaklaşıma örnek olarak verilebilir.

> *"Yetkin paydaşların daha sınırlı tecrübeye sahip paydaşlara mentörlük edebileceği dinamik paylaşım ve performans destek sistemlerine gereksinim duyulabilir. Ayrıca kısa aralıklarla yeni deneyimlerin benzer problemleri yaşayabilecek paydaşlara aktarılması, çözüm*

önerilerinin tartışılması, test edilen aksiyonların sonuç ve doğurgularının paylaşılması önerilebilir." Ufuk

Her ne kadar eğitim ve mentörlük yapılanması sağlansa da süreçlerde hala sınırlı karar verme yetisine sahip insan faktörünün yer aldığını söylemek mümkündür. Bu noktada "Akıllı Sistemlerden Yararlanılması" alt temasında yer alan görüşleri incelemenin faydalı olacağı düşünülmektedir.

"…İnsan sınırlılıkları, en baştan beri bahsettiğimiz gibi, insan doğasının sınırlılıklarından dolayıdır bu. Ama çok iyi hazırlık yaparsanız, çok iyi eğitim verirseniz cihaza, bilgisayara; ne uyur, ne dinlenir, çok hızlı cevap verir, çok hızlı hareket eder. Sizin sınırlılıklarınızın ötesinde iş yapabilir. İşte karar verirken de yine bunları eğer devreye alabilirsek, ama tabi insan faktörü olan durumlarda karar vermekten bahsetmiyorum, siber güvenlikte acil durumlarda karar veren bir sistemden bahsediyorum, o zaman daha yararlı olur…" Cem

"…Burada karar dediğimizde zaten karar destek sistemleri hemen akla geliyor. Burada yine sistemi otomatikleştirmek gerekiyor…" Burak

"…siber güvenlikte de sisteme bir eğitim vereceksiniz. Bak bu olursa şunu yap, bu olursa şunu yap, bu olursa şunu yap diye. Dolayısıyla karar sistemlerinin kendisini de eğer algoritmanın içine, yapay zekânın, doğal dil işlemenin içine, kütüphanenin içine yerleştirebilirseniz işte asıl karar mekanizmasındaki insan sınırlılığını asıl o zaman en aza indirmiş olursunuz. Öbür türlü birçok şeyi kaçırırsınız…" Cem

Yukarıda yer alan yorumlardan yola çıkarak açık ve uzaktan öğrenme sistemindeki paydaşların siber güvenlik faaliyetlerindeki karar verme yetilerini geliştirmeye yönelik eğitilmelerinin yanı sıra sistemin kendisinin de eğitilmesinin önemli olduğu söylenebilir. Bu, kendi kendine öğrenen algoritmaları işaret eden makine öğrenmesi ve derin öğrenme gibi yaklaşımları işaret etmektedir. Bunların yanı sıra karar birimlerinin destek yapısı olarak yapılanması ve bunların akıllı sistemlerle etkileşimli ve otomatikleşmiş bir yapıda faaliyet gösterilmesi önerilebilir. Birim tabanlı olarak yapılandırılan tüm bu karar odaklı süreçlerin ve faaliyetlerin sistem çatısında yapılandırılmasında ve yaygınlaştırılmasında ise yönetsel bir karar destek yapısının gerekliliğinden bahsedilebilir. Bulgulardan yola çıkarak ilgili gerekliliği destekleyen alt tema, "Yönetsel Süreçlerin Tasarlanması" başlığı ile aşağıdaki görüşleri kapsamaktadır.

"…yönetici bazında bence, yani üst kademe olarak, önce başta bir karar verilmesi gerekiyor. Yani sistem analizi yapılmış ve sistemde böyle bir gereksinim var. Biz şimdi sistem analizi kısmını bitirmişiz bence. Tasarımdayız. Hani sistemi, bu eksiklikleri nasıl giderebiliriz kısmındayız. Dolayısıyla hani bunun kararını verecek kişiler, yani bu sistemin yöneticileri

> *aslında, onların bir karar vermesi lazım. (...) karar merciindeki kişilerle görüşerek "bizim güvenlik seviyemiz ne olmalı?". Hani ona karar vermek lazım önce. Ona göre de yöntemler üzerinde çalışılır tabii ki de…"* Ayça

Bu görüş doğrultusunda yapılandırılan alt tema, farklı görüşler çerçevesinde daha alt temalar halinde kodlanmıştır. Bunlardan ilki "Anlaşılır Bilgilendirmeler ile Etkileşim Sağlanması" hakkında yer alan görüşü içermektedir.

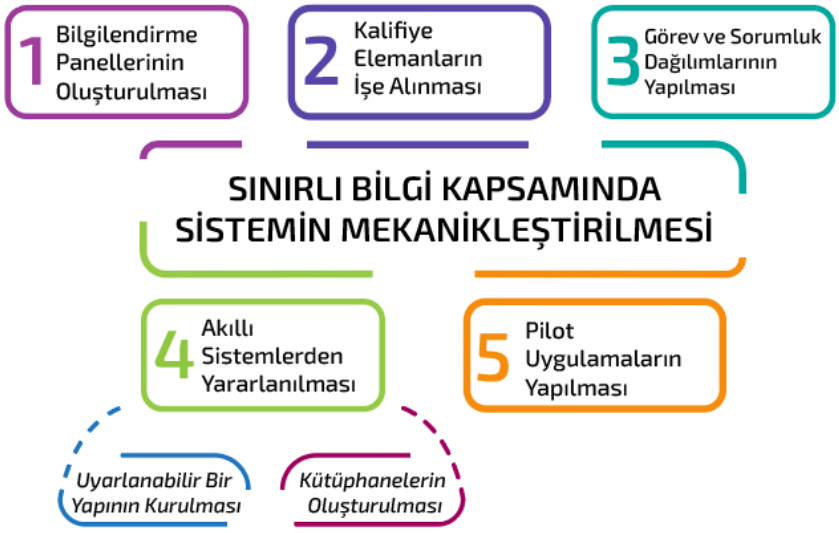
> *"…çok rahat bir şekilde anlaşılabilecek, çok karmaşık terimler, programlama dilleri, algoritmalar kullanılmaksızın burada mutlaka siber taraflar yönetim tarafı birbiri ile bu şekilde etkileşim halinde olmak zorunda. Ve bunu da gerekirse biraz önce dediğim bu görselleştirmelerle, grafikleştirmelerle, tablolaştırmalarla rahat bir şekilde anlatmayı düşünüyorum…"* Burak

Sistem yapılanmasında tasarlanacak süreçlerin, faaliyetlerin ve tekniklerin çok daha ötesindeki gerekliliğin "yönetimin iletişim becerileri" olduğu söylenebilir. Bu süreçteki iletişimde gerek alıcı gerekse kaynak rolünü üstlenecek olan yönetimin, iletişim süreçlerini etkili bir şekilde yürütebilmesinin tüm siber güvenlik faaliyetlerinin temelini oluşturacağı savunulabilir. Çünkü özünde siber uzamda gerçekleşen saldırıların, önlemlerin, analizlerin, değerlendirmelerin ve yorumlamaların karşı tarafın mesajına cevap vermeyi kapsadığı bir iletişim sürecini temsil ettiği söylenebilir. Doğru bir iletişim kanalı oluşturulmasının öncelikle yönetsel boyutta, daha sonra bu boyuttan gelen sağlıklı iletişim çıktılarıyla sistem boyutunda daha rasyonel karar verme süreçlerinin yapılanması mümkün olabilir. Bu noktada yönetimin iletişim becerisi kadar desteğinin de önemli olduğu düşünülmektedir.

4.1.6. Sistemin mekanikleştirilmesinde sınırlı bilgiye sahip olunması

Bu araştırma, Endüstrileşme Kuramını göz önünde bulundurarak sistemdeki tüm paydaşların sahip olduğu sınırlı bilgi kapsamında siber güvenlik faaliyetlerinin yürütülmesinde mekanikleşmenin yeri ve önemi de irdelemektedir. Bu doğrultuda elde edilmesi planlanan bulgular "siber güvenliğin sağlanmasında sınırlı bilgi çerçevesinde yapılanan teknik destek hizmetleri nasıl mekanikleştirilebilir?" sorusu çerçevesinde toplanmıştır. Bu bulgular "Sınırlı Bilgi Kapsamında Sistemin Mekanikleştirilmesi" temasını meydana getirmiş olup ilgili temanın altında "bilgilendirme panellerinin oluşturulması", "akıllı sistemlerden yararlanılması", "kalifiye elemanların işe alınması",

"görev ve sorumluluk dağılımlarının yapılması" ve "pilot uygulamaların yapılması" olmak üzere 6 alt tema olduğu belirlenmiştir. Bunların yanı sıra akıllı sistemlerden yararlanılması alt bulgusu "uyarlanabilir bir yapının kurulması" ve "kütüphanelerin oluşturulması" şeklinde daha alt iki temada incelenmiştir.



Şekil 4.6. *Sınırlı bilgi kapsamında sistemin mekanikleştirilmesi*

Açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanması adına insanın bilişsel sınırlılıkları göz önünde bulundurularak yürütülecek faaliyetlerde ilgili sınırlılığın beslenmesinde "Bilgilendirme Panellerinin Oluşturulması" yönünde görüşler elde edilmiştir.

> *"…büyük resmi gördüğümüz zaman, o yapılanma kurulduğu zaman, ben onları izliyor olabildiğim zaman, o zaman hani sorun nerede sanki daha böyle karar daha rahat verilebilir gibi geliyor. Yani o büyük resmi çizmek önemli. Sistemi izleyebileceğiniz, networkü izleyebileceğiniz, bant genişliğini izleyebileceğiniz, sunucuların durumunu izleyebileceğiniz o yapılanmaları yaptıktan sonra sanki o, alarm yapılarını kurmak sanki daha kolay olacakmış gibi. Dolayısıyla o büyük resmi çizmek lazım…"* Emir
>
> *"…Uzaktan eğitimin temel kuramlarından olan endüstri kuramı ile ilgili bugüne kadar daha çok içerik üretme ve bu içeriklerin mekanikleştirilmesi üzerine çalışmalar yapıldığını düşünüyorum. Ancak teknik destek hizmetleri konusunda bu kuramdan benzer şekilde yararlanılıp belli bir uzantıya sahip teknik destek hizmetleri paketleri oluşturulabilir. Güvenlik ihtiyaçlarına göre uzaktan eğitim birimleri bu paketlerden ihtiyacı olanları tercih*

edebilirler. LMS ya da kullanılan platformdan bağımsız olarak geliştirilebilecek bu tür bir nevi paket sistemler gelecek te de yaygınlaşabilir…" Efe

Yukarıdaki bulgular doğrultusunda sistemin mekanik bir yapıda siber güvenlik faaliyetlerini yürütebilmesi için ön çalışmalar yapılması gerektiği söylenebilir. Özellikle sınırlı bilgi söz konusu olduğunda, bu yapıların sınırlı bilgiyi besleyecek bilgilendirme panelleri olarak sistem paydaşlarının ve birimlerinin kullanımına sunulması önerilmiştir. Ayrıca, açık ve uzaktan öğrenme sistemlerinin farklı birimlerinde faaliyet gösteren mekanikleşmenin teknik destek hizmetleri kapsamında siber güvenlik uygulamalarında da kullanılma gerektiği savunulabilir. Kuramsal çerçevede teknik destek hizmetlerinin mekanik bir siber güvenlik yapılanmasıyla beslenmesinin yeni bir konsept olacağını söylemek mümkündür.

Siber güvenlik faaliyetlerindeki sınırlı bilginin desteklenmesine yönelik mekanikleşmiş yapılardan bir diğerin "Akıllı Sistemlerden Yararlanılması" alt teması altında değinilmiştir. Bu tema da kendi içinde iki ayrı alt temaya ayrılmıştır.

"…akıllı sistemlerden yararlanmak zorundayız yani. Bunu bu şekilde yapabiliriz. (…) belki teknik destek personeliyle makinenin birlikte organize olduğu bir yapı. Teknik destek personeli belki zafiyet içindedir ama bunun açığını kapatacak da bu makine öğrenmesi veya akıllı ajanlar veya karar destek sistemleri gibi sistemler burada devreye girmek zorunda…" Burak

"…Otonom sistemleri, doğal dil işleme, doğal dil işleme alt modelleri, iterasyonlar, döngüler olabilir burada. (…) teknik olarak yapay zekânın asıl olayı daha hızlı olması, sınırsız olması, bilişsel kapasitesinin sınırsız olması ve kütüphanelerle destekleniyor olması…" Cem

"…Teknik destek hizmetleri bu konuda bilişim sistemlerinin dış saldırılara korunması açısından saldırı tespit sistemleri ve saldırı engelleme sistemleri geliştirilmiştir. Teknik destek hizmetlerinin mekanikleştirilmesi açısından saldırı tespit sistemlerinde makine öğrenmesi, derin öğrenme ve yapay zekâ algoritmalarının kullanılması saldırılarının daha hızlı ve doğru tespit edilmesi açısından iyi bir yöntemdir…" Taylan

İnsan-bilgisayar etkileşimini de göz önünde bulundurarak mekanikleştirilecek teknik yapının, siber güvenlik çatısındaki sınırlı bilgiyi destekleyecek algoritmalar, yaklaşımlar ve tekniklerle destekleneceği söylenebilir. Saldırıların gerçekleşmeden önceki ve sonraki süreçlerinin yanı sıra saldırı anında hızlı, doğru ve etkili yanıtlar verilebilmesi adına mekanik yapıların sürece dahil edilmesinin önemli olduğu düşünülebilir. Siber uzamın dinamik ve agresif doğası göz önünde bulundurulduğunda ise bu mekanizmaların duruma göre farklı stratejiler sunacak şekilde yapılanmasının da önemli olduğunu söylemek mümkündür. Bu durum, akıllı sistemlerden yararlanılmasını

içerin alt temanın bir alt düzeyini oluşturan "Uyarlanabilir Bir Yapı Kurulması" alt teması ile aşağıdaki bulgularla ifade edilmiştir:

> *"…sistem adaptive olmalı, tabi yani mesela o saldırıyı hemen önleyen bir sistem adaptive bir şekilde hemen bu saldırının karşı cevabını belki vermeli ki kendini uyarlayabilmeli…"* Burak
>
> *"…Merkezi bir yapı ya da bölgeselleşmenin yanı sıra öğrenen elektronik performans destek sistemlerine gereksinim duyulabilir. Güncel sorunlar için geliştirilen standart çözümlerin tüm paydaşlara hızlıca ulaştırılması, sistem ve altyapının düzenli olarak güncellenmesi, güncellemelerin sistemlere hızlıca entegre edilmesi, yeni katılacak sistemler için aranan standartların düzenli olarak gözden geçirilmesi önerilebilir…"* Ufuk

Değişkenlik gösteren durumlar doğrultusunda hızlı, uyarlanabilir ve etkili çözümlerin sunulmasının yanı sıra güvenlik verilerinin öğrenme geçmişlerinin bir araya getirilmesi, paketlenmesi, arşivlenmesi ve yeniden kullanılabilir yapılara dönüştürülmesinin de önemli olduğu söylenebilir. Çünkü benzer saldırılar ya da faaliyetler için her seferinde işlemleri baştan almak yerine, bunu daha önce yapmış tanımlı paketleri kullanmak hem zaman kazandıracaktır hem de sistemin öğrenmesi pekişecektir. Bu doğrultuda akıllı sistemlerden yararlanılmasının incelendiği alt temanın bir alt düzeyini ifade eden "Kütüphanelerin Oluşturulması" alt teması, bu savı destekleyen bir bulgu içermektedir.

> *"…çok iyi bir teknik alt yapı, doğal dil işleme, işte algoritmalar, otonom sistemler ve kütüphaneler… Kütüphaneleriniz yoksa çok zor; hiçbir şey yapamazsınız…"* Cem

Kütüphaneler, mekanikleşmenin en büyük işaretçilerinden biri olarak görülebilir. Çünkü mekanik bir yapıda, hazır stratejiler ya da strateji geliştirmeye her an hazır paket yazılımların var olduğu söylenebilir. Dolayısıyla akıllı sistemlerin etkili bir şekilde kullanılabilmesi için verilerin beslediği ve dolayısıyla ileri yönelik veri akışlarını besleyen kütüphanelerin oluşturulmasının sınırlı bilginin mekanik bir şekilde desteklenmesi için önemli olduğunu söylemek mümkündür.

Bunların yanı sıra daha önce de belirtildiği gibi insan-bilgisayar etkileşiminin de göz önünde bulundurulması gerekebilir. Bu doğrultuda her ne kadar sınırlı bilgiden bahsedilse de bu sınırlılığın olabildiğinin en optimize şekilde yapılanmaya dahil edilmesi gerektiği söylenebilir. Bu durum, "Kalifiye Elemanların İşe Alınması" alt temasıyla aşağıdaki gibi desteklenmiştir:

> *"…Yani bu bir yazılım olacak. Değil mi? Hani nihayetinde çıkan ürün bir yazılım olacak. Yani işte burada hani bilgisayar programcısı, programcıları ya da işte programlama yeteneği güçlü olan kişiler olmalı. Çünkü hani ben de bir kod yazabilirim, sen de yazabilirsin ama sen aynı sonuca bir saniyede erişebiliyorken benim yazdığım kod 10 dakikada da*

erişiyor olabilir. Burada hız önemli. Dolayısıyla etkin bir kod yeteneği olan bir ekipte böyle kişiler olması lazım…" Ayça

Siber güvenlik faaliyetlerinde her ne kadar sınırlı bilgiden bahsedilse de bu süreçlerdeki sınırlılığın giderilmesinde önerilerin akıllı sistemlerin, bilgilendirme panellerinin ve eğitim faaliyetlerinin düzenlenmesinde ve yürütülmesinde ilk adım yine bireyler, birimler ya da yönetim tarafından atılacağı düşünülebilir. Dolayısıyla mekanikliğe gidilen yolda ilk adımın sağlam atılması adına, ilgili süreçlerdeki elemanların kalifiye kişilerden seçilmesinin sınırlı bilginin mekanik bir yapıyla desteklenmesi yolunda önemli olduğu savunulabilir. Bu noktada kalifiye elemanların işe alınmasının yanı sıra görev dağılımlarının ve rol tanımlarının da düzenlenmesinin önemli olduğunu söylemek mümkündür. Bu düzenlemelerin gerekliliğini destekleyen alt temada, "görev ve sorumluluk dağılımlarının yapılması" ile ilişkin bulgu aşağıda yer almaktadır:

"…Hani bir ekip olmalı, hani işler bu şekilde paylaşılarak ya da bir kişi de yapabiliyor da bir kişi… Ama bunlar adım adım olmalı..." Ayça

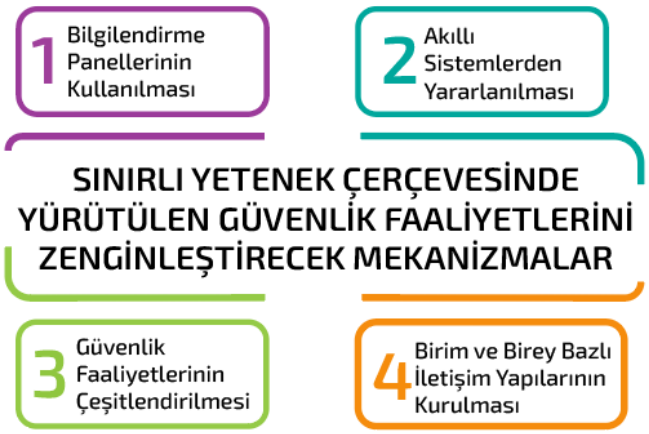
Tüm bunların yanı sıra sınırlı bilginin mekanikleşmiş bir teknik destek kapsamında verilmesi için bu uygulamaların faaliyete konmasından önce deneme, değerlendirme ve iyileştirme çalışmalarının yapılmasının; bu doğrultuda hedef kitle, hedef faaliyet ve hedef maliyetlerin belirlenmesinin önemli olduğu söylenebilir. "Pilot Uygulamaların Yapılması" alt teması, aşağıdaki bulgu ile bu doğrultudaki görüş çerçevesinde şekillenmiştir.

"…Hani bir de pilot uygulama yapılmak zorunda. Ama sürekli, işte belki öğrenci grubu, teknik destekten mevcut yine teknik destek ekipleri var. Onlarda belli kişiler, yöneticiler, hani sürekli düzenli görüşmeler, haftada bir olur bu belki iki üç günde bir olabilir, yani nasıl tanımlandıysa çalışma takvimi. Ama sürekli görüşme şeklinde pilot uygulamadan sonra artık uygulamaya geçme aşaması. Tabi bunların da hep fayda-maliyet analizleri yapılmalı…" Ayça

4.1.7. Sınırlı yetenek kapsamında yürütülen güvenlik faaliyetlerinde ilgili yetenekleri besleyecek mekanizmalar

Açık ve uzaktan öğrenme sistemlerinin güvenliğinin sağlama faaliyetlerinde rol oynayan paydaşların ve ekiplerin, bu süreçlerde sınırlı yeteneklerinin olduğu; bu sınırlılığın giderilmesinde ise mekanik destek yapılarının kullanılabileceği varsayılan bu çalışmada "teknik destek hizmeti uzmanlarının sınırlı yeteneği kapsamında sunulan güvenlik faaliyetlerinin hangi mekanizmalarla nasıl zenginleştirilebilir?" görüşme sorusu

ile bu doğrultuda 8 uzmandan görüşleri alınmıştır. Görüşme sorusuyla elde edilen bulgular "Sınırlı Yetenek Çerçevesinde Yürütülen Güvenlik Faaliyetlerini Zenginleştirecek Mekanizmalar" teması altında incelenmiştir. Bu temayı oluşturan alt temalar ise "bilgilendirme panellerinin kullanılması", "güvenlik faaliyetlerinin çeşitlendirilmesi", "akıllı sistemlerden yararlanılması" ve "birim ve birey bazlı iletişim yapılarının kurulması" olmak üzere Şekil 4.7'de şematize edilmiştir.



Şekil 4.7. *Sınırlı yetenek çerçevesinde yürütülen güvenlik faaliyetlerini zenginleştirecek mekanizmalar*

Siber güvenliğin sağlanmasında sahip olunan sınırlı yeteneğin desteklenmesinde bilgi tabanlı yapılardan yararlanılabileceğini savunan görüş, "Bilgilendirme Panellerinin Oluşturulması" alt teması altına incelenmiştir.

> *"…Dashboard, anlık izlenebilecek, geriye gidebilecek, o verileri takip edebileceğimiz, geçmişle kıyaslayabileceğimiz bir yapılanma geliyor aklıma…"* Emir

Bu doğrultuda, sınırlı yeteneğin mekanikleştirilebilmesi için geçmiş, mevcut ve olası siber faaliyetlerin izlenebileceği bir panel ile aksiyona geçecek bireylerin yeteneklerinin zeminini besleyecek enformasyon, öngörü ve veriler ile destek sağlanabilir. Çünkü yeteneğin sınırlarının genişletilebilmekten bahsedebilmek için öncelikle o yeteneğin faaliyete dönüşebilmesindeki ön yeterliklerin sağlanmasının önemli olduğu söylenebilir. Bununla birlikte sınırlı yetenek, "Güvenlik Faaliyetlerinin Çeşitlendirilmesi" alt temasında yer alan bulgularda incelendiği üzere farklı teknik yaklaşımlar aracılığıyla da desteklenebilir.

> *"…Güvenlik faaliyetleri olarak güvenlik duvarları, saldırı tespit sistemleri, saldırı engelleme sistemleri, uygulama tabanlı güvenlik duvarları kullanılarak zenginleştirilebilir. Aynı zamanda kullanılan güvenlik duvarlarının casus yazılımlar, virus, zararlı url, zararlı dosyalar, gibi tehditlere karşı koruyan yeni nesil güvenlik duvarları kullanmak önemlidir…"* Taylan

Bunların yanı sıra, bu teknik ve yaklaşımlar da göz önünde bulundurularak yukarıda bahsi edilen önlem, savunma ve öngörü faaliyetlerinin siber uzamın dinamik ve agresif faaliyetlerinde etkili ve anlık cevaplar oluşturabilmesi için akıllı sistemler de sınırlı yeteneğin mekanik bir kapsamda destek yapısı olarak kullanılabilir. Bu doğrultuda elde edilen bulgular "Akıllı Sistemlerin Kullanılması" alt temasıyla aşağıda yer almaktadır:

> *"…bu tür işleri insan faktöründen arındırıp yapay zekâ uygulamaları ve benzeri tekniklerle analizler halinde ortaya koymak ve bu doğrultuda algoritmalar geliştirip sistemi canlı bir sitem haline getirmek önemli olacaktır…"* Efe

> *"…yapay zekâyla güçlendirilmiş teknik destek hizmetlerinin yaygınlaştırılması önem arz etmektedir. İnsan kaynaklı hataları önleyebilmek adına stabil çalışan algoritmalara sahip destek hizmetlerinin tasarımlarının ve geliştirme süreçlerinin üzerinde daha fazla durulabilir…"* Efe

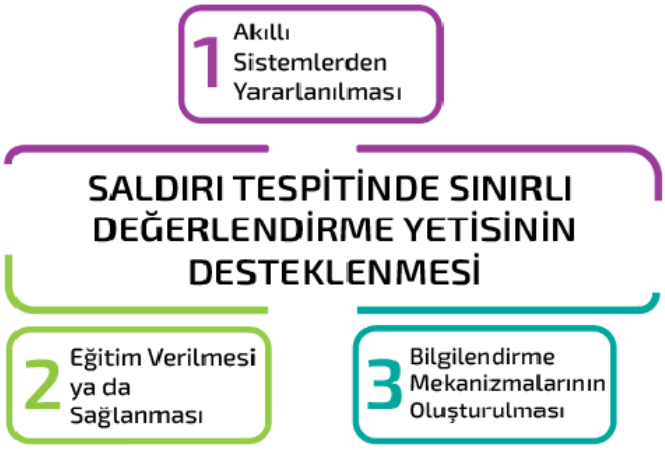
Bahsi edilen süreçlerin gerek insanlar tarafından gerekse akıllı sistemler tarafından yürütülmesinde koordinasyonun sağlanması, faaliyetlerin kontrol edilmesi ve sistemin paydaşlarıyla birlikte güvenliğinin sağlanması için iletişimin kritik bir öneme sahip olduğu söylenebilir. Bu görüş, "Birim ve Birey Bazlı İletişim Yapılarının Kurulması" alt teması altında yer alan bulguyla aşağıdaki gibi belirtilmiştir.

> *"…Düzenli olarak yetkin personel ile yeni personel arasında sağlıklı iletişim ve mentörlük olanaklarının sunulması; dinamik elektronik performans destek sistemlerinden yararlanılması; atipik durumları yaşayan personel ile gerek yetkin gerek yeni paydaşların buluşturularak mevcut çözüm önerilerinin ve alternatif çözümlerin mercek altına alınması önerilebilir…"* Ufuk

4.1.8. Sınırlı değerlendirme yetisiyle gerçekleştirilen saldırı tespit süreçlerinin desteklenmesi

Bireyin sınırlı bilişsel doğasının ve sınırlı karar verme kapasitesinin yansıması boyutu olan sınırlı değerlendirme yetisinin açık ve uzaktan öğrenme sistemlerinin siber güvenliğini sağlamada rasyonelliği riske attığı söylenebilir. Çünkü bir sistemin ya

güvenliği olduğundan ya da güvenli olmadığından bahsedilebilir. Başka bir ifadeyle güvenliğin ikili (binary) bir bulunuşluk olduğu savunulabilir. Güvenlik faaliyetlerinde gerek açık ve uzaktan öğrenme sisteminin teknik destek ekibinin değerlendirmesi gereken pek çok farklı aksiyon ve uygulama olduğu düşünülebilir. Bu doğrultuda bu araştırma kapsamında "siber saldırıların tespitinde sınırlı değerlendirme yetisine sahip teknik destek hizmeti uzmanlarının değerlendirme süreçleri nasıl desteklenebilir?" görüşme sorusu ile 8 uzmanın bu sınırlılığın desteklenmesi sürecine yönelik görüşleri toplanmıştır. "Saldırı Tespitinde Sınırlı Değerlendirme Yetisinin Desteklenmesi" temasını oluşturan bu bulgular; "bilgilendirme mekanizmalarının oluşturulması", "eğitimler verilmesi/ sağlanması" ve "akıllı sistemlerden yararlanılması" olmak üzere üç alt temada aşağıdaki gibi kategorize edilmiştir.



Şekil 4.8. *Saldırı tespitinde sınırlı değerlendirme yetisinin desteklenmesi*

Değerlendirme süreçlerindeki sınırlı kapasitenin desteklenmesinde farklı yapılanma ve yaklaşımların var olduğuna dair elde edilen bulgular doğrultusunda oluşturulan ilk alt tema "Bilgilendirme ve Müdahale Mekanizmalarının Oluşturulması" başlığı ile ilgili sürecin mekanikleşmesi adına aşağıdaki görüşleri içermektedir:

> *"...büyük resmi çizip dashboardlar oluşturup ondan sonra kişinin gidip geçmişle verileri kıyaslaması, ondan sonra mikro ölçekte sorunun olduğun muhtemel alanları inceleyebilecek şeyi, geçmiş verileri görebileceği, şu anki verileri, anlık verileri görebileceği, bir anomallik var mı onları izleyebileceği aslında o büyük resimdeki mikro ölçekteki detaylardan kastım*

buydu aslında. Yani bu tür bir yapılanma hem geçmişteki veriyle işte şu anki veriyi karşılaştırıp bir muhtemel bir pattern bir örüntü yakaladığında onun bir anomalliğe dönüşüp dönüşemeyeceğini sistemin tabi ki söyleyebilecek bir yapısı olursa çok güzel olur. Bu karar alma mekanizmalarını çok kolaylaştırır…" Emir

"…Doğrudan, eğer iyi yapılandırılmışsa destek sistemi, otomasyonu, hatanın nerede oluştuğu, güvenlik açığının nerede, ne zaman, nasıl oluştuğu bilgisini verir, ki bu en temel şeydir. Yani güç açısında düşünürsek en zayıf güvenlik protokolüdür, bilgi vermek. Bir sonraki aşama ne? Müdahale etmek. Aslında asıl olay o, müdahale etmek. Ama onun da bir üstü var. Müdahaleden sonra da benzer durumların yaşanmaması için de önlem almak. Tıpkı insanın da yaptığı gibi. Dolayısıyla teknik ekibe aslında üç aşamalı bir destek sunulmuş olur…" Cem

Yukarıdaki bulguların, siber güvenliğin sağlanmasındaki sınırlı değerlendirme yetisinin desteklenmesi için oluşturulacak bilgilendirme mekanizmalarının yalnızca bilgi sunma düzeyinde bir mekanizmadan çok; verilerle şekillenen, güncellenen ve beslenen bir yapıyı betimlediği söylenebilir. Sistemdeki faaliyetleri izleme, verileri kıyaslama ve bu doğrultuda gerek teorik gerekse uygulamalı bilgileri kullanma gibi farklı boyutları kapsayacağı öngörülen bu yapıların değerlendirme süreçlerindeki ilk adım olduğu savunulabilir. Bu doğrultuda atılacak sonraki adımların, değerlendirme süreçlerini maksimum rasyonelliğe ulaştıracak ileri aşamaları beslemesi gerektiği düşünülebilir. Dolayısıyla siber güvenliğin sağlanmasında değerlendirme süreçlerinin birbirini besleyen ve destekleyen bir "bilgilendirme birimleri topluluğu" olması önerilebilir. Bunun yanı sıra değerlendirme süreçlerini destekleyecek eğitimler sunulabileceğine dair bulgu, "Eğitimler Verilmesi/ Sunulması" alt temasında yer almaktadır.

"…Yani ben burada sınırlı değerlendirme yetisine sahip kişilere, belki ekstra hizmet içi eğitimler aklıma geliyor yani. Değerlendirme yeteneğini daha da arttırmak, hangi saldırı neye yöneliktir bunları bilebilmesi için ek eğitimlere mesela, yurtiçinde yurtdışında eğitimlere gönderilebilir…" Burak

Bilgilendirme mekanizmalarından farklı olarak, eğitim verilmesi ya da sunulması kapsamında siber güvenliğe yönelik yalnızca teorik ve uygulamalı enformasyonların aktarılabileceği bir yapının olduğunu söylemek mümkündür. Değerlendirme süreçlerindeki sınırlılığı beslemek için bu uygulamaların önemli olduğu söylenebilir. Çünkü sınırlı biliş ve karar verme yetisinin yansımalarından biri olduğu düşünülen sınırlı değerlendirme yetisinin kuvvetlenebilmesi için neyin, hangi kapsamda, ne amaçla ve neye karşı değerlendirilmesi gerektiğinin ilk olarak ilgili değerlendirme biriminin ne

hakkında olduğunu bilmekten geçtiği savunulabilir. Dolayısıyla bilgi kapsamında bireyleri, birimleri ve sistemleri eğitmenin önemli olduğu düşünülmektedir.

Siber güvenliğin sağlanabilmesi için sınırlı değerlendirme yetisinin desteklenmesinde "Akıllı Sistemlerden Yararlanılması", uzman görüşleri kapsamında oluşan bir diğer alt temayı temsil etmektedir. Aşağıda ilgili bulgular doğrudan aktarılmıştır.

> *"…Burada, değerlendirme süreçlerinde, akıllı sistemler vasıtasıyla belki, mesela yönetim bilişim sistemlerine, karar destek sistemlerine akıllı tekniklerle bazı eklemler yapmak gerekecek..."* Burak

> *"…teknik destek uzmanlarının gelişen teknolojiyle ortaya çıkmış bu tür akıllı sistemler konusunda bilgilendirme ve eğitilmelerine ihtiyaç duyulabilir. İnsan beyninin sınırlı hesaplama yetisi düşünüldüğünde destek hizmetleri kapsamında bu tür akıllı sistemlerin yapacağı analizler üzerinden üst analizler yapmak üzere eğitilebilirler. Ya da bu analizleri yorumlamak ve hayata geçirmek üzere…"* Efe

4.1.9. Siber uzamda yer alan sınırsız belirsizliğin tespit edilmesinde kullanılan teknikler

Dijital teknolojilerin süreğen gelişim ve dönüşümü ışığında evrilerek siber uzamı oluşturan 21.yüzyıl dünyasında siber güvenliğe yönelik agresif faaliyetler de gün geçtikçe gelişmekte ve dönüşmektedir. Sınırları genişleyen ve gün geçtikçe daha fazla veriyi, bireyi, teknolojiyi ve süreci barındıran siber uzamın, kötü niyetli faaliyetleri de barındırdığı görülmektedir. Açık ve uzaktan öğrenme sistemlerinin de içinde yer aldığı bu uzamdaki belirsizliklerin çeşitlenerek ve agresifleşerek artması öğrenme-öğretme faaliyetlerinin sürdürülebilirliği ve verimliliği için önemli görülmektedir. Bu doğrultuda bu araştırma kapsamında "siber uzamdaki sayısız belirsizliğin tespitinde ve değerlendirilmesinde teknik destek hizmetleri kapsamında nasıl teknikler geliştirilebilir?" görüşme sorusu ile 8 uzmanın sınırsız belirsizliğin bulunduğu siber uzamdaki açık ve uzaktan öğrenme sistemlerinin siber güvenlik faaliyetlerinde ilgili belirsizliklere yönelik geliştirebilecekleri tutumlara yönelik görüşleri alınmıştır. Elde edilen bulgular "Sınırsız Belirsizliğin Tespitinde Kullanılan Teknikler" başlıklı tema altında "insan-bilgisayar etkileşiminin oluşturulması", "akıllı sistemlerden yararlanılması", "blok zincir

teknolojilerinin kullanımı" ve "öneri sistemlerinin kurulması" alt temalarıyla aşağıdaki gibi şematize edilmiştir.

Şekil 4.9. *Sınırsız belirsizliğin tespitinde kullanılan teknikler*

Siber tehditlerin ya da saldırıların sınırsız bir uzamda sınırsız belirsizliğe yol açtığını işaret eden ilk temada ilgili belirsizliklerin insan ile makine etkileşimiyle çözülebileceği görülmektedir. Geçmiş ve mevcut güvenlik verilerinin kurumsal hafızayı oluşturacağı bir sistem önerisinde işin özünü bilen bireylerin yer almasının da önemli olduğu aşağıdaki doğrudan alıntıda belirtilmiştir:

> *"…çok farklı sorunlar gelebiliyor, bazen hiç beklemediğiniz bir taraftan olabiliyor. Dolayısıyla kişinin o anomalilikleri görebilmesi için her ne kadar bu işi mekanikleştirsek de insan aklının da hani o mekanikleştirme sürecindeki o makinelerin bilmeyeceği ama o kişide var olan know how ya da o kurum hafızası çok değerli. Dolayısıyla ikisini bir araya getiriyoruz burada. Yani hem sistemin o mekanikteki verileri kullanıyoruz ama öbür tarafta hiç makinelerin öngöremeyeceği ama kullanıcının o kurumsal hafızasından mütevellit oluşmuş deneyimini evidence-based bir yapıya dönüştürebileceği bir yapılanma…"* Emir

İnsan-bilgisayar etkileşimindeki kritik noktanın kurum hafızasını besleyen "nasıl olduğunu bilmek (know how)" olduğu görülmektedir. Bu doğrultuda süreçlerin ne olduğunu ya da süreçlerde neler yapılacağını bilen bireylerin sistemdeki makinelerle etkili bir etkileşim ve iletişim içinde olabilmesi için yeterli bilgiye ve değerlendirme yetisine sahip olması gerektiği düşünülebilir. Bunun yanı sıra elde edilen bulgular

doğrultusunda ilgili bilgisayarların öğrenen akıllı yapılar olmasını öneren başka bir alt temada aşağıdaki görüşler incelenmiştir:

> *"…bu tür işleri insan faktöründen arındırıp yapay zekâ uygulamaları ve benzeri tekniklerle analizler halinde ortaya koymak ve bu doğrultuda algoritmalar geliştirip sistemi canlı bir sistem haline getirmek önemli olacaktır…"* Efe

> *"…Mesela karar destek sistemleri burada yine geçerli, yani makine öğrenmesi yine geçerli olacak, akıllı ajanlar yine geçerli olacak. Dijital asistanlar kullanılabilir. (…) nesnelerin interneti ve her şeyin interneti sürecinde sayısız gerçekten belirsizlik orada gerçekleşebilir. Yani nerelere hangi saldırıların yapılacağı, en hassas noktalara neler gerçekleşebilir? Tabi sayısız belirsizlik var bu süreçte. Bu sayısız belirsizliği de hangi tekniklerle derseniz biraz önce söylediğim akıllı teknikler burada yine konuşmamız gereken…"* Burak

Yukarıdaki görüşler doğrultusunda açık ve uzaktan öğrenme sistemlerinin de içinde yer aldığı siber uzamdaki sınırsız belirsizliğin tespit ve analiz edilmesinde geçmiş güvenlik verileri her ne kadar önemli olsa da bu veriler doğrultusunda örüntüler oluşturup geleceğe yönelik öngörü ve önlem faaliyetleri yürütebilen akıllı yapıların kullanılmasının önemli olduğunu söylemek mümkündür. Özellikle nesnelerin interneti gibi gelişen ve çeşitlenen teknolojilerin ve teknolojik yaklaşımların siber uzamdaki olumlu ve faydalı faaliyetleri arttıracak olması olumsuz ve zararlı faaliyetleri de benzer oranda arttıracağına işarettir. Dolayısıyla dijital dünya teknolojilerinin gelişen, değişen ve dönüşen formlarını öğrenme faaliyetlerinde güncel bir şekilde kullanan açık ve uzaktan öğrenme sistemlerinin bu yenilikleri güven içinde takip edebilmesi adına akıllı sistemlerin kullanılmasının önemli olduğu görülmektedir.

Her ne kadar teknolojik yeniliklere hazırlıklı olmak önemliyse bu teknolojileri güvenlik faaliyetlerine de dahil etmek önemli görülebilir. Çünkü güncellenen dünyanın ritmine güncel yaklaşımlarla ayak uydurmanın daha kolay ve tutarlı olacağı söylenebilir. Bu doğrultuda sınırsız belirsizliğin yer aldığı siber uzamda kullanılabilecek tekniklerden birine blok zincir teknolojilerinin kullanımı aşağıdaki görüş ile örnek verilmiştir:

> *"…Yeni teknikler geliştirilebilir. Yani mevcutların üstüne yeni teknikler geliştirilebilir. Ben burada da blockchain teknolojisinin çok güzel kullanılabileceğini düşünüyorum…"* Cem

> *"…benim önerim güvenlik protokollerini yapılandırırken bu protokolleri merkezi serverlarda değil; blockchain teknolojisi ile dağıtık sistemlerde tutmak. Bu da saldırıların tamamen devre dışı kalması demek. Çünkü güvenliğim merkezde değil. Güvenliğim dünyanın*

her yerinde. Yani sen bütün dünyaya saldırırsan ancak benim güvenlik mekanizmalarımdan, protokollerimden mahrum edebilirsin. Bu da yeni teknikler. Cem

Tüm bunların yanı sıra sistem verilerinin geleceğe yönelik saldırı ve tehditlerin indirgenmesi için örüntü, öneri ve öngörü oluşturmak için önemli olduğu söylenebilir. Çünkü bir saldırıya gerçekleştiği anda hızlı cevap verebilmek kadar o saldırının geleceği yolu öngörüp açıkları kapatmanın da önemli olduğunu söylemek mümkündür. Bu doğrultuda sınırsız belirsizliğin tespit edilmesinde öneri sistemlerinin kurulmasına yönelik alt temada aşağıdaki görüşler yer almaktadır:

"…Bilişim sistemlerimizi gizlilik, bütünlük ve erişilebilirlik açısından siber saldırılara karşı korumak destek hizmetleri kapsamında önemli bir görevdir. Siber uzamdaki sayısız belirsizliğin tespitinde ve değerlendirilmesinde öneri sistemleri yaklaşımı geliştirilebilir. Bir saldırının daha önce hangi yoldan tespit edildiğini ve benzer saldırıların ne tür yollardan gelebileceğini tahmin edecek öneri sistemleri yaklaşımı geliştirilerek saldırı tespiti yapılabilir…" Taylan

"…Yetkin paydaşların gerek erken tespit sırasında işe koştuğu mevcut çözümlerin, gerekse ortak akıl toplantılarında gündeme getirilen diğer alternatif önerilerin ve bunların doğurgularının paylaşımı ile yol haritaları oluşturulabilir…" Ufuk

4.1.10. Savunma ve tespit faaliyetlerinin gerçekleştirilmesinde faaliyet gösteren karar destek sistemlerinin güçlendirilmesinde kullanılan mekanizmalar

Siber uzamda durmadan çeşitlenerek ve farklılaşarak gerçekleşen agresif faaliyetlerin tespit edilmesinin zor ve bir o kadar kritik olduğu söylenebilir. İlgili faaliyetlerin tespit edilmesi bu doğrultuda savunma stratejilerinin ve uygulamalarının gerçekleştirilmesinde ise belirli strateji, protokol ve uygulamaların nasıl sürece nasıl dahil edileceği, hayata geçirileceği ve sürdürüleceğine dair süreç ve sonuç odaklı karar süreçlerinin olduğunu söylemek mümkündür. Açık ve uzaktan öğrenme sistemlerinde teknik destek hizmetleri kapsamında ilgili süreçlerin planlanmasına, tasarlanmasına ve yürütülmesine dair uzman görüşleri "sınırlı karar verme yetisine sahip bireyler tarafından kontrol edilen savunma ve tespit karar sistemlerini güçlendirilmek için hangi mekanizmalar nasıl kullanılabilir?" görüşme sorusu aracılığıyla toplanmıştır. Bulgular doğrultusunda aşağıdaki alt temalara ulaşılmıştır.

Şekil 4.10. *Savunma ve tespit karar sistemlerinin güçlendirilmesinde kullanılan mekanizmalar*

Araştırma kapsamında yapılan görüşmelerden elde edilen bulguların analizi sonucunda "verilerin korunması ve depolanması", "öngörü protokollerinin oluşturulması", "eğitim verilmesi/ sağlanması", "güvenlik uzmanlarının yetiştirilmesi ya da işe alınması" ve "akıllı sistemlerden yararlanılması" alt temalarına ulaşılmıştır. Dijitalleşen teknolojiler sayısında veri üreten, dağıtan ve veriden beslenen açık ve uzaktan öğrenme sistemlerinin siber saldırılara karşı tespit ve savunma faaliyetleri gerçekleştirmelerinde verilere yönelik öncelikli faaliyetlerin gerçekleştirilmesi gerektiğine dair elde edilen bulgu aşağıda doğrudan alıntı olarak verilmiştir:

> *"…Yani burada tabi hep aklımıza gelen büyük verinin korunması süreçleri... Bu büyük veriyi ve analitik veriyi korumak için veri tabanı güvenliği çok önemli. Yani veri tabanını eğer güvenli tutarsak ve bunun yedeklemesini mutlaka, yani yedek belki birden fazla da olabilir, belki serverlar yurtdışında da kurulabilir…"* Burak

Geçmiş güvenlik verilerinden yola çıkarak tespit ve savunma faaliyetlerindeki karar süreçlerinin beslenmesini işaret eden bu bulgunun sistemin geçmiş verilerden örüntüler oluşturarak beslenebilmesi için öncelikle verilerin korunmasının önemini vurguladığı görülmektedir. Dolayısıyla karar süreçlerinin mekanik olarak desteklenebilmesi için öncelikle verinin üretimindeki, dağıtımındaki ve depolanmasındaki süreç ve stratejilerin güvenliğini sağlamak gerektiği düşünülebilir. Bunun yanı sıra sistemdeki teknik ekibin eğitilmesinin de ilgili mekanizmaları oluşturma ve sürdürme aşamalarında gerekli olduğu bulgulanmıştır.

"…öz kaynaklarımızla çözemiyorsak ekstra serverlarla, yedek alarak veya mesela alanında dünyanın en iyisi kişileri bir beyin transferi şeklinde gelip mesela burada eğitimler versinler; o siber güvenlik uzmanlarının hiç bilmediği o önlemleri hayata geçirsinler…" Burak

"…sonuçta bir tehdit olduğunda nelere olabileceğine dair, işte dedik ya bir karar destek sistemi… İşte bu sistemi kullanacak teknik destek ekibi eğitilebilir, düzenli aralıklarla. İşte farklı simülasyonlarla…" Ayça

Yukarıdaki bulgular, eğitimlerin güncellenebilir ve sürekli olması gerektiğini işaret etmektedir. Bu, siber uzamdaki belirsizliğin dinamik yapısına göre şekillenen bir yaklaşımın gerekli olduğunu desteklemektedir. Benzer doğrultuda fakat daha farklı bir kapsamı ifade eden bir diğer alt temada yetersiz sayıdaki güvenlik uzmanlarının yetiştirilmesi ve işe alımı süreçlerine dikkat çekmektedir.

"…yani siber güvenlik alanında çalışan çok uzman kişi yok. Ve bu uzman kişilerin bir bölümü de kötü niyetli. Az, elimizde ufacık bir grup kalıyor. Bu ufacık grubu zaten beslememiz gerekiyor. Bir de o ufacık grubu belki çoğaltmak için dediğim gibi biraz önceki o kötü niyetli kişileri bir şekilde sisteme dahil etmek de bir çözüm olabilir diye düşünüyorum…" Burak

"…merkezi ya da bölgesel yapılarda yetkin personel sayısının ve personelin mevcut yetkinliğinin düzenli olarak desteklenmesi; bölgesel olarak nöbet sisteminin hayata geçirilmesi dikkate alınabilir…" Ufuk

Sistem açıklarını en iyi kapatacak kişinin o sistemdeki açıkları en iyi bilen kişiler olması gerektiği söylenebilir. Yukarıdaki bulgular, sistemin güvenliğinin sağlanmasında saldırı faaliyetleri gerçekleştirmiş kişilerin yer almasının farklı ve etkili bir yapılanma olabileceğini göstermektedir. Bu doğrultuda işe alınacak kişilerin belirli yarışmalar ya da teşvik ödülleriyle seçilerek sözleşmeler doğrultusunda sisteme dahil edilmesi öngörülebilir. Bunun yanı sıra ilgili kişilerin rol tanımlarının yapılmasının ve görev tanımları kapsamında birimlere ayrılan iş süreçlerinin merkezi bir havuzda yer alması gerekebilir. Bu bulgulara ek olarak saldırıların tespit edilmesinde ve savunulmasında öngörü yapılarının kurulmasının önemli olduğunu vurgulayan görüşler aşağıda yer almaktadır:

"…şunu düşünmemeliyiz: günümüzde bu koşullar var, ben bu sınırlılıklar içerisinde sadece işte doğal dil işlemeyi devreye koyabiliyorum; bunun ötesine geçemiyorum dememek lazım. Şunu demek lazım: 10 yıl sonra beklenen gelişim bütün dünyanın bir meta evrende oluşacağı, bir işte siber uzay, ismine ne derseniz deyin bir dijital dünyada olacağı ve eksiksiz bir evren olacağı. İsmine neden evren diyoruz, dünya diyoruz? Dünyada olup bitenlerin tamamını yapabileceğimiz bir yer. Bunu düşünerek eğer güvenlik protokollerinizi, mekanizmalarınızı,

ona göre önü açık geliştirirseniz, bunu göz önünde bulundurursanız işte o zaman eskime riskini de ortadan kaldırırsınız…" Cem

"*…Bürokrasi ve siber hukuk bağlamında da onaylanmış, ortak akıl sonucu belirlenmiş adımların mekanikleştirilmesi, standartlaştırılması yoluna gidilebilir…"* Ufuk

Son olarak görüşme sorusu kapsamında elde edilen bulgular, tespit ve savunma faaliyetlerinin gerçekleştirilmesinde akıllı sistemlerden yararlanmasını vurgulamaktadır. Daha önceki bulguların temel oluşturduğu görüşleri destekleyen bu görüşlerde genel yapının insan faktöründen kaynaklanabilecek güvenlik problemlerinin ya da açıklarının verilerden öğrenme yolları oluşturan mekanizmalar tarafından geçmiş ve mevcut verilere dayanarak yapılandırılmasının önemli olduğu belirtilmiştir.

"…yapay zekayla güçlendirilmiş teknik destek hizmelerinin yaygınlaşıtrılması önem arz etmektedir. İnsan kaynaklı hataları önleyebilmek adına stabil çalışan algoritmalara sahip destek hizmetlerinin tasarımlarının ve geliştirme süreçlerinin üzerinde daha fazla durulabilir…" Efe

"…Ama siber güvenlikte tamamen insanlar, yani sınırlı bilgi evet doğru, tamamen insanlara bırakılmasının da doğru olmadığını, biraz önce bahsettiğim mekanikleşme sürecinin bu bahsettiğim uygulamalarla, yazılımlarla gerçekleşmesi gerektiğini söylüyorum sadece…" Burak

"…Savunma ve tespit karar sistemlerini güçlendirmek için bu sistemlerde derin öğrenme algoritmaları, makine öğrenmesi algoritmaları, yapay zeka sistemleri kullanılabilir. Aynı şekilde bu algoritmalar hibrit bir şekilde kullanılabilir. Saldırıların tespitinde makine öğrenmesi algoritmalarında kullanılan algoritmaların saldırıyı hem doğru hem de hızlı bir şekilde tespiti saldırıya müdahale açısından önemli bir konudur…" Taylan

"…Yani aslında şu da olabilir, eğitim datası sistem kullanılmaya başlandığında da işte aylık o verilerin bir kısmı yine eğitim datasına aktarılıp makine öğrenmesinin de yine yeni verilerle de öğrenmesini test edip de sağlayabiliriz…" Ayça

Elde edilen bulgular doğrultusunda tespit ve savunma faaliyetlerinde öncelikle verilerin, daha sonra bu verilerin öğrenen mekanizmalarda kullanılmasını programlayacak kişilerin eğitilmesinin ya da güvenlik uzmanlarının işe alınması gerektiğinin, ilgili yapıyı mekanikleştireceği söylenebilir.

4.2. Araştırma Sorularının Yanıtlanması

Doküman analizi ve görüşmeler doğrultusunda elde edilen tüm bulgular ilk olarak açık ve uzaktan öğrenme sistemlerinde siber güvenliğin öğrenme faaliyetlerinde yer alan

tüm paydaşları, varlıkları, birimleri ve sistemin kendisini kapsadığını göstermektedir. *"Açık ve uzaktan öğrenme sistemlerinde siber güvenlik faaliyetleri sistemin hangi bileşenlerini ve bireylerini kapsamaktadır?"* araştırma sorusunu yanıtlamak amacıyla toplanan veriler, açık ve uzaktan öğrenme sistemlerinin benimsediği açıklık politikası ve bünyesinde farklı rollerle yer alan çok sayıdaki paydaşı ile siber saldırılara açık birer hedef olduğunu işaret etmektedir. Siber güvenlik faaliyetlerinde öncelikli olarak sistem yapılanmasının önemini vurgulayan bulgular, güvenliği sağlamak adına birimler arası iletişim ve koordinasyonun da kritik olduğunu işaret etmektedir. Bunun yanı sıra siber güvenlik kapsamında bireylerin ve birimlerin olası saldırı senaryolarına yönelik farkındalık ve aksiyon eğitimlerinin de önemli olduğu görülmüştür. Teknik destek hizmetleri kapsamında ele alınan siber güvenlik faaliyetlerinin yalnızca teknik ekibi ilgilendirmediğini işaret eden bulgularda, açık ve uzaktan öğrenme faaliyetlerinde siber güvenlik faaliyetlerine yönelik ayrı birimlerin kurulması gerektiği belirtilmiştir. Dolayısıyla açık ve uzaktan öğrenme sistemlerindeki siber güvenlik faaliyetlerinin teknik ekibi de içine alan bir yapılanmayla desteklenmesi gerektiği söylenebilir.

Araştırma kapsamında yanıt aranan *"açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanmasında sistem paydaşlarının ve teknik destek hizmetlerinin sınırı ve sınırlılıkları nedir?"* sorusu doğrultusunda toplanan veriler, teknik destek ekibinin siber güvenlik ekibinden ayrı tutulmamasından kaynaklandığını göstermektedir. Siber güvenlik faaliyetlerini yürütmede kalifiye elemanlardan oluşan bir birimin gerekliliğini vurgulayan bulgular, bu doğrultuda kurum hafızasının da önemli olduğunu işaret etmektedir. Ayrıca sistemdeki paydaşların ve teknik ekibin bir diğer sınırlılığının sınırlı bilişsel kapasiteye sahip olmalarından kaynaklandığı bulgular tarafından desteklenmiştir. Bu doğrultuda gerek sistem paydaşlarının gerekse teknik ekibin gerekli ve yeterli siber güvenlik farkındalığına sahip olmaması, teknik ekibin bu faaliyetlere yönelik eğitimler görmemesi, kurumsal siber güvenlik kültürünün olmaması, güvenlik faaliyetlerinde rol ve sorumluluk dağılımlarının yapılandırılmaması ve tüm bunların yönetsel bir destek altında ele alınmaması sınırlar ve sınırlılıklar olarak tanımlanmıştır.

"Açık ve uzaktan öğrenme sistemlerinin teknik destek hizmetlerinde siber güvenliğin sağlanması için makine öğrenmesinden nasıl yararlanılabilir?" sorusuna yönelik elde edilen bulgularda öncelikle sistemdeki paydaşların faydalanması gereken bir bilgilendirme mekanizmasının kullanılması gerektiği önerilmiştir. Bu mekanizmanın

öğrenen bir mekanizma olması; dolayısıyla siber güvenliğin sağlanmasında farkındalık ve öngörü oluşturması savunulmuştur. Bu doğrultuda oluşturulması önerilen kurum hafızasının, farklı kurumlarla etkileşim halinde olan bir yapılanma ile kuvvetlendirilmesi vurgulanmıştır. Aynı zamanda oluşturulacak kurum hafızasının kurumsal bir siber güvenlik kültürünü de temsil etmesinin önemli olduğu görülmüştür. Bu faaliyetlerin siber güvenliği sağlamak için sosyal bir boyutu ifade ettiği düşünülebilir. Sosyal boyutun yanı sıra akademik ve teknik boyutların da olduğu söylenebilir. Akademik boyutu temsil eden bulgularda siber güvenliğin sağlanması için kullanılacak makine öğrenmesi algoritmalarının ve mekanizmalarının oluşturulmasında eğitimli ve nitelikli personelin işe alınmasının önemli olduğu belirtilmiştir. Aynı zamanda bu bağlamda faaliyet gösterecek kişilerin siber güvenlik eğitimleri almış kişiler olması gerektiği vurgulanmıştır. Bulgulardan da elde edilen sonuçlar doğrultusunda makine öğrenmesinin siber güvenlik faaliyetlerinde rol oynayan bireylerin sınırlı doğasını desteklemesi; fakat bu destek yapısının oluşturulması için ise nitelikli bireylerin sürece dahil edilmesi gerektiği sonucu çıkarılabilir. Dolayısıyla bu noktada insan-bilgisayar etkileşiminin göz önünde bulundurulması gerektiği görülmektedir. Bu boyutun hem teknik hem de akademik bir kapsama sahip olduğu düşünülebilir. Bunların yanı sıra teknik bir bakış açısıyla siber güvenliğin sağlanmasında nesnelerin interneti, blok zincir teknolojileri, derin öğrenme modelleri ve doğal dil işleme gibi farklı tekniklerin ve teknolojilerin öğrenen akıllı sistemleri oluşturmada önemli olduğu belirtilmiştir. Dolayısıyla siber güvenliğin sağlanmasında makine öğrenmesi hem sosyal hem akademik hem de teknik açıdan başvurulması gereken bir yaklaşım olarak görülmektedir.

5. TARTIŞMA

Açık ve uzaktan öğrenme sistemlerinde teknik destek hizmetleri kapsamında ele alınan siber güvenlik faaliyetlerinin bilişsel sınırlılıklar göz önünde bulundurularak endüstrileşmesini savunan bu çalışma, üç araştırma sorusu kapsamında hazırlanan 10 görüşme sorusu ile 8 ayrı alan uzmanından görüşler alındığı bir durum çalışmasıdır. Bu doğrultuda elde edilen bulgular, çalışmanın bu bölümünde konuyla ilişkili alanyazın ışığında tartışılmıştır.

5.1. Açık ve Uzaktan Öğrenmede Siber Güvenliğin Kapsamı

Araştırmayı şekillendiren araştırma sorularından biri olan "*açık ve uzaktan öğrenme sistemlerinde siber güvenlik faaliyetleri sistemin hangi bileşenlerini ve bireylerini kapsamaktadır?*" sorusu kapsamında açık ve uzaktan öğrenme sistemlerinde siber güvenliğin yeri ve önemi incelenmiştir. Gerek konuyla ilgili literatürden gerekse uzman görüşlerinden elde edilen bulgular doğrultusunda siber güvenliğin açık ve uzaktan öğrenmedeki kapsamı saptanmaya çalışılmıştır.

Kağıttan güncel internet teknolojilerine kadar farklı teknolojilerin öğrenme süreçlerinde çeşitli amaçlarla gerek araç gerekse aracı olarak kullanılabildiği açık ve uzaktan öğrenme sistemlerinin farklı teknolojiler ile yapılandığını; dolayısıyla bu yapılanmanın teknik ve teknolojik bir varoluşu temsil ettiğini söylemek mümkündür. Kendine özgü kapsamlı bir atmosferi olan açık ve uzaktan öğrenme sistemlerinde öğrenme süreçleri ile ilişkili pek çok faaliyet, uygulama ve hizmet yürütülmektedir. Bu süreçlerde ise öğrenen, öğreten, personel ya da yönetici gibi farklı paydaşların farklılaşan amaçları, beklentileri ve ihtiyaçları doğrultusunda çeşitli teknolojiler süreçlerin tasarımında, yönetiminde ve sürdürülebilirliğinde kullanılmaktadır (Genç Kumtepe vd., 2019).

Teknoloji kullanımıyla şekillenen ve yine teknoloji kullanımı gerektiren açık ve uzaktan öğrenme atmosferinin genel anlamda dijital dünyada gerçekleştirilen eylemleri kapsadığını söylemek mümkündür. Fakat teknoloji kullanımıyla gerçek dünyanın sanal bir tezahürü olan dijital dünya, günden güne gerek kişileri gerek kurumları gerekse hükümetleri hedef alan çeşitli suçların işlendiği ya da saldırıların gerçekleştiği bir siber uzam dönüşmüştür (Alexei, 2021; Fischer, 2016). Bu noktada dünyanın farklı yerlerindeki çeşitli paydaşları farklı teknolojiler aracılığıyla bir sistem çatısında bir araya getiren açık ve uzaktan öğrenme sistemleri ise siber saldırılara oldukça açık ve faydalanılabilecek bir hedef haline gelmiştir (Alexie & Alexie, 2021; Bandara, Ioras & Maher, 2014). Araştırma kapsamında elde edilen bulgular ise, sınırsız belirsizliğin var olduğu siber uzamda varlık gösteren açık ve uzaktan öğrenme sistemlerinin siber saldırılardan doğrudan etkilendiğini ve etkilenmeye devam edeceğini işaret etmektedir.

Bireylerin ya da kurumların karar verme süreçlerindeki rasyonelliği sınırlayan üç faktörün "risk ve belirsizlik, "eksik enformasyon" ve "karmaşıklık" olarak sıralandığı

Sınırlı Rasyonellik Kuramı (Simon, 1972) kapsamında şekillenen bu çalışmada, siber güvenlik faaliyetlerinin siber uzamda yer alan sınırsız belirsizlik ve bireylerin sınırlılıkları dolayısıyla rasyonel bir şekilde yürütülmesinin mümkün olmadığı varsayımı, sekiz farklı alan uzmanıyla yapılan görüşmeler doğrultusunda elde edilen bulgularla desteklenmiştir. Teknolojik değişimler, dönüşümler ve gelişimler göz önünde bulundurulduğunda ise sınırsız belirsizliğin ve veri hacminin arttığı doğrultuda bireysel sınırlılıkların arttığı varsayılabilir. Moore Yasasına göre (1965) bu ivmeli artış, her 1,5 senede bir devre elemanlarının barındırabileceği bileşen kapasitesinin 2 katına çıkmasına rağmen üretim maliyetinin düşme eğiliminde olması prensibini yansıtmaktadır. Moore Yasası 2020'li yıllardan itibaren her ne kadar etkisini, artıştaki ivmenin kontrol edilemez hızıyla kaybetmiş olsa da (Candoğan, 2020) siber uzamda da benzer bir senaryonun olacağından söz etmek mümkündür.

Donanım cihazlarının siber saldırılara maruz kalmasıyla başlayan sürecin yazılım boyutunda artan bir ivmeyle ilerlemesi ve artık dijital dünyanın bütün verilere ve nesnelerine erişilebiliyor olması ve bunu yapmak için gerekli olan maliyetin gitgide düşmesi (Chadd, 2020) Moore Yasası'ndakine benzer bir ivmeli artışı işaret etmektedir. Bu noktada siber güvenliğin sağlanmasında büyük verinin ve nesnelerin interneti kavramlarının; siber saldırıların etkisini, yönünü ve büyüklüğünü gerek olumlu gerekse olumsuz bir şekilde değiştirecek bir geleceğe sahip olduğu söylenebilir. Açık ve uzaktan öğrenme ortamları için gelecek vadeden kavramlardan olan büyük veri ve nesnelerin interneti ile gerçek dünyada fiziksel olarak var olan nesnelerin ve insanların siber uzamda internet aracılığı ile etkileşim ve iletişim halinde olmaları farklı kanallar aracılığıyla mümkün hale gelmiştir (Altınpulluk, 2018).

Açık ve uzaktan öğrenme ortamlarında çeşitlenen teknolojilerin farklı faaliyetler kapsamında kullanılmasıyla birlikte nesnelerin interneti kavramının da kullanılmasının kaçınılmaz olduğu düşünülebilir. Fakat insanlar ve nesneler arasındaki bu iletişim ve etkileşim, büyük verinin ve nesnelerin interneti teknolojilerin siber saldırılara açık birer hedef olmasına yol açmakta ve bu teknolojilerin gerek kullanımını gerekse faydalı bir şekilde yayılmasını engellemektedir (Alferidah & Jhanjhi, 2020). Bu araştırmada elde edilen bulgular doğrultusunda siber güvenlik faaliyetlerin hem mevcut hem de gelecekteki açık ve uzaktan öğrenme faaliyetlerinin planlanmasında, şekillenmesinde ve yürütülmesinde göz önünde bulundurulması gerektiğini söylemek mümkündür.

Araştırmada elde edilen bulgulara göre siber güvenliğe yönelik geçmiş deneyimlerin ve kurumsal siber güvenlik kültürünün, çeşitlenen güvenlik faaliyetlerinde önemli bir rol oynadığı görülmüştür. Çünkü bilgi kültürünün önemli bir parçası olan siber güvenlik kültürünün oluşturulmasının modern toplum ve modern eğitim ögelerinin bütünlüğünü sağlayacağı savunulabilir. Kurumsal çerçevede siber güvenlik kültürü oluşturmak; teknik önlemlerin yanı sıra kurumsal önlemlerin de alındığı bir oluşum sürecini ifade etmektedir (Reegård, Blackett, & Katta, 2019). Siber güvenlik kültürünün oluşturulması her ne kadar teknik elemanların, birimlerin ya da yapıların eğitilmesini içerse de tamamen bunu kapsamadığını söylemek mümkündür.

Bireylerin, birimlerin, sistemlerin, kurumların ve devletlerin siber güvenliği sağlamak adına belirli sorumluluklardan haberdar olmaları ve bu sorumlulukları bir kültür ögesi olarak üstlenmeleri oldukça önemlidir (Malyuk & Miloslavskaya, 2016). Siber güvenlik kültürünün oluşturulması için Reegård, Blackett ve Katta (2019); "yönetim desteği", "siber güvenlik politikası", "siber güvenlik farkındalığı ve eğitimleri", "katılım ve iletişim" ve "deneyimden öğrenme" bileşenlerinin sistem yapısında bulunması gerektiğini savunmuştur. Bu araştırmada elde edilen bulgular doğrultusunda ise kurumsal siber güvenlik kültürünü besleyen bileşenlerin sırasıyla:

- Enformasyon ve uygulama topluluklarının oluşturulması,
- İletişim ve bilgilendirme mekanizmalarının kurulması,
- Geçmiş öğrenmelerden ve deneyimlerden yararlanılması,
- Bireyler ve birimler arasında ağız ve iş birliğinin kurulması,
- Rol ve sorumluluk tanımlarının yapılandırılması,
- Yönetsel desteğin oluşturulması ve
- Eğitim ve farkındalık çalışmalarının sağlanması olduğu görülmüştür.

Bu noktada kurum kültürünün oluşturulmasında teknik, teknolojik, yönetsel, akademik ve sosyal kararların alınması ve bu doğrultuda hizmetler sunulması gerektiği söylenebilir. Bu noktada açık ve uzaktan öğrenme sistemlerinde siber güvenlik kültürünü oluşturmak için bu hizmetler göz önünde bulundurularak bir destek yapılanmasına gidilebileceği savunulabilir. Siber güvenliğin sağlanmasında teknik destek hizmeti çatısı altında incelenmesi gereken faaliyetlerin sistemin tümünü kapsayacak şekilde şekillenmesinin ise sistem güvenliğinin yanı sıra devamlılığının da sağlanmasında önemli olduğu düşünülmektedir.

5.2. Açık ve Uzaktan Öğrenmede Siber Güvenliğin Sağlanmasında Sınırlı Rasyonellik

Siber güvenliğin açık ve uzaktan öğrenme sistemlerindeki yeri ve öneminin yanı sıra siber güvenliğin sağlanmasının, güvenliği sağlayacak yapıların ve tüm bu ilgili süreçlerin incelenmesinin önemli olduğu düşünülmektedir. Bu noktada siber güvenliğin sağlanmasındaki öncelikli aktörün insan olduğu görülmektedir (Bone, 2016; Chowdhury, Adam & Teubner, 2020). Sınırlı Rasyonellik Kuramı çerçevesinde şekillenen bu araştırmada, insan faktörünün sınırlı bilişsel doğasının siber güvenliğin sağlanmasındaki rasyonaliteyi sınırladığı savunulmaktadır. Bu doğrultuda bu araştırma kapsamında "*açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanmasında sistem paydaşlarının ve teknik destek hizmetlerinin sınırı ve sınırlılıkları nedir?*" sorusuna yanıt aranmıştır.

Ekonomi çerçevesinde yapılanan Sınırlı Rasyonellik Kuramı ile Herbert Simon (1955: 1976), değerlendirme ve karar verme süreçlerinin rasyonel olmasını sınırlayan bazı faktörlerin olduğundan ve bu faktörlerin hiçbir zaman tamamen ortadan kaldırılamayacağından bahsetmektedir. Simon (1976) 'a göre insan, rasyonel karar alma mekanizmasını gerçekleştiremeyecek sınırlılıklara sahiptir. Bu sınırlılıkların ise sosyal bir varlık olan insanın bilişsel doğasından kaynaklandığı; insan faktörünün doğası gereği sınırlılığı, belirsizliği ve değişkenliği beraberinde getirdiği araştırma kapsamında elde edilen bulgularla desteklenmektedir. Dolayısıyla bu kurama göre bireylerin rasyonel karar alma ve değerlendirme yetilerinin sınırsız belirsizlik kapsamında çizilen belirli bir sınır çerçevesinde ele alınabileceği savunulmaktadır. Söz konusu siber güvenliğin sağlanması olduğunda da benzer durumla karşılaşmak mümkündür. Gerek literatür (Alferidah & Jhanjhi, 2020; Bone, 2016; Chowdhury, Adam & Teubner, 2020) gerekse araştırma bulguları siber uzamın sınırsız belirsizliği içeren sanal bir dünyayı ifade ettiğini işaret etmektedir.

Organik bir yapıda olan gerçek dünyanın sentetik bir formu olan siber uzamın; insan bilinciyle, davranışıyla, tıklamalarıyla ve etkileşimleriyle oluşan bir simülasyonu ya da bir davranış çıktısını temsil ettiği söylenebilir. Dolayısıyla bu noktada insan müdahalesiyle oluşmuş bir yapıdan söz edilebilir. Büyük verinin ortaya çıkışı ve dijital teknolojilerin yaygınlaşması ile daha da genişleyen siber uzamdaki (Alferidah & Jhanjhi,

2020; Dhillon, 2020) eğitim sistemlerinde bu tür verilerin çeşitlenen teknolojiler ile üretilmesi, dağıtılması ve depolanmasıyla bireylerin bilişsel sınırlılıklarının daha da arttığı düşünülmektedir.

Öğrenme-öğretme faaliyetlerini siber uzamda gerçekleştiren açık ve uzaktan öğrenme sistemlerinin, siber güvenlik planlamalarında ve uygulamalarında yukarıda bahsedilen belirsizlik ile karşı karşıya olduğu savunulabilir. Sınırsız belirsizlik kapsamındaki risklerin ve saldırıların öngörülmesinde, önlenmesinde ve savunulmasında ise bireysel değerlendirme, karar verme ve yeterlikler, siber güvenliğin kaderini belirlemektedir (Bone, 2016). Bu doğrultuda bu çalışmada açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanması süreçlerinde ilgili sınırlılıkların tespit edilebilmesi için Sınırlı Rasyonellik Kuramı göz önünde bulundurulmuştur. Sınırlı Rasyonellik Kuramı kapsamında açık ve uzaktan öğrenme sistemlerinde siber güvenliği riske atan sınırlılıklar aşağıdaki gibi sıralanabilir:

- Sınırlı bilgi,
- Sınırlı yetenek,
- Sınırlı değerlendirme yetisi,
- Sınırlı karar verme yetisi ve
- Siber uzamda yer alan sınırsız belirsizlik.

Bu noktada sınırlı bilgi, bir konu hakkındaki tüm enformasyonun bilişsel olarak elde edilemeyeceğini savunurken sınırlı yetenek gerekli yeterlikler ve yetkinlikler olmasına rağmen sınırlı bir aksiyonun ortaya çıkacağını öne sürmektedir (Bone, 2016; Li, 2018). Benzer şekilde gerek bireysel gerekse kurumsal kararların alınması; bu kararların, süreçlerin ya da çıktıların değerlendirilmesi süreçlerinde hem sınırlı bilgi hem sınırlı yetenek hem de sınırsız seçenek doğrultusunda bir sınırlılık söz konusudur (Bone, 2016; Zhang vd., 2021). Araştırma kapsamında elde edilen bulgular ise sınırsız belirsizliğin sınırlı bilgiyi; sınırlı bilginin sınırlı yeteneği; sınırlı bilginin ve yeteneğin sınırlı değerlendirmeyi; sınırlı değerlendirmenin sınırlı karar vermeyi; ve tüm bunların ise yine sınırsız belirsizliği hem etkilediğini hem de sınırsız belirsizlikten etkilendiğini göstermiştir. Dolayısıyla bulgular doğrultusunda açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanmasında:

- Saldırıyı ya da tehdidi ayırt edecek ya da savunma faaliyetlerinde ne yapılacağına dair yeteri kadar bilgiye sahip olmak,
- Bir saldırının sistemi ve sistemin bileşenlerini nasıl etkileyeceğini değerlendirmek,
- Risk ya da saldırı karşısında yapılacak savunmaya karar vermek,
- Bir karar doğrultusunda ilgili karara karşılık gelen faaliyeti gösterecek yeterliğe ve yeteneğe sahip olmak,
- Sınırsız seçenek arasında doğru bilgiye ulaşmak, doğru değerlendirmeyi yapmak, doğru kararı vermek ve doğru yöntemi uygulamak gibi sınırlılıklardan bahsetmek mümkündür.

Açık ve uzaktan öğrenmede siber güvenliğin sağlanmasındaki süreçlerin tümünde farklı görev tanımlarıyla yer alan bireylerin sistemdeki tüm paydaşları kapsadığı söylenebilir. Bir siber güvenlik kültürü çerçevesinde kurumsal bir topluluğu temsil eden bu paydaşların her birinin siber güvenlik faaliyetlerinde rol oynadığını savunmak mümkündür. Çünkü siber güvenliği yalnızca teknolojiyi bilmek ya da teknik ekibe sahip olmak şeklinde adlandırmak ve yapılandırmak oldukça yanlış ve tehlikeli bir savunma stratejisi olacaktır (Dhillon, 2020; Li, 2018). Dolayısıyla farklılaşan siber güvenliğin faaliyetlerinde açık ve uzaktan öğrenmenin öğrenen, öğreten, yönetici ve personel olmak üzere her biri sınırlı bir bilişsel doğaya sahip olan tüm paydaşların yeri ve sorumlulukları olduğu düşünülebilir.

Bir sistemde yer alan bireyler siber güvenliği sağlamada rol oynayabilecekleri gibi siber saldırının ya da saldırılara sebep olan açıkların kaynağı da olabilmektedir (Dhillon, 2020; Fischer, 2016). Bu durum siber güvenliğin tehlikeye atan sistem dışı kaynaklar olabileceği gibi sistemde yer alan kullanıcıların da olabileceğini işaret etmektedir. IBM (2021), siber saldırıların %95'inin kullanıcı kaynaklı olduğunu raporlamıştır. Bu doğrultuda sistemde yer alan tüm paydaşların siber güvenlik hakkında farkındalık kazanmasının ve eğitilmesinin önemli olduğu araştırma kapsamında elde edilen bulgularla desteklenmiştir. Açık ve uzaktan öğrenme sistemleri kapsamında düşünüldüğünde bu bireylerin öğrenenler, öğretenler ya da yöneticiler olabileceği gibi personel çatısı altında teknik ve teknolojik hizmetlerden sorumlu olan teknik personel de olacağı söylenebilir. Bu noktada araştırmada elde edilen bulgular, teknik personelin siber güvenlik senaryolarında çoğunlukla öngörü, tespit ve savunma faaliyetlerinde yer aldığını

işaret etmektedir. Dolayısıyla açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanmasında teknik personelin aktif güvenlik faaliyetlerde rol oynadığı olduğu düşünülebilir.

Açık ve uzaktan öğrenme faaliyetlerinin zamansal, mekânsal ve etkileşimsel uzaklık ögeleri barındırmasından dolayı farklı hizmet yapılarıyla öğrenme süreçlerinin desteklenmesi gerekmektedir (Roddy vd., 2017; Tuquero, 2011). Destek hizmetleri olarak adlandırılan bu yapılanma, farklı paydaşların değişen ihtiyaç ve beklentileri doğrultusunda pek çok farklı tanım ve sınıflama ile ele alınmaktadır (Genç Kumtepe vd., 2019). Açık ve uzaktan öğrenme sistemlerinde siber güvenliğin incelendiği bu çalışmada, güvenlik faaliyetleri teknik bir yapıyı temsil ettiği için sahip olduğu için teknik destek hizmetleri bu faaliyetlerin merkez üssü olarak görülmektedir. Ayrıca destek yapıları öğrenen ya da öğreten olmak üzere farklı paydaşları kapsamasına rağmen teknik destek hizmetleri tüm paydaşları ve sistemin kendisini kapsamaktadır (Alshammari, 2020). Dolayısıyla tüm paydaşları ve sistemin kendisini ilgilendiren ve etkileyen siber güvenlik faaliyetlerini de teknik destek hizmetleri kapsamında ele almak mümkündür. Bu noktada teknik destek hizmetlerinin kapsamında siber güvenlik faaliyetlerinde hizmet vermesi beklenen bireylerin Sınırlı Rasyonellik Kuramı kapsamında sınırlı bir bilişsel yapıya sahip olduğu, araştırma kapsamında elde edilen bulgular tarafından desteklenmiştir. Fakat açık ve uzaktan öğrenme sistemlerinde doğrudan bu işe adanmış bireylerin, ekiplerin ya da birimlerin olmadığı; tüm faaliyetlerin sadece teknik hizmet olarak tanımladığı belirtilmiştir. Siber güvenliğin sistemin kendisini ilgilendiren, tüm paydaşların dahil olduğu bir süreç olduğunu göz önünde bulundurmak önemlidir. Bunun yanı sıra sistem kullanıcıları arasında olan öğrenen ve öğretenlerin de saldırıların farkına varma, bu saldırılara yönelik önlemler alma ve bu doğrultuda belirli kararlar alarak saldırılardan korunma gibi konularda sınırlı bir bilgi, değerlendirme ve karar verme yetisine sahip olduğu görülmüştür.

5.3. Açık ve Uzaktan Öğrenmede Siber Güvenliğin Sağlanmasında Endüstrileşme

Açık ve uzaktan öğrenmede siber güvenliğin sağlanması süreçlerinde sistem paydaşlarının ve teknik destek ekibinin sınırlı bilişsel doğası göz önünde bulundurulduğunda, bu bireylerin güvenliğini sağlamak için insan faktöründen nispeten

arındırılmış bir yapının kullanılmasının daha rasyonel ve güvenli sistemi meydana getireceği düşünülmektedir. Bu doğrultuda "*açık ve uzaktan öğrenme sistemlerinin teknik destek hizmetlerinde siber güvenliğin sağlanması için makine öğrenmesinden nasıl yararlanılabilir?*" araştırma sorusu aracılığıyla rasyonel ve mekanik bir yapıdan söz edebilmek için 8 alan uzmanından rasyonelliği sınırlayan beş faktöre yönelik çözüm önerileri alınmıştır.

Otto Peters (1993: 2000)'ın Endüstrileşme Kuramı, mektupla başlayıp güncel internet teknolojileriyle devam eden açık ve uzaktan öğrenmenin endüstrileşmesi doğrudan eğitimin endüstrileşmesini değil; eğitimle ilişkili faaliyetlerin, içeriklerin ve süreçlerin öğrenme süreçlerindeki üretimine, dağıtımına ve kullanımına yönelik bir endüstriyel bakışı temsil etmektedir. Araştırma kapsamında elde edilen bulgular, endüstrileşme kuramının çoğunlukla içerik üretimiyle ve dağıtımıyla ilişkilendirildiğini; genelde teknik destek hizmeti faaliyetlerde özelde siber güvenlik faaliyetlerinde de benzer yapının kullanılması gerektiğini göstermektedir. Çünkü açık ve uzaktan öğrenme sistemlerinin teknik ve teknolojik yapısı kapsamında hizmet veren teknik destek hizmetleri; eğitsel faaliyetlerin, süreçlerin ve içeriklerin üretimini, dağıtımını, devamlılığını ve sürdürülebilirliğini doğrudan etkilemektedir (Fırat, 2020; Yumurtacı, 2020). Dolayısıyla teknik destek hizmetlerinin endüstriyel bir formatta yapılanmasının hem sistemin endüstriyel formdaki birimleriyle uyumlu olması hem de siber güvenliğin rasyonel ve mekanik bir şekilde yapılandırılması adına önemli ve gerekli olduğu söylenebilir.

Teknik destek hizmetleri kapsamında incelenen siber güvenliğin, insan faktörünün sınırlı doğasını gerek sistem kullanıcısı gerek teknik ekip elemanı olarak barındırdığı, araştırma kapsamında elde edilen bulgular tarafından desteklenmektedir. Dolayısıyla endüstriyel bir destek yapısında rasyonelliği sınırlayan faktörlerin rasyonel ve mekanik yapılara dönüştürülmesinin faydalı olacağı düşünülebilir. Bu doğrultuda araştırma kapsamında on görüşme sorusu aracılığıyla elde edilen bulguların analiz edilmesiyle bulgulanan kod ve temaların hepsinde ön plana çıkan ortak önerinin akıllı sistemlerin kullanılmasına yönelik olduğu görülmektedir.

Geleneksel siber güvenlik, belirli stratejiler ve kurallar çerçevesinde güvenlik protokollerinin uygulanması için sistemlerin donanım, yazılım ve ağ yapılarının izlendiği güvenlik duvarları, sızma tespit sistemleri ve sızma önleme sistemleri gibi statik kontrol

mekanizmalarının uygulanması gerekmektedir (Li, 2018). Ancak bu pasif savunma yöntem ve yaklaşımlar, dijital teknolojilerin kullanımının ve büyük verinin hızlı artışından dolayı giderek genişleyen, belirsizleşen ve agresifleşen siber uzamdaki yeni siber tehditlere karşı yalnız başına etkili ve hızlı yanıtlar oluşturmakta yetersiz kalmaktadır (Zhang vd., 2021).

Bu araştırma kapsamında elde edilen bulgular, verilerle öğrenen akıllı sistemlerin açık ve uzaktan öğrenmenin güvenliğini sağlamak ve sürdürmek için güvenlik faaliyetlerinde rol oynaması gerektiğini belirtmektedir. Siber saldırılara cevap verebilmek ya da siber saldırılara karşı güçlü olabilmek ve sistemlerin korunması uygulamak için sistemin geçmiş ve güncel güvenlik durumu verilerini elde etmesi ve uyarlanabilir güvenlik yönetimi ve kontrolü sağlayabilecek akıllı kararlar alması gerekir (Li, 2018). Dolayısıyla destek hizmeti yapılarında Bulgular; makine öğrenmesi, derin öğrenme ve doğal dil işleme gibi yapay zekâ yaklaşımlarının bu süreçlerde kullanılabileceğini işaret etmektedir. Benzer bir yaklaşımla öğrenen desteğinde akıllı sistemlerden doğal dil işleme teknolojilerinin kullanılabileceğini belirten Fırat (2020)'ın bulgularından yola çıkarak bu teknolojilerin genelde teknik destek hizmetlerinde de kullanılabileceği araştırma kapsamında elde edilen bulgular doğrultusunda söylenebilir.

6. SONUÇ VE ÖNERİLER

Açık ve uzaktan öğrenmede teknik destek hizmetleri kapsamında siber güvenliğin nitel araştırma yöntemlerinden durum çalışması yaklaşımıyla incelendiği araştırmanın bu bölümünde, doküman incelemesi doğrultusunda oluşturulan 10 görüşme sorusu aracılığıyla 8 alan uzmanından elde edilen bulgular doğrultusunda araştırma sonuçlarına ve ileri yönelik önerilere yer verilmiştir.

Açık ve uzaktan öğrenme toplulukları ve bu toplulukları barındıran sistemler, teknolojinin araç ya da aracı olarak kullanıldığı öğrenme faaliyetleri, uygulamaları ve planlamaları çerçevesinde kendine özgü bir atmosferi olan yapıları temsil etmektedir. Bireysel farklılıklarla zenginleşen açık ve uzaktan öğrenme ortamlarında, ilgili farklılıklar kapsamında çeşitlenen farklı beklenti ve ihtiyaçlardan söz etmek mümkündür. Bu beklenti ve ihtiyaçlar öğrenenlerin zamandan ve mekândan bağımsız esnek öğrenmelerini kapsadığı gibi öğrenme süreçlerine dahil olan öğretim elemanlarının,

personelin ve yöneticilerin de yer aldıkları faaliyetlere ve durumlara göre şekillenebilmektedir. Sistem çatısı altında yer alan tüm ihtiyaçların incelendiği, değerlendirildiği ve çözüm odaklı faaliyetlerin gerçekleştirildiği yapılanmalar destek hizmetlerini temsil etmektedir. Farklı paydaşların değişen ihtiyaç ya da beklentilerine göre şekillenen destek faaliyetleri, farklı tanımlar ve sınıflandırmalar kapsamında incelenmektedir. Tüm tanımların çıkış noktası ise açık ve uzaktan öğrenme faaliyetlerinin sürdürülebilir ve verimli olmasını sağlamaktır. Teknik ve teknolojik yapısı dolayısıyla bu ihtiyaç ya da beklentilerin hiyerarşik bir süreci temsil ettiği düşünülebilir. Bu noktada Maslow'un ihtiyaçlar piramidi açık ve uzaktan öğrenmeye aşağıdaki gibi uyarlanabilir.

Şekil 6.1. *Maslow'un ihtiyaçlar hiyerarşinin açık ve uzaktan öğrenmeye uyarlanması*

Sisteme ve öğrenme faaliyetlerine dahil olmak isteyen bireylerin, azami düzeyde bir teknolojik hazırbulunuşluğunun (fiziksel ihtiyaç) olması gerektiği düşünülebilir. Maslow'un hiyerarşi doğrultusunda ilerlendiğinde ise ikinci basamağın güvenlik olduğu görülmektedir. Gerek bireylerin, teknolojilerin, faaliyetlerin ve alt yapı servislerinin; gerekse sistemin kendisinin güvenliği, farklılaşan ve çeşitlenen faaliyetler ve uygulamalar kapsamında ortaya çıkan ya da çıkması öngörülen ihtiyaçlar doğrultusunda ikincil önemli ihtiyaca denk gelmektedir. Öğrenme süreçlerini sürdürmeye yetecek azami teknoloji varsa öncelikli çaba bu teknolojinin ve bu teknolojiyle etkileşime giren bireylerin ve nesnelerin güvenliğini sağlamak olmalıdır. Araştırma kapsamındaki bulgular, sistem yapılanmalarının siber güvenlik uygulamalarını ve siber saldırı faaliyetlerini göz önünde bulundurarak yapılandırılması gerektiğini göstermiştir. Siber güvenlik kurum kültürünün

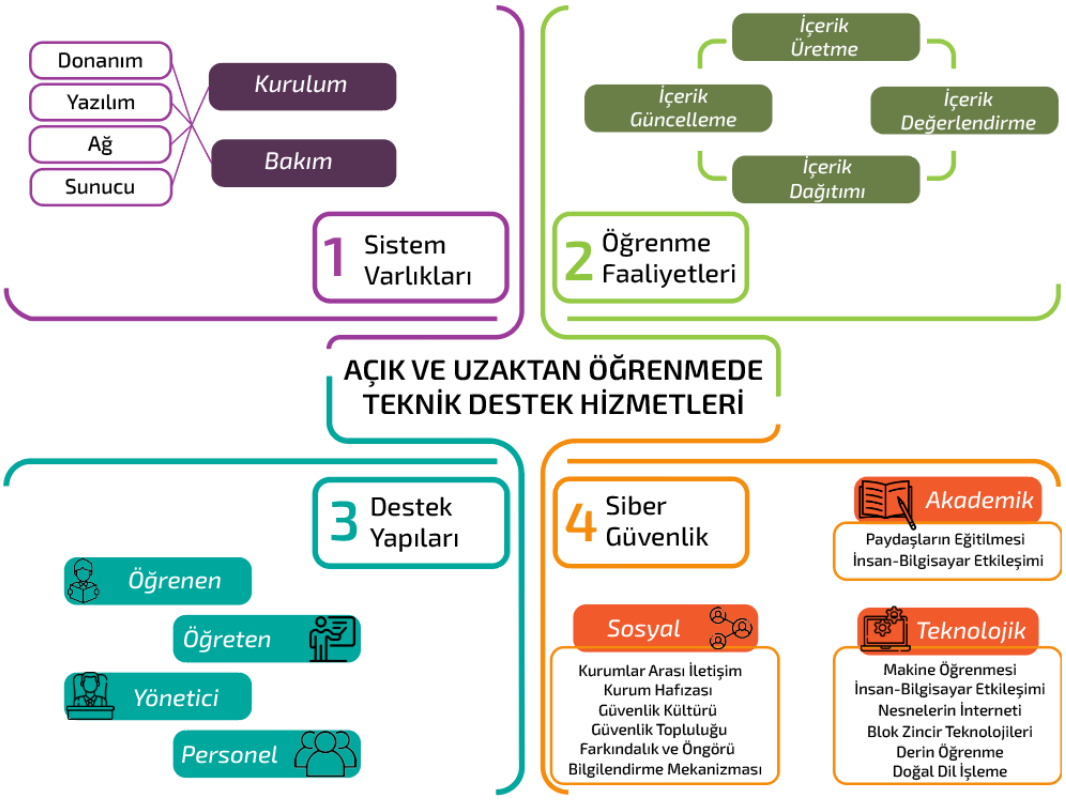
oluşturulmasının, siber güvenlik uygulamalarının ve siber güvenlik faaliyetlerinde rol oynayacak teknik ekibin yönetim tarafından desteklenmesinin önemli olduğu sonucuna ulaşılmıştır.

Bu araştırma kapsamında açık ve uzaktan öğrenme sistemleri çatısında hizmet veren teknik destek birimlerinin ayrı bir rol ve sorumluluk tanımı olan siber güvenlik birimlerinin kurulmasıyla etkileşimli olarak desteklenmesi ve beslenmesi gerektiğine ulaşılmıştır. Gerek sistem paydaşlarına gerekse teknik destek ekibine siber güvenlik farkındalığı kazandırma ve rol tanımları doğrultusunda eğitimler verilmesi önemlidir. Bilgi tabanlı sistemlerin oluşturulması, bu sistemlerin ihtiyaca yönelik sorgulara anlık yanıt veren bir yapısının olması, sürekli güncellenmesi ve geçmiş verilerle beslenerek kurum hafızası oluşturulması mevcut ve geleceğe yönelik siber güvenlik faaliyetlerini şekillendirmede faydalı olacaktır. Bu doğrultuda uygulama, enformasyon ve bilgi toplulukları göz önünde bulundurularak "güvenlik topluluklarının" oluşturulması önerilebilir.

Siber güvenliğin sağlanmasında pek çok paydaşın tanımlı ve tanımsız olmak üzere çeşitlenen rolleri ve sorumlulukları olduğu söylenebilir. Siber tehditler ya da saldırılar sistem dışındaki saldırganlardan kaynaklanabildiği gibi sistemin içinde yer alan kullanıcıların hareketlerinden de kaynaklanabilmektedir. Bireylerin sınırlı bilişsel doğası göz önünde bulundurulduğunda tehdit ve saldırı kaynaklarının sınırlı bilgi, yetenek, değerlendirme ve kara yetisi ile sınırsız belirsizlikten kaynakladığı görülmektedir. Bu doğrultuda uzmanlardan elde edilen bulgular, insan faktörünün siber güvenlik zincirindeki en zayıf halka olduğunu göstermektedir. Bu noktada açık ve uzaktan öğrenme sistemlerindeki teknik destek ekiplerinin desteklenmesinde ve siber güvenliğin sağlanmasında rasyonel ve mekanik yapılanmalar benimsenebilir. Araştırma kapsamında elde edilen bulgular, siber güvenliğin sağlanması faaliyetlerinde akıllı sistemlerin kullanımının hem bireylerin hem birimlerin hem de sistemin kendisinin güvenliğini sağlamada rasyonel bir mekanikleşmeyi meydana getireceğini göstermektedir. Özellikle öğrenen yapıların kurulmasına yönelik vurgulanan görüşler, makine öğrenmesi gibi yöntemlerin bu tür faaliyetlerde daha etkin, etkili ve verimli olacağını göstermektedir.

Açık ve uzaktan öğrenme sistemlerinde teknik ve teknolojik yapıların öğrenme süreçlerindeki bütün faaliyetlerde kullanılıyor olması, bu sistemlerin teknik yönüne vurgu yapar niteliktedir. Dolayısıyla teknik destek hizmetlerinin öncelikle sistemin kendisini

daha sonra farklı beklentilere ve kurumsal yaklaşımlara göre şekillenen diğer destek yapılarını içine alması gerektiği düşünülmektedir. Yukarıda bahsi edilen Maslow hiyerarşisi de göz önünde bulundurularak teknik ve teknolojik yapılanmanın kurulmasının ardından bu yapılanmanın öncelikle güvenliğinin sağlanması gerektiği söylenebilir. Araştırma kapsamında elde edilen bulgular, siber güvenliğin sağlanmasında sınırlı bir rasyonellik olduğunu destekler niteliktedir. Bu nedenle siber güvenliğin sağlanmasında teknik destek yapısının endüstrileştirilmesi öngörülmektedir. Elde edilen bulgular doğrultusunda teknik destek hizmetleri yapısının aşağıdaki gibi modellenmesi önerilebilir.



Şekil 6.2. *Açık ve uzaktan öğrenmede teknik destek hizmeti modeli*

Yukarıda yer alan şekildeki teknik destek hizmeti modeli, 4 temel bileşenden oluşmaktadır. Bu bileşenlerden ilki olan sistem varlıkları, açık ve uzaktan öğrenmedeki teknolojik hazırbulunuşluğu besleyen ve sürdürülebilir kılan sistem varlıklarının desteklenmesini kapsamaktadır. Açık ve uzaktan öğrenme faaliyetlerinin gerçekleştirilmesi için gerekli olan sistem varlıklarının kurulumunun ve bu varlıkların sürdürülebilirliğini sağlamanın, teknik destek hizmetlerinin bu bileşeni ile sağlanması öngörülmektedir. Öğrenme faaliyetlerinin gerçekleştirilmesinde ve yürütülmesinde ise

içeriklere ve içeriklerin yönetilmesine dair yapılanması gerektiği düşünülen teknik destek hizmeti bileşeni ise öğrenme faaliyetleri kapsamında ele alınabilir. Bu kapsamda farklı ihtiyaçlar doğrultusunda farklı amaçlara hizmet eden çeşitli içeriklerin farklı bireyler ve birimler tarafından gerek akademik gerekse teknik bağlamda ele alınabilir. İçeriklerin üretilmesi, değerlendirilmesi, dağıtılması ve güncellenmesi, bu çatı altında sürdürülebilir.

Teknik ve teknolojik bir yapılanmayı temsil eden açık ve uzaktan öğrenme faaliyetlerinin öğrenme faaliyetlerinde teknolojiyi ön koşul olarak kullanması, teknolojiyi destekleyen ve teknoloji tabanlı desteklenen farklı hizmetleri kapsayabilmektedir. Bu hizmetlerin sistemde yer alan öğrenen, öğreten, personel ve yönetici paydaşlarının tümü kapsadığı bulgular tarafından desteklenmektedir. Dolayısıyla teknik destek hizmetlerinin çatı bir destek yapısı olarak kurgulanmasının önemli olduğu düşünülmektedir. Her ne kadar kurumsal kültür ve yaklaşımlara göre şekillenen farklı destek yapıları olduğunu söylemek mümkün olsa da bu doğrultuda yürütülen açık ve uzaktan öğrenme faaliyetlerindeki teknik destek hizmeti modelinin genel kapsamda farklı paydaşların tümünü kapsaması gerektiği öngörülebilir.

Teknik destek hizmetleri kapsamındaki son bileşen olan siber güvenlik, sistemde yer alan varlıkların, bireylerin ve sistemin kendisini doğrudan ilgilendirmektedir. Dolayısıyla teknolojik tekniklerin öğrenme süreçlerine dahil olduğu açık ve uzaktan öğrenme faaliyetlerinin tümünde güvenlik faaliyetlerine öncelik verilmesi gerektiği görülmüştür. Teknik destek hizmetleri çatısı altında incelenen bu bileşen akademik, sosyal ve teknolojik olarak üç temel başlıkta incelenebilir. Araştırma kapsamında yapılan doküman incelemeleri ve görüşmeler, bu yaklaşımı destekler niteliktedir. Bu doğrultuda açık ve uzaktan öğrenme faaliyetlerinde ve teknik destek hizmetlerinde rol oynayan bireylerin eğitilmesi, kurumsal farkındalık oluşturulması ve tüm bu faaliyetlerde insan-bilgisayar etkileşiminin sağlanması siber güvenliğin sağlanmasındaki akademik boyutu kapsamaktadır. Aynı zamanda sistemin güvenliğini sağlamada endüstrileşmeye gidilmesinde rol oynayacak teknik ekibin akıllı sistemleri kodlama ve bunu siber güvenlik çerçevesinde gerçekleştirebilmesi, bu faaliyetlerin gerekliliğini işaret etmektedir. Bunlar sosyal boyutu temsil ederken şunlar teknolojik boyutu ön plana çıkarmaktadır.

Açık ve uzaktan öğrenme sistemlerinde teknik destek hizmetleri kapsamında siber güvenliğin sağlanmasında sosyal bir boyutun olduğundan da söz etmek mümkündür. Araştırma kapsamında elde edilen bulgular siber güvenlik kapsamında kurum hafızasının

oluşturulması, birimler arası iletişim ve koordinasyonun sağlanması, güvenlik kültürünün oluşturulması, güvenlik topluluklarının oluşturulması ve bilgilendirme mekanizmalarının kurulması gerektiğini göstermiştir. Bu mekanizmalarda makine öğrenmesinin kullanıldığı akıllı sistemlere ihtiyaç olduğunu öngören araştırma bulguları, bu faaliyetlerde de farkındalık ve öngörü çalışmalarının göz önünde bulundurulmasını ve farklı kurumlarla iletişim halinde olunması gerektiğini göstermiştir. Dolayısıyla siber güvenliğin sağlanmasındaki sosyal boyutun siber güvenlik çerçevesinde şekillenecek sistem yapılanmasında önemli olduğu düşünülmektedir.

Açık ve uzaktan öğrenme sistemlerinde siber güvenliğin sağlanması adına hem akademik hem de sosyal boyutlarda beslenen teknolojik boyut, öğrenme faaliyetlerindeki teknik ve teknolojik yapılanmayı kapsar niteliktedir. İlgili boyutlarda verilen bileşenlerin yanı sıra siber güvenliğin sağlanmasında farklı teknik ve teknolojilerin kullanılmasını kapsayan bu boyutta insan-bilgisayar etkileşiminin gözetilerek makine öğrenmesi, nesnelerin interneti, blok zincir teknolojileri, derin öğrenme modelleri ve doğal dil işleme teknolojilerinin kullanılması, araştırma bulguları tarafından desteklenmektedir. Siber güvenliğin sağlanmasında bilişsel rasyonelliğin endüstrileşmiş bir hizmet yapısına dönüşmesini öngöre bu çalışma, güvenlik faaliyetlerinde akademik, sosyal ve teknolojik boyutların birbirini beslediği söylenebilir.

Akademik boyutu temsil eden bulgularda siber güvenliğin sağlanması için kullanılacak makine öğrenmesi algoritmalarının ve mekanizmalarının oluşturulmasında eğitimli ve nitelikli personelin işe alınmasının önemli olduğu belirtilmiştir. Aynı zamanda bu bağlamda faaliyet gösterecek kişilerin siber güvenlik eğitimleri almış kişiler olması gerektiği vurgulanmıştır. Bulgulardan da elde edilen sonuçlar doğrultusunda makine öğrenmesinin siber güvenlik faaliyetlerinde rol oynayan bireylerin sınırlı doğasını desteklemesi; fakat bu destek yapısının oluşturulması için ise nitelikli bireylerin sürece dahil edilmesi gerektiği sonucu çıkarılabilir. Dolayısıyla bu noktada insan-bilgisayar etkileşiminin göz önünde bulundurulması gerektiği görülmektedir. Bu boyutun hem teknik hem de akademik bir kapsama sahip olduğu düşünülebilir. Bunların yanı sıra teknik bir bakış açısıyla siber güvenliğin sağlanmasında nesnelerin interneti, blok zincir teknolojileri, derin öğrenme modelleri ve doğal dil işleme gibi farklı tekniklerin ve teknolojilerin öğrenen akıllı sistemleri oluşturmada önemli olduğu belirtilmiştir.

Dolayısıyla siber güvenliğin sağlanmasında makine öğrenmesi hem sosyal hem akademik hem de teknik açıdan başvurulması gereken bir yaklaşım olarak görülmektedir.

Elde edilen bulgular doğrultusunda açık ve uzaktan öğrenme faaliyetlerinin gerçekleştirilmesi ve sürdürülebilirliğinin sağlanması adına güvenlik faaliyetlerinin sistem yapılanmasının temeline oturulması önerilmektedir. Teknik ve teknolojik süreçlerin öğrenme faaliyetlerindeki yeri ve önemi açık ve uzaktan öğrenmeye uyarlanan Maslow hiyerarşisi de göz önünde bulundurulduğunda, sistem yapılanmalarının güvenlik endişelerine öncelik vererek şekillendirilmesi gerektiği düşünülmektedir. Aynı zamanda açık ve uzaktan öğrenme faaliyetlerinin güvenle sürdürülebilmesi adına siber güvenliğin teknik ve teknolojik yönlerinin yanı sıra akademik ve sosyal boyutlarının da göz önünde bulundurulması gerekmektedir. Uygulamaya yönelik faaliyetlerde siber güvenlik kültürünün kurumsal kültür çerçevesinde şekilleneceği düşünülerek, sistem bazlı güvenlik yaklaşımının birey ve birim odaklı çözümler sunması gereken bir bütünü oluşturacağı unutulmamalıdır.

KAYNAKÇA

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), 1-15.

Alemdağ, E., Çevikbaş, S. G., & Baran, E. (2019). The design, implementation and evaluation of a professional development programme to support teachers' technology integration in a public education center. *Studies in Continuing Education*, 1-27.

Alexei, A. (2021). Cyber security strategies for higher education institutions. *Journal of Engineering Science, 2021*(4), 74-92.

Alexei, A., & Alexei, A. (2021). Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. *International Journal of Scientific & Technology Research, 10*, 128-133.

Alferidah, D. K., & Jhanjhi, N. Z. (2020, October). Cybersecurity impact over bigdata and iot growth. In *2020 International Conference on Computational Intelligence (ICCI)* (pp. 103-108). IEEE.

Almaiah, M. A., Al-Khasawneh, A., & Althunibat, A. (2020). Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic. *Education and Information Technologies, 25*, 5261-5280.

Alshammari, S. H. (2020). The Influence of Technical Support, Perceived Self-Efficacy, and Instructional Design on Students' Use of Learning Management Systems. *Turkish Online Journal of Distance Education, 21*(3), 112-141.

Altınpulluk, H. (2018). Nesnelerin interneti teknolojisinin eğitim ortamlarında kullanımı. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi (AUAd), 4*(1), 94-111

Antwi-Boampong, A. (2021). An Investigation into Barriers Impacting Against Faculty Blended Learning Adoption. *Turkish Online Journal of Distance Education, 22*(3), 281-292.

Arko-Achemfuor, A. (2017). Student support gaps in an open distance learning context. *Issues in Educational Research, 27*(4), 658-676.

Aytaçlı, B. (2012). Durum çalışmasına ayrıntılı bir bakış. *Adnan Menderes Üniversitesi Eğitim Fakültesi Eğitim Bilimleri Dergisi*, *3*(1), 1-9.

Baltacı, A. (2019). Nitel araştırma süreci: Nitel bir araştırma nasıl yapılır?. *Ahi Evran Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *5*(2), 368-388.

Bandara, I., Ioras, F. & Maher, K. (2014). Cyber Security Concerns in E-Learning Education. *In: Proceedings of ICERI2014 Conference* (728-734), IATED.

Baran, E. & Correia, A. P. (2016). What motivates exemplary online teachers? A multiple-case study. *Learning, Design, and Technology*, 1-17.

Berge, Z.L. (1995). Facilitating computer conferencing: Recommendations from the field. *Educational Technology*, *35*(1), 22-30.

Bone, J. (2016). Cognitive Risk Framework for Cybersecurity: Bounded Rationality: Executive Summary: Part I. *EDPACS*, *54*(5), 1-11.

Brindley, J. E. (1987). *Attrition and completion in distance education: The student's perspective* (Doctoral dissertation, University of British Columbia).

Brindley, J. (1995). Learners and learner services: The key to the future in open distance learning. *Why the information highway*, *102*, 125.

Brindley, J. E. (2000). *The effects of a social support intervention on distance learner behaviour*. Doctoral dissertation, University of Ottawa.

Birochi, R., & Pozzebon, M. (2011). Theorizing in distance education: The critical quest for conceptual foundations. *MERLOT Journal of Online Learning and Teaching*, *7*(4), 562-575.

Candoğan, O. (2020). *Bir IBM Araştırmacısına Göre Intel'in Moore Yasası'nın Sonuna Gelindi*. Erişim Adresi: https://www.webtekno.com/moore-yasasinin-sonuna-mi-geldik-h80436.html (Son erişim tarihi: 17.01.2022).

Chadd, K. (2020). *The history of cybersecurity*. Erişim adresi: https://blog.avast.com/history-of-cybersecurity-avast#the-1960s (Son erişim tarihi: 16.01.2022).

Chowdhury, N. H., Adam, M. T., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*, *97*, 101931.

Chua, Y. T., Parkin, S., Edwards, M., Oliveira, D., Schiffner, S., Tyson, G., & Hutchings, A. (2019). Identifying unintended harms of cybersecurity countermeasures. In *2019 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1-15). IEEE.

Creswell, J. W. (2013). *Research design: qualitative, quantitative, and mixed methods approaches* (4th Edition). London: Sage Publications.

Çalışkan, H. (2015). Bilişim Güvenliği. G. Eby & M. R. Okur (Eds.). *Temel Bilgi Teknolojileri-II* (38-60). Eskişehir: Anadolu Üniversitesi.

Çiftçi, A., & Karakuş, Y. (2019). Dijitalleşen Zamanın İzdüşümünde: Kimliğin, Bedenin ve İletişimin Dönüşümü. *AJIT-e: Bilişim Teknolojileri Online Dergisi*, *10*(37), 7-30.

Dalton, C., Thornton, A., Dinsmore, C., Beyer, W., Akiva, K., & King, B. (2019). Multidisciplinary team-based model for faculty supports in online learning. *Collected*
Essays on Learning and Teaching, 12, 127-138.

Dhillon, M. (2020). Challenges and Issues of E-Learning. In *Emerging Trends in Big Data IoT, and Cybersecurity* (182-184).

Durak, G. (2017). Uzaktan eğitimde destek hizmetlerine genel bakış: sorunlar ve eğilimler. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi, 3*(4), 160-173.

El Turk, S. & Cherney, I. (2016). Perceived online education barriers of administrators and faculty at a U.S. university in Lebanon. *Creighton Journal of Interdisciplinary Leadership, 2*(1), 5-31.

Fırat, M. (2016). 21. Yüzyılda Uzaktan Öğretimde Paradigma Değişimi. *Yükseköğretim ve Bilim Dergisi*, *6*(2), 142-150.

Fırat, M. (2020). Öğrenci destek servislerinde doğal dil işleme: GPT-3 örneği. In *International Conference of Strategic Research in Social Science and Education* (pp. 532-536).

Fırat, M. (2021). *Uygulamadan Kurama Açık ve Uzaktan Öğrenme* (2. Baskı). Nobel Yayınları.

Fischer, E. A. (2016). *Cybersecurity issues and challenges: In brief*.

Floyd, D. L. & Casey-Powell, D. (2004). New roles for student support services in distance learning. *New directions for community colleges, 2004*(128), 55-64.

Fraenkel, J. R., Wallen, N. E. & Hyun, H. H. (2012). How to Design and Evaluate Research in Education (8th Edition). New York: McGrae-Hill Companies.

Garrison, R. (2000). Theoretical challenges for distance education in the 21st century: A shift from structural to transactional issues. *International Review of Research in Open and Distributed Learning, 1*(1), 1-17.

Garrison, D.R. & Baynton, M. (1987). Concepts: Beyond independence in distance education: The concept of control. *The American Journal of Distance Education, 1*(3), 3-15.

Genç Kumtepe, E., Toprak, E., Öztürk, A., Tuna Büyükköse, G., Kılınç, H., & Aydın Menderis, İ. (2019). Açık ve uzaktan öğrenmede destek hizmetleri: Yerelden küresele bir model önerisi. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi, 5*(3), 41-80.

Gökmen, Ö. F., Duman, İ., & Horzum, M. B. (2016). Uzaktan eğitimde kuramlar, değişimler ve yeni yönelimler. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi, 2*(3), 29-51.

Grimes, R. A. (2020). *9 types of malware and how to recognize them*. Erişim Adresi: https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html (Son erişim tarihi: 16.06.2021)

Gutiérrez-Santiuste, E., Gámiz-Sánchez, V. M., & Gutiérrez-Pérez, J. (2015). MOOC & B-learning: Students' Barriers and Satisfaction in Formal and Non-formal Learning Environments. *Journal of Interactive Online Learning, 13*(3).

Gümüş, S. (2020). Açık ve Uzaktan Öğrenme Destek Hizmetlerinde Teknolojinin Kullanımı. M. Kesim & T. V. Yüzer (Eds.). *Açık ve Uzaktan Öğrenmenin Teknoloji Boyutu* (263-283). Ankara: Pegem Yayınları.

Gürer, M. D., Tekinarslan, E. & Yavuzalp, N. (2016). Çevrim içi ders veren öğretim elemanlarının uzaktan eğitim hakkındaki görüşleri. *Turkish Online Journal of Qualitative Inquiry*, *7*(1), 47-78.

Hardman, S. L. & Dunlap, J. C., (2003). Learner support services for online students: scaffolding for success. *The International Review of Research in Open and Distributed*
Learning (IRRODL), *4*(1).

Holmberg, B. (1995). *Theory and practice of distance education*. London and New York: Routledge.

Hughes, G., (2007). Using blended learning to increase learner support and ımprove retention. *Teaching in Higher Education, 12*(3), 349-363.

Hui, H. W. (1989). Support for students in a distance learning programme – an experience with a course in Fashion and Clothing Manufacture. A. Tait (Ed.), In *Conference papers: Interaction and Independence: Student Support in Distance Education and Open Learning* (129-141). Cambridge: The Open University.

IBM (2021). Why Human Error is #1 Cyber Security Threat to Business in 2021. Erişim Adresi: https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html#:~:text='Human%20error%20was%20a%20major,in%2095%25%20of%20all%20breaches.&text=Mitigation%20of%20human%20error%20must,cyber%20business%20security%20in%202021. (Son erişim tarihi: 30.01.2022)

Inkelaar, T. & Simpson, O. (2015) Challenging the 'distance education deficit' through 'motivational emails'. *Open Learning*, *30*(2), 152-163.

Jang-Jaccard, J. & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993.

Kaspersky (2021). *Bilgisayar Virüsleri ve Kötü Amaçlı Yazılımlarla İlgili Bilgiler ve SSS.* Erişim Adresi: https://www.kaspersky.com.tr/resource-center/threats/computer-viruses-and-malware-facts-and-faqs (Son erişim tarihi: 06.08.2021).

Kaspersky (2021). *Rootkit nedir – Tanım ve Açıklama.* Erişim Adresi: https://www.kaspersky.com.tr/resource-center/definitions/what-is-rootkit (Son erişim tarihi: 06.12.2021).

Keast, D. A. (1997). Toward an effective model for implementing distance education programs. *American Journal of Distance Education*, *11*(2), 39-55.

Keegan, D. (2003). *Pedagogy and support systems in e-learning*. ZIFF PAPIERE 121.

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic.

Khanna, P. & Basak P. (2013). An OER architecture framework: Needs and design. *The International Review of Research in Open and Distributed Learning*, *14*(1), 66-83.

Kron. (2021). *En Sık Karşılaşılan 10 Siber Saldırı Yöntemi.* Erişim Adresi: https://kron.com.tr/en-sik-karsilasilan-10-siber-saldiri-yontemi (Son erişim tarihi 06.08.2021).

Lee, J. Y. (2003). Current status of learner support in distance education: emerging issues and directions for future research. *Asia Pacific Education Review*, *4*(2), 181-188.

Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474.

Malyuk, A., & Miloslavskaya, N. (2016, July). Cybersecurity culture as an element of IT professional training. In *2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC)* (pp. 205-210). IEEE.

McLoughlin, C. (2002). Learner support in distance and networked learning environments: Ten dimensions for successful design. *Distance Education 23*(2), 149-162.

Mısırlı, Z. A., İzmirli, S. & Şahin İzmirli, Ö. (2018). Öğretim elemanlarının uzaktan eğitime ilişkin farkındalıkları. H. Gür, & H. H. Şahan (Eds.), *Uluslararası Necatibey Eğitim ve Sosyal Bilimler Araştırmaları Kongresi* (480-486). Balıkesir: Balıkesir Üniversitesi.

Miles, M. B & Huberman, A. M. (1994). Qualitative Data Analysis. London: Sage Publication.

Minh Hoang T. B., Dang-Pham, D., Hoang, A. P., Le Gia, B. & Nkhoma, M. (2020). Network Analytics for Improving Students' Cybersecurity Awareness in Online Learning Systems. In *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)* (1-7). IEEE.

Montelongo, R. (2019). Less than/more than: Issues associated with high-impact online teaching and learning. *Administrative Issues Journal: Connecting Education, Practice, and Research*, *9*(1), 68-79.

Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics 38*(8).

Muilenburg, Y. L. & Berge, Z. (2005). Student barriers to online learning: a factor analytic study. *Distance Education, 26*(1), 29–48.

Nespoli, P., Papamartzivanos, D., Mármol, F. G., & Kambourakis, G. (2018). Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks. *IEEE Communications Surveys & Tutorials*, *20*(2), 1361-1396.

Okur, R. (2012). *Açık ve uzaktan öğrenmede öğretim elemanlarına yönelik çevrimiçi destek sistemi tasarımı* (Yayınlanmış Doktora Tezi, Anadolu Üniversitesi).

Özden, M. Y & Durdu, L. (2016). *Nitel Araştırma Yöntemleri*. Ankara: Anı Yayıncılık.

Peters, O. (1993). Distance education in a postindustrial society. D. Keegan (Ed.). *Theoretical principles of distance education* (39-58). Routledge.

Peters, O. (2002). *Distance education in transition: New trends and challenges* (5th Ed.). BIS Verlag.

Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. In *29th European Safety and Reliability Conference* (pp. 4036-4043).

Reid, J. (1995). Managing learner support. F. Lockwood (Ed.), In *Open and distance learning today* (265-275). London: Routledge.

Rekkedal, T. (1981). *Introducing the Personal Tutor/Counsellor in the System of Distance Education.* Project Report 1: Experiment Description.

Rekkedal, T. & Qvist-Eriksen, S. (2003). *Internet based e-learning, pedagogy and support systems*. Norway: NKI Distance Education.

Robinson, B. (1995). Research and pragmatism in learner support. F. Lockwood (Ed.), In *Open and distance learning today* (221-231). London: Open and distance learning today.

Roddy, C., Amiet, D. L., Chung, J., Holt, C., Shaw, L., McKenzie, S., Garicaldis, F., Lodge, J. M. & Mundy, M. E. (2017). Applying best practice online learning, teaching, and support to intensive online environments: an integrative review. *Frontiers in Education 2*(59).

Rowntree, D. (1992). *Exploring open and distance learning*. Routledge.

Sewart, D. (1980). Creating an information base for an individualized support system in distance education. *Distance Education, 1*(2), 171-187.

Sewart, D. (1993). Student support systems in distance education. *Open Learning, 8*(3), 3-12.

Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2014). AVOIDIT: A cyber attack taxonomy. In *9th annual symposium on information assurance* (pp. 2-12).

Simon, H. A. (1955). A behavioral model of rational choice. *The quarterly journal of economics, 69*(1), 99-118.

Simon, H. A. (1976). From substantive to procedural rationality. In *25 years of economic theory* (65-86). Springer, Boston, MA.

Simonson, M., Schlosser, C., & Hanson, D. (1999). Theory and distance education: A new discussion. *American Journal of Distance Education, 13*(1), 60-75.

Simpson, O. (2002). *Supporting students in online, open and distance education*. London: Routlege Falmer.

Subaşı, M., & Okumuş, K. (2017). Bir araştırma yöntemi olarak durum çalışması. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 21*(2), 419-426.

Tait, A. (2002). Rethinking learner support in the Open University UK. A. Tait & R. Mills (Eds.), In *Rethinking learner support in distance education: Change and continuity in an international context* (185-197). Routledge, London.

Tait, A. (2003). Reflections on student support in open and distance learning. *International Review of Research in Open and Distance Learning,* 4(1).

Thomas, G. (2011). A typology for the case study in social science following a review of definition, discourse, and structure. *Qualitative inquiry, 17*(6), 511-521.

Thomas, G. (2021). *How to do your case study*. London: Sage.

Thorpe, M. (2003). Collaborative online learning: Transforming learner support and course design. A. Tait & R. Mills (Eds.), In *Rethinking learner support in distance education* (198-211). London: Routledge Falmer.

Tuan, T. A. (2020). An intuitive software for teaching and learning cyber attacks. *TRƯỜNG ĐẠI HỌC THỦ ĐÔ HÀ NỘI, 39*, 126-134.

Turhan, E. (2002). Web tabanlı öğretimde etkileşim ve öğrenci destek hizmetlerinin geliştirilmesi. *Açık ve Uzaktan Eğitim Sempozyumu*, 23-25.

Tuquero, J. M. (2011). A meta-ethnographic synthesis of support services in distance learning programs. *Journal of Information Technology Education, 10*, 157-179.

Uslu, A. (2021). *Siber Saldırı Nedir?* Erişim Adresi: https://www.niobehosting.com/blog/siber-saldiri-nedir/#Siber_Saldiri_Korunma_Yontemleri (Son erişim tarihi 06.10.2021)

Yıldırım, A. & Şimşek, H. (2013). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri* (9. Baskı). Ankara: Seçkin.

Yin, R. K. (2009). *Case Study Research Design and Methods* (5. Baskı). London: Sage Publications.

Yin, R. K. (2017). *Applications of case study research* (3th Ed.). London: Sage.

Yumurtacı, O. (2020). Öğrenen, Öğreten ve Teknoloji. M. Kesim & T. V. Yüzer (Eds.). *Açık ve Uzaktan Öğrenmenin Teknoloji Boyutu* (1-27). Ankara: Pegem Yayınları.

Zawacki-Richter, O. (2004). The growing importance of support for learners and faculty in online distance education. J. Brindley, C. Walti, & O. Zawacki-Richter (Eds.), In *Learner support in open, distance and online learning environments* (205-217).

Zawacki-Richter, O. (2019). The Industrialization Theory of Distance Education Revisited. I. Jund (Ed.). *Open and Distance Education Theory Revisited Implications fort the Digital Era* (21-29). Springer: Singapore.

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2021). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1-25.